New Jersey Institute of Technology (NJIT)
IS682-101: Computer forensics I
Summer; May 23, 2016 - Aug 08, 2016

Instructor:
Dr. Charles Pak
Email: cpak@njit.edu; charlespak@verizon.net
Email is the best way to contact me. Here is my cell number if needed: (443)610-7986

General Course Information
This is a graduate level class. Students are expected to apply time management skills to their work, home, and academic life. Any due dates for materials for these classes are designed to spread the workload over the semester. Material, such as reading assignments, with no due date given should be done as soon as possible by the student so the workload does not become overwhelming prior to the end of class.

Course Description

This course deals with the preservation, identification, extraction, documentation, reporting, acquisition, analysis, interpretation and reconstruction of computer data. Topics covered include evidence handling, chain of custody, collection, preservation, identification and recovery of computer data.

Course Objectives
Upon completion of this course, the student will be able to:

1. Describe the handling process of a forensic analysis of a storage media.
2. Secure the data without contamination or compromising the integrity.
3. Create a bit stream image of the original data.
4. Demonstrate how to acquire evidence while adhering to reasonable practices of Handling, Chain of custody, Collection, Identification, Transportation, Storage, and Documentation of the investigation.
5. Describe and demonstrate how to authenticate forensic evidence.
6. Document the scene using pictures
7. Create an electronic fingerprint of acquired data using hashing techniques
8. Describe how and why it is necessary to create a copy of evidence data: - Forensic backups, Preservation of the original data
9. Describe and demonstrate how to recover data in a forensic evaluation of a hard or floppy disk, including Slack data, Recycle bin, Deleted data, Unallocated data, Swap data
10. Describe the physical and logical disk structure such as Disk volumes, Data area, Cluster size, FAT entries, and Slack
11. Provide written reports for each case image file.

Reading Materials:
Required Text Book:
Marjie T. Britz (2009). COMPUTER FORENSICS AND CYBER CRIME;
ISBN-13: 978-0132677714 ISBN-10: 0132677717; 3rd Edition

Method of Instruction

The method of instruction will combine the following elements:
- Online Class Discussion, Collaboration, Forensic Research Analysis and Report
- Forensic Research Presentation, Project Paper Deliverable

Policy on Paper Submission

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time. Papers MUST be submitted electronically via Blackboard.

All papers must include the following statement:
"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____"

Reading Assignments:

The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. Recommended background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.
Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

Grading Policy:

The overall course grade will be established as follows:

Grading Criteria	Percentage
Forensic Case Study Research Project Paper	30
Forensic Case Study Research Project Presentation Slide Deck	10

Discussion Participation	30
Final exam	30
Total	**100**

Other Items of Importance

Don't ask for an incomplete for convenience. The University has very specific policy on when a grade of incomplete may be awarded. See the Bulletin for more information on grading policies.

Writing and Speaking Standards:

Written communication is an important element of the total communication process. This is a graduate program. **Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.** The University recognizes and expects exemplary writing to be the norm for course work. To this end, all papers, individual and group, must demonstrate graduate level writing and comply with and conform to standard academic format as specified in A Manual For Writers of Term Papers, Theses, and Dissertations by Kate L. Turabian, Seventh Edition. Points will be subtracted for format errors. Points will also be subtracted for spelling and grammatical errors. Use of Standard English ensures that your points will be both understood and correctly interpreted by all readers, a skill that will be vital to your success after graduation.

Effective managers, leaders, and teachers are also effective communicators. It is no understatement to say that effective speaking and writing skills are as important to career success as technical mastery of a subject. Speaking and writing effectively are a critical part of this course. Correct and graduate level Standard English must be used.

***Academic integrity*:**

Academic integrity is central to the learning and teaching process. Students are expected to conduct themselves in a manner that will contribute to the maintenance of academic integrity by making all reasonable efforts to prevent the occurrence of academic dishonesty. Academic dishonesty includes, but is not limited to, obtaining or giving aid on an examination, having unauthorized prior knowledge of an examination, doing work for another student, and plagiarism of all types.

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; paraphrasing ideas, conclusions, or research without citing the source; and using all or part of a literary plot, poem, film, musical score, or other artistic product without attributing the work to its creator. Students can avoid unintentional plagiarism by following carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources.

There is no such thing as "boilerplate" in academia.

