SYLLABUS
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY
PREFIX IT-6853: COMPUTER FORENSICS
SPRING 2021

Course Information

Class meeting time: *Online*
Modality and Location: *Online 100%*
Syllabus is posted in D2L

Instructor

Name: Dr. Maria Valero
E-mail: mvalero2@kennesaw.edu
Office Location: Atrium J-312
Office Phone: (470) 578-7638
Office Hours: Wed 4:00pm – 5:30 pm (In office) or by appointment
Thus 4:00pm – 5:00 pm (online) or by appointment
Course Communication:

- Email is the best way to reach the instructor. Please email me directly from your KSU email address. (e.g. yourlogin@students.kennesaw.edu)
- Use D2L Discussion Forums and D2L Chat to interact with your classmates
- Students' emails will be replied WITHIN 24 hours during the weekday. Weekend and holidays don't apply.
- When email the instructor using accounts other than D2L email, put the course number in the subject line. Emails without proper subject line will not be replied.
- Avoid using personal email. Sensitive information (such as your grades) can ONLY be sent to D2L email or KSU email account.

Course Description

Prerequisites/Corequisites: --
Credit Hours: 3
Required Texts: None. The following books are optional
Optional Texts*:*

- Guide to Computer Forensics and Investigations (6th Edition)
  By Bill Nelson, Amelia Phillips, Christopher Steuart.
  Cengage, Copyright 2018, ISBN-13: 978-1337568944, ISBN-10: 1337568945
- Digital Forensics with Open-Source Tools

By Cory Altheide and Harlan Carvery
Elsevier, Copyright 2011, ISBN 978-1-59749-586-8

Course Description:
This course studies techniques and tools in computing investigation, digital evidence collection, recovery, and analysis. Topics include understanding the computer forensics profession; understanding different OS file systems; image recovery; network forensics; investigating logs and network traffic, recovery of passwords. The course will provide hands-on experience labs conducting a variety of forensics practices. These skills can help prepare trainees for a variety of IT positions, including: Computer Forensic Analyst, Digital Forensic Examiner, Digital Forensics Incident Response and Security Administrator.

Technology Requirements:

- This class uses D2L as hosting site. Run a system check to ensure your computer work with D2L. Check out UITS D2L training: http://uits.kennesaw.edu/support/d2ltraining.php .
- Internet Connection. A high-speed Internet connection such as DSL or cable Internet access is highly recommended. You may also use computer labs on campus to complete the coursework.
- This class uses NetLab provided by KSU to do the labs. Please check D2L for further instructions.
- A web camera is required for a student to take final exam.

Student Learning Outcomes

By the end of this course, a student should be able to:
- Describe the role of computer forensics professionals.
- Analyze hard disks and File System in Window and Linux OS.
- Perform data carving and steganography.
- Evaluate digital forensics tools for web browser, network, and email forensics.
- Recover passwords, analyze log data files, and create professional forensic reports

Course Requirements and Assignment

The requirements of this course are listed as follows.
Labs: There are nine (9) hands-on labs in this course named from “A” to “I”. Lab A is an introductory lab about useful Linux commands for forensics. Lab B is about Windows File Systems forensics. Lab C is about Linux File System forensics. Lab D is about data acquisition. Lab E is about Network forensics. Lab F is about automatic forensic analysis. Lab G is about data carving and stenography. Lab H is regarding mobile forensics. Lab I is about recovering passwords and log analysis. Each lab is related with a lab number in NetLab (See course schedule). For example, Lab A is Lab 6 in NetLab; Lab B is Lab 1 in Netlab, and so on.
Quizzes: There are three (3) quizzes which mainly contain multiple choice and short answer questions related to the content of corresponding learning modules.
Exams: There are two exams: midterm and final. Midterm exam is multiple choice and short answer questions. Final exam is composed of a list of short-answer or problem-solving questions.
Research Paper: This is an individual student work to conduct and in-depth research on a focus area of computer forensics. Student must select a topic a get approval from the instructor. An initial abstract is graded. Student may submit an initial draft for instructor feedback. Final submission of the paper will be graded.

Evaluation and Grading Policies

Weight Distribution

Grading Item	Weight
Labs (9)	45%
Quizzes (3)	15%
Research Paper	15%
Midterm Exam	10%
Final Exam	15%
Total	**100%**

Grading Scale:
90% - 100% A
80% - 89% B
70% - 79% C
60% - 69% D
0% - 59% F

Grades will be rounded up if they are > or = .5 or above, for example, an 89.6 is an A, but 79.2 is a C.

Course Policies

Course Attendance Policy

- For online section, students' attendance is also measured by how often a student login in D2L course website, participation of online discussion, as well as on-time completion of homework.

Grading Items Turnaround Time

- The grades for the quizzes and exams will be available 48 business hours after the due date
- The grades for labs/assignments/projects will be available 96 business hours after the due date

Assignments & Exam Policy

- All assignments **MUST** be submitted through D2L (https://kennesaw.view.usg.edu/) course website by the deadline specified in course calendar. Email submission will **NOT** be accepted. Any assignment that is less or equal than 24 hours late is subject to 10% penalty. Any assignment that is less or equal than 48 hours late is subject to 20% penalty. Any assignment that is more than 48 hours late will **NOT** be accepted.
- All quizzes and exams MUST be completed on D2L website by the deadline specified in course calendar. The quizzes exams can't be opened/submitted after the deadline.
- If you must miss an exam due to illness, you must e-mail or call the instructor before the scheduled time. Failure to notify the instructor prior to the scheduled time will produce an automatic zero for the exam. NO makeup test except for emergencies with proof (e.g. doctor's slip).

