CSUS
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
Department of Computer Science (RVR 3018; 278-4238/6834)

CSC 153 Computer Forensics Principles and Practice/C Sc 253- Computer Forensics, Spring 2013 (MW 545-7pm; RVR 1006)

INSTRUCTOR: Isaac Ghansah
Office: RVR (ECS)-4004; Phone: 278-7659;
Email: ghansah@csus.edu (Please insert "CSc253 OR CSc153-" somewhere in the subject line);
No email via WebCT
WWW: http://gaia.ecs.csus.edu/~ghansah/;
Office Hours: MW 2-245, 7-715p, TU 11-12; and other times by appointment

153 & 253 Differences: Even though the classroom lectures will be the same for both courses, more will be expected from 253 students. The difference will be in some assignments and in some cases, exams. The instructor will use different methods including project proposals, additional examination questions, oral examinations, etc.

Introduction: This course will introduce you to the fundamentals of computer forensics and cyber-crime scene analysis including laws, regulations, international standards, and formal methodology for conducting computer forensic investigations. For the first time we will cover code analysis (reverse engineering, malware analysis) in addition to media analysis and network analysis. There will be hands-on laboratory assignments, use of forensic tools, and independent projects.

CATALOG DESCRIPTION:
CSC 253: Structured security incident investigations internal and external; emphasis on analysis of electronic evidence and proper audit; utilization of scientific aids in obtaining information from computing devices; legal electronic evidence.

Prerequisite: Fully Classified Graduate Status in CSC, SE, or CPE, or permission of instructor.

CSC 153: Fundamentals of computer forensics and cyber-crime scene analysis and electronic discovery. Topics include technical and formal methodology for conducting security incident investigations; file systems and storage analysis, data hiding techniques, network forensics; projects involving using, understanding, and design of digital forensic tools; anti-forensics; legal issues and standards. Prerequisite: CSc 138

Prerequisite Proof:
The Computer Science Department has a policy that each instructor will verify the student transcript and ascertain that the student has the prerequisites. You can log on to My Sac State go to "Student Center" and select "Unofficial Transcripts" to print. You also can select and print "Transfer Credit Report" if you have transferred from another institution. You must submit your transcript for verification, with the prerequisites EXPLICITLY IDENTIFIED BY CIRCLING, SHADING, etc. I WILL ALSO ACCEPT ELECTRONIC VERIFICATION PROVIDED THE PREREQUISITES ARE EXPLICITLY IDENTIFIED VIA SHADING, CIRCLING, ETC). Any student who has completed one or more prerequisites at another
school must provide similar verification to the instructor. Any student who has not submitted their transcript by the end of the second week will be dropped from the class.

Repeat Policy:

The department has a policy specifying that students may not repeat a Computer Science course more than once. Any student who wishes to repeat a course more than once (that is, take a course for a third time) must submit a petition requesting permission to do so. Student records will be reviewed to determine whether a student is taking this course for three or more times. Any such student must return an approved petition to the instructor within the first two weeks of class. Any student who does not submit an approved petition will be dropped from the class. Petitions are available in the Department office (RVR 3018) and require the signature of both the Instructor and the Dept. Chair.

Textbooks:

2. K. Jones, R Bejtlich, and C Rose, Real Digital Forensics, Addison Wesley, 2006
3. Ghansah I., C Sc 253/153 Class Notes, 2013 on SacCT online.csus.edu (required)

Recommended

2. H. Carvey, Windows Forensics and Incident Recovery, Addison Wesley, 2005


Prerequisites by Topic:

1. Fundamentals of computer Security
2. Computer Organization

Goals and Expected Learning Outcomes:

At the successful completion of this course students should be able to:
1. Demonstrate the phases of proper forensic procedures: identification, preservation, collection, examination, analysis, and presentation.
2. Utilize computer forensic tools to perform a forensic analysis of a suspected security incident.
3. Demonstrate an understanding of the various laws dealing with computer forensic analysis.
4. Understand the rules of evidence and the importance of the chain of custody.
5. Understand the fundamentals and basic principles of computer forensics and crime scene analysis.
6. Apply the principles and procedures of computer forensics.
7. Understand how to deal with categories of electronic evidence including media, software (e.g., Malware), email, and networks.
8. Study detection and prevention of intrusion and attacks including malware analysis.
10. Use and understand commercial and open-source computer forensics and malware analysis tools.
11. Understand the legal issues involved in computer forensic analysis.

**TENTATIVE GRADING POLICY:**
The following allocation of points is tentative. These may change during the semester.

**CSC 253 Students:**
- Quizzes: 25%
- Final: 25%
- Assignments/Homework: 30%
- Project/Oral-and-Written-Communication: 15%
- Attendance to Oral Presentations: 5%

**CSC 153 Students:**
- Quizzes: 30%
- Final: 25%
- Assignments/Homework: 40%
- Attendance to Oral Presentations: 5%

**Grading Breakdown (%):**
- A = 93-100
- A- = 90-92
- B+ = 87-89
- B = 83-86
- B- = 80-82
- C+ = 77-79
- C = 73-76
- C- = 70-72
- D+ = 67-69
- D = 63-66
- D- = 60-62
- F = 59 or below

You must pass both the assignments/project and the exams in order to obtain a passing grade for the course. Students are required to keep backup (machine-readable) copies of all submitted work, and also to keep all returned (graded) work, until after final grades are posted.