If you don't understand what plagiarism is and how to avoid it, consult the University's academic integrity policy. See also http://www.prism-magazine.org/december/html/student_plagiarism_in_an_onlin.htm
This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.

The penalties for plagiarism include a zero or a grade of "F" on the work in question, a grade of "F" in the course, suspension with a file letter, suspension with a transcript notation, or expulsion. Students are not permitted to submit an assignment or paper that already has been submitted for another course at any institution, even if it is entirely their own work. This includes cutting and pasting portions of previous papers or other written assignments. The penalties will be the same as those listed above for plagiarism. Please check your work carefully. Turabian contains complete guidance on how to correctly reference all forms of material.

There is no such thing as "boilerplate" or "standard language" in academia. Students are expected to write their reports themselves. If it is necessary to use material from other sources, it is expected (and mandatory) that the

standards of academic style and integrity will be followed. Every student is encouraged to visit these websites for interesting information regarding this issue:

- A true story about plagiarism gone awry
http://www.aweekofkindness.com/blog/archives/the_laura_k_krishna_saga/000023.html (May only be available in a Google Cache as Domain expired 2/23/2011).
- Goucher College's "Plagiarism-by-Paraphrase Risk Quiz"
http://faculty.goucher.edu/writingprogram/sgarrett/Default.html
- Copyright law, frequently asked questions, and other good stuff
http://www.copyright.gov/
- The Islam Online.net Fatwa on Plagiarism
http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503549102

http://www.ipl.org—home page of the Internet Public Library. Users may search the databases for topics of various interests. The site provides links for viewing and downloading numerous academic articles on the development of technology, the history of computers and the Internet, and the evolution of digital communication.

http://www.isoc.org—The Internet Society (ISOC) is a professional membership society with more than 100 organization and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).

http://www.fcc.gov—The Federal Communications Commission (FCC) is an independent U.S. government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

http://www.netlingo.com—This site contains thousands of definitions about computers, the Internet, and the online world of business, technology, and communication.

Disabled Students: Any student who has a disability and is in need of special consideration must inform the instructor of this need within the first week of class (or immediately if the disability appears after the first week of class) so that appropriate arrangements can be made. This includes students with reading or learning disabilities who may require extra time on tests. In all cases, the student must communicate with the Disability Services Center and have registered the disability with the University.

Forensic Case Study Research Project

The student will conduct a Forensic Case Study Research and produce a forensic report paper for submission in a length of 10-15 pages, double-spaced. The paper must conform to APA; see http://www.apastyle.org/ for a proper APA style. The paper should include a comprehensive evaluation of a Forensic case of a real or potential fictitious case. The paper will be assessed on a case build-up, analysis, arguments, and recommendations on the case. Please do not include any organizational sensitive or confidential data on the paper. The paper should be properly formatted with a cover page, table of contents, content sections, conclusions, and a list of references.

Conference Post

The following table depicts a conference rubric that guides students how to prepare each conference post and how each conference post will be graded by the instructor. Each conference discussion will be graded with its own criteria, and the following rubric depicts the first week discussion forum. Conference rubric for weekly discussion forum, thread, and post participation will be available online.

Course Schedule

Week	Date	Discussion Topic	Assignments
1	5/23	Introduction and overview of computer forensic and cybercrime Computer terminology and history	Read Ch. 1&2 Discussion Post
2	5/30	Traditional Computer Crime: Early Hackers and Theft of Components Contemporary Computer Crime	Read Ch. 3 & 4 Discussion Post
3	6/6	Identify Theft and Identity Fraud Terrorism and Organized Crime	Read Ch. 5 & 6 Discussion Post
4	6/13	Avenues for Prosecution and Government Effort	Read Ch. 7 Discussion Post
5	6/20	Applying the First Amendment To Computer-Related Crime	Read Ch. 8 Discussion Post
6	6/27	The Fourth Amendment and Other Legal Issues	Read Ch. 9 Discussion Post
7	7/4	Computer Forensics: Terminology and Requirements	Read Ch. 10 Discussion Post
8	7/11	Searching and Seizing Computer-Related Evidence	Read Ch. 11 Discussion Post
9	7/18	Processing of Evidence and Effort Preparation	Read Ch. 12 Forensic Case Study Research Project Presentation Slide Deck Due
10	7/25	Conclusions and Future Issues	Read Ch. 13 Forensic Case Study Research Project Paper Due
11	8/1	Final Exam	Final