Computer Forensics I

IS 485-451

IS 682-850

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.

LECTURES: Each class session will consist of a lecture and possible lab exercise.

STUDENTS: Are expected to study the material and complete all exercises. The instructor may assign additional laboratory, exercises or outside assignments as the class progresses. Poor attendance on virtual lectures or participation discussion in the forum will adversely affect the overall grade. Students missing more than ½ of the virtual lecture sessions will be counted absent. Students missing four or more class sessions without instructor approval will have their final letter grade reduced at the discretion of the instructor. Late assignments will be reduced at the discretion of the instructor.

LABS Labs for each module are expected to be completed prior to taking any tests or examinations.

GRADING: Computation of Course Grade:

Forensic analyses & assignments	40%
Midterm Exam	25%
Forum Participation	10%
Final Exam	25%
	100%

MATERIALS NEEDED:

Minimum 256 MB USB Flash Drive

Books:

Corporate Computer Forensics Training System Text Manual Volume I **Price ($60.00)**
By Cyber Defense Training Systems, J. A. Lewis
http://www.lulu.com/product/paperback/corporate-computer-forensics-training-system-text-manual-volume-i/4909983?productTrackingContext=center_search_results

Corporate Computer Forensics Exercise Manual Volume I 4th Edition **Price ($30.00)**
By James Lewis
http://www.lulu.com/product/paperback/corporate-computer-forensics-exercise-manual-volume-i-4th-edition/4952397?productTrackingContext=center_search_results

DISTANT LEARNING COURSE PROCESS:

All Graduate and Undergraduate student will be required to listen to the professor's pre-recorded lecture which will be made available on Mondays. In the lecture, the student will be given instructions on the lab exercises as well as the assignments that will be due that Sunday by 12 noon. The students both Graduate and Undergraduate are required to join the Professor in a 60 minute webinar which will be held on Friday nights from 6:00 pm until 7:00 pm. During the webinar the professor will answer any questions relating to the assignments as well as any text book or forensic type of questions. Your participation is critical during the webinar process and the Professor shall be marking attendance during that time.

COURSE OBJECTIVES:

Students successfully completing this course are expected to be able to:

1. Describe the handling process of a forensic analysis of a hard disk or floppy disk to include:
   - Securing the data without contamination or compromising the integrity
   - Creating a bit stream image of the original data

2. Demonstrate how to acquire evidence while adhering to reasonable practices of:
   - Handling
   - Chain of custody
   - Collection
   - Identification
   - Transportation
   - Storage
   - Documentation of the investigation

3. Describe and demonstrate how to authenticate forensic evidence to include:
   - Documenting the scene using pictures
   - Creating an electronic fingerprint of acquired data using hashing techniques

4. Describe how and why it is necessary to create a copy of evidence data:
   - Forensic backups
   - Preservation of the original data

5. Describe and demonstrate how to recover data in a forensic evaluation of a hard or floppy disk, to include:
   - Slack data
   - Recycle bin
   - Deleted data
   - Unallocated data
   - Swap data

6. Describe the physical and logical disk structure:
   - Disk volumes
   - Data area
   - Cluster size
   - FAT entries
   - Slack

7. Provide written reports for each case image file.

SYLLUBUS

Week #	Topics	Practical Exercises	Assignments Due
1 **May 24**	Module 1: Introduction to Computer and Digital Forensics. Learner Level of Preparation		Assignments 1 – 5 **IS 485/IS 682**
2 **May31** **And** **June 7**	Module 1: Introduction to Computer and Digital Forensics. Module 2: The Role of Computer and Digital Forensics	Forensics Exercises # 1 & 2 **IS 485/IS 682** Forensics Exercises # 3 & 4 **IS 485/IS 682** Forensics Exercises 5 – 6 **IS 485/IS 682**	Assignments 6 & 7 **IS 485/IS 682** Assignments 8 – 10 **IS 682**
3 **June 14**	Module 2: The Role of Computer and Digital Forensics. Module 3: Evidence Handling and Recovery	Forensics Exercises 7 – 8 **IS 682**	Assignments 11 – 14 **IS 682** Assignments 15 – 18 **IS 485/IS 682**
4 **June 21**	Module 4: The One's and Zeros of Disk Technology	Forensics Exercises 9 – 14 **IS 485/IS 682**	Assignments 19 – 21 **IS 485/IS 682**
5 **June 28**	Module 5: Forensics, The Command Line and Certifications. Module 6: Acquisition, Analysis and Examination of Storage Media Devices	Forensics Exercises 15 & 16 **IS 485/IS 682** Forensics Exercises 17 -19 **IS 485/IS 682**	Assignment 22 **IS 485/IS 682**
6 **July 5**	Module 6: Acquisition, Analysis and Examination of Storage Media Devices **Mid Term**	Forensics Exercises 21 – 25 **IS 485/IS 682**	
7 **July 12**	Module 6: Acquisition, Analysis and Examination of Storage Media Devices Module 7: Forensic Reporting	Forensics Exercises 26 -31 **IS 682** Forensic Exercises 32 – 34 **IS 485/IS 682**	Assignment 23 **IS 485/IS 682**
8 **July 19**	Module 7: Forensic Reporting	Forensics Exercises 35 – 42 **IS 682**	Assignment 24 **IS 485/IS 682**
9 **July 26**	Module 8: Case Analysis and Reporting	Forensics Exercises 43 – 46 **IS 485/IS 682**	
10 **August 2**	Module 8: Case Analysis and Reporting	Forensics Exercises 47 – 51 **IS 682**	
11 **August 9**	**Final examination**		Lab exercise 43 **IS 485/IS 682**