**COURSE POLICIES:**
1. Information in this syllabus is subject to change with notice.
2. Attendance to class and frequent check of email is expected. Class roll will not be checked after first week of classes unless the instructor deems it necessary. However, you are responsible for material presented and announcements made in class or by email. This could include changes to the syllabus, exam dates, etc.
3. Late assignment/project will be penalized by 20% if one lecture late. Nothing will be accepted if more than one lecture late, or if solution has been posted.
4. Make-up exams will only be given under extreme circumstances. The instructor reserves the right to reject make-up requests. There will be no make-up for unannounced quizzes under any circumstances.

5. Be aware of the institution policy on drops and incomplete.

Ethics/Academic Honesty

Any work submitted is a contractual obligation that the work is the student’s and for which he/she could be quizzed in detail. Discussion among students in assignments and projects is part of the educational process and is encouraged. No discussion among students is allowed in any exams/quizzes. However, each student must make an effort to do his/her own work in all assignments and exams. No type of plagiarism will be tolerated except in the case of group work. In that case each student should indicate the part of the work, which was their major responsibility in their final joint submission. Nevertheless, I emphasize any work submitted is a contractual obligation that the work is the student’s and for which he/she could be quizzed in detail. The minimum penalty for even a single incident of cheating brought to the attention of the instructor in this course is automatic failure of the course; additional more severe penalties may also be applied. Note that cheating is grounds for dismissal from the University.

Please refer to the Computer Science Dept. document entitled “Policy on Academic Integrity” (available online via the Computer Science department, www.ecs.csus.edu/csc home page) and to the University Policy Manual section on Academic Honesty (all available online via the instructor’s home page) for additional information. IT IS THE RESPONSIBILITY OF EACH STUDENT TO BE FAMILIAR WITH, AND TO COMPLY WITH, THE POLICIES STATED IN THESE DOCUMENTS. In addition, unless otherwise stated, the use of the following devices during exams/quizzes is prohibited: cell phones, pagers, laptops, and PDAs.

ADVICE on WORKLOAD and CLASS NOTES:

There are a lot of reading assignments. You should endeavor to read the assigned pages before coming to class. There will also be laboratory and homework assignments to be handed in. In addition, you will be required to complete an independent project, which is worth a considerable fraction of your grade for the course.

The class notes are online and should be considered as a guide. Many parts of it are not detailed enough to be self-contained. In addition, experience shows that new material is added every semester. Therefore, attendance to class is necessary in order to understand the details.

INDEPENDENT PROJECT/ORAL AND WRITTEN COMMUNICATION

Independent student projects involving programming (ie. simulation or implementation), or research paper. List of possible projects are provided by the instructor. Students may choose their own topics upon approval of instructor. Joint programming projects are encouraged. Oral and written communication skills are essential for any work environment you find yourself. Therefore, the deliverables for the Projects will include a detailed report and oral PPT presentation (for research papers) or demonstration (programming projects). The final written report should be professional and potentially publishable in a technical magazine/journal such as IEEE Communications, IEEE Network Magazine, etc. The grading will assess your written and oral communication skills. For details of the specific grading criteria see details of Independent Project call for proposals (to be given later in the semester).

COMPUTER ACCOUNTS AND ELECTRONIC COMMUNICATION:

a) gaia account
You must have a UNIX account on the ECS system "gaia" for this class. If you don't have a UNIX account on gaia,
a. Use your favorite Browser and Go to www.ecs.csus.edu
b. Click on Computing Services -> Network Accounts -> Get a new Account.
c. Fill out all required fields

You can also obtain an account by getting one from the College IT staff in room 2011. For both security reasons and convenience all email to me must be sent from the gaia account. The College has a web-based email system on gaia (gaia.ecs.csus.edu/mail) that you can use for email. You must also use your gaia account for subscribing to the class mailing list which is described below.

b) Mailing List
I have established a Mailing List for this course with a web-based maillist interface called Mailman. It is MANDATORY for every student accepted into the course to subscribe to the Mailing List within the first two weeks of classes. The list will be used to facilitate electronic communication for the course. Failure to subscribe to the list in a timely manner could result in your missing important assignments, clarifications, announcements, etc that are sent by email. You must check email on a regular basis and I will assume that you have received and read all messages I send to the list. The instructor will not be held responsible for your failures. To subscribe to the list go to the following website and fill out appropriate forms there. PLEASE FILL IN YOUR NAME ON THE FORM SO I KNOW YOU BELONG IN THIS CLASS.
http://hera.ecs.csus.edu/mailman/listinfo/csc153
http://hera.ecs.csus.edu/mailman/listinfo/csc253

This will add your email address (the one from which you send the message, hopefully gaia) to the csc253 mailing list. Subsequently you can send questions or discussion items regarding topics in csc253 to everyone on the list. To do this, just send an email message to the address “csc253@ecs.csus.edu”. This is a good way to send messages to other students in the class regarding clarifications about assignments, lecture, etc. Note that these email messages are sent to everyone on the csc253 list (including the instructors). If you need to communicate privately with the Instructor, use the instructor’s individual email address as given above. Note: Do not send HTML e-mail to the list. Some mail reader programs do not understand HTML Tags.

To make sure that your gaia account is used for subscription to the mailing list you must send the email from gaia. I will check the list from time to time to determine who is registered. If I notice any email address other than one from gaia, I will delete it. The instructor will not be held responsible if you do not receive messages sent to the list.

c) Assignment/Homework Submission
You must submit all homework/assignments/project reports electronically via WebCT, which can be reached from mySacState (my.csus.edu). I will not accept a hardcopy. Any file which is placed in WebCT will be named according to one of the formats below (depending on the type of assignment). Please do NOT submit PDF files as I will not be able to make comments on them. Word format is preferable.

Your-name_course#_hmwk_hmwk#, your-name_course#_lab_lab#, your-name_course_project_project#
For example if a student named John Doe is submitting homework#1 the file name of the email attachment should be *doe-john_253_hmwk_1*

**Please note:** If the attachment is not according to proper format as stated above, it will not be accepted.

**Legal Policy:**
Every student that enrolls in this course will be required to sign a "Legal Policy" that reads: *Computer and Network Security course mission is to educate, introduce and demonstrate hacking tools and forensic tools for educational purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to invade privacy or compromise any computer system, and to indemnify California State University, Sacramento and College of Engineering and Computer Science with respect to the use or misuse of these tools, regardless of intent.*

**253/153 Tentative Schedule (Subject to Change)**

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Readings</th>
</tr>
</thead>
</table>
| 1    | 1. Class Intro  
     2. Course Intro 
     3. Intro to Computer Forensics 
     4. | • Class Notes  
     • Real Digital Forensics (RDF) Preface, Case Studies  
| 2A   | 1. Digital Forensics and Incident Response Proceses | • NIST SP 800-86  
     • Class Notes |
| 2B   | 2. Disk geometry  
     3. Partitions & Formatting  
     4. The Boot Process  
     5. File Systems | • Class Notes |
| 3A   | 1. Data Acquisition: Imaging - Basic Concepts  
     2. Imaging Methods & Software | • RDF Ch 7, 8  
     • Class Notes |
| 3B   | 1. Media Analysis  
2. Media Analysis Tools  
3. String Searches, Pattern Matching, Regular Expressions  
4. Win Hex  
5. FTK, Encase, Open source tools | • RDF Chapters 9  
• NIJ/IACIS Forensic Procedures  
• NIST Forensic Search String Specification  
• Class Notes |
| 4 (QUIZ #1) | 1. Common Data Hiding Techniques  
2. Advanced Data Hiding Techniques Deleting, Formatting, Encryption, Steganography | • Class Notes  
• RDF Ch 12 |
| 5 | 1. Live Incident Response  
2. Network Forensics | • RDF Ch 1-2 |
| 6A | 1. E-mail Forensics  
2. Web Forensics | • RDF Ch 3-5, 10-11  
• Class Notes |
| 6B | 1. Mobile Forensics  
2. Chat Forensics | • RDF Ch 3-5  
• Class Notes |
| 7 | Reverse Engineering – Malware. Static and Dynamic Analysis. Inspection Tools. PE Header, ELF formats | • Practical Malware Analysis (PMA) Ch 1, 2, and 3.  
• Class Notes |
| 8 | Reverse Engineering Analysis – Disassembler, Decompiler | • PMA Ch 4, 5  
• Class Notes |
| 9 (QUIZ #2) | Reverse Engineering - Debuggers, Code Analysis, control structures, Anti Reverse Engineering techniques, etc | • PMA Ch 6, 7, 14-18  
• Class Notes |
| 10 | 1. Law  
2. Criminal  
3. Civil | • Class Notes |
| 11-12 | 1. Search and Seizure  
2. Search and Seizure Laws  
3. Civil Laws  
4. Sedona Principles  
5. e-Discovery | • Class Notes  
• NIJ Search and Seizure Procedures  
• Sedona Principles Document |
<table>
<thead>
<tr>
<th>Week</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>6. Advanced Topics in Computer Forensics, as time permits: Eg Hardware/Firmware Forensics, Forensics in Embedded systems and Critical Infrastructures (eg. Smart Grid), Distributed Forensics, etc.</td>
</tr>
<tr>
<td>14-15</td>
<td>Project Presentation</td>
</tr>
<tr>
<td>16</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

**IMPORTANT DATES:**
Caesar Chavez Holiday: April 1, 2013
FINAL EXAM: Monday 5/20/13, 515-715pm