Midterm and Final Exam

Respondus Lockdown Browser + a Webcam will be used for the final exam. LockedDown Web Browser Student Guide
https://apps.kennesaw.edu/files/pr_app_uni_cdoc/doc/Respondus-LockDown-Browser_StudentGuide.pdf
Please contact the instructor if you have any questions.

Student Responsibility
For this class, you are expected to spend seven to eight hours each week on coursework:

- Check KSU email regularly;
- Login D2L course website frequently to access the course material (at least every other day);
- Follow the weekly study guide in the learning module;
- Study the assigned material such as virtual lectures, textbook chapters and the PowerPoint slides;
- Complete assigned quiz/assignment/discussion/project on time.
- On every Monday, you will be provided with the following materials:
    - An overview of our contents, materials, and goals for this week (this is where you start from: all homework, quizzes, assignments will also be announced in this study guide).
    - Assigned reading from textbooks and/or provided material.
    - PowerPoint slides.
    - Homework assignments, or lab, or quiz.
    - A brief video lecture to walk you through the PPT slides.
- During each week, you should:
    - Read the assigned sections of the textbook and/or provided materials.
    - Digest the PowerPoint slides.
    - Take online quiz if assigned.
    - Finish homework assignments and submit it on time.

Tips for Effective Online Learning
For an online class, students can really enjoy the benefits of learning at you own pace and at the place of your choice. Below are some tips for effective online learning.

- *Check D2L course website frequently*. It's recommended that students should login D2L course site **AT LEAST** every other day. Always be aware of current status of the course. Take advantage of the posted learning material such as recorded lectures.
- *Work with the instructor closely*. If you have any question, contact the instructor immediately. You can either email or text me and your message is guaranteed to be replied within 12 hours.
- *Start your work early*. If you can start a task early, don't start late. Assuming you spend the same amount of time completing the task, starting later will be much more stressful than starting early. Never start until the last minute! You'll have no turnaround time if you need help or something happens.
- *Keep up with the work*. Don't fall behind. If you do, contact the instructor immediately for what you need to do. The instructor may also contact you if he is concerned. Respond to the instructor's inquiry promptly.

Class Communication Rules
In any classroom setting there are communication rules in place that encourage students to respect others and their opinions. In an online environment, the do's and don'ts of online communication are referred to as **Netiquette**. As a student in my course you should:

- Be sensitive and reflective to what others are saying.

- **Avoid typing in all capitals** because it is difficult to read and is considered the electronic version of 'shouting'.
- Don't flame - These are outbursts of extreme emotion or opinion.
- Think before you hit the post (enter/reply) button. You can't take it back! Don't use offensive language.
- Use clear subject lines.
- Don't use abbreviations or acronyms unless the entire class knows them. Be forgiving. Anyone can make a mistake.
- Keep the dialog collegial and professional, humor is difficult to convey in an online environment.
- Always **assume good intent** and **respond accordingly**. If you are unsure of or annoyed by a message, wait 24 hours before responding.

Course Schedule

The course schedule is tentative and is subject to change. Please use D2L course calendar as accurate due dates.

Week	Date	Course Contents	Assignments
01	01/11 – 01/17	Mod 1: Introduction to Computer Forensics	Introduce yourself nongraded-quiz Lab A (Lab 6 NETLAB)
02	01/18 – 01/24	Mod 2: Windows File Systems and Artifacts	Lab B (Lab 1 NETLAB)
03	01/25 – 01/31	Mod 3: Linux File Systems and Artifacts	Lab C (Lab 2 NETLAB)
04	02/01 – 02/07	Mod 4: Introduction to Partitions	Quiz #1
05	02/08 – 02/14	Mod 5: Data Acquisition	Lab D (Lab 4 NETLAB)
06	02/15 – 02/21	Mod 6: Registry Forensics	Research topic selection Quiz #2
07	02/22 – 02/28	Mod 7: Web Browser Forensics	MIDTERM
08	03/01 – 03/07	Mod 8: Network Forensics	Lab E (Lab 10 NETLAB)
09	03/08 – 03/14	Spring Break	
10	03/15 – 03/21	Mod 9: Automatic Forensic Analysis	Lab F (Lab 11 & 12 NETLAB)
11	03/22 – 03/28	Mod 10: Data Carving & Steganography	Lab G (Lab 15 NETLAB)
12	03/29 – 04/04	Mod 11: Email Forensics	Quiz #3
13	04/05 – 04/11	Mod 12: Mobile Forensics	Lab H (Lab 16 & 17 NETLAB)
14	04/12 – 04/18	Mod 13: Recovering passwords Mod 14: Log Analysis	Lab I (Lab 18 & 19 NETLAB)
15	04/19 – 04/25	Mod 15: Cloud Forensics	Draft of research paper
16	04/26 – 05/02	Review	Research paper due
17	05/03 – 05/09	12/7 – Last Day of Class Final Exam - TBD	Final Exam

Important dates:

- Add/Drop ends: Jan 15 11:45pm
- Last Day to Withdraw Without Academic Penalty: Mar 15 11:45 p.m.
- Last Day to Withdraw for the Term With a WF: Apr 26.
- Last Day of Class: May 3.

Institutional Policies

- Federal, BOR, & KSU Course Syllabus Policies
- Academic Integrity Statement
    - Examples of violation of academic integrity: 1) copy from others or from Internet; 2) allow others to copy your work; 3) use other's help or help other in completing the quizzes or exams.
    - The first violation of academic integrity, the student will immediately receive 0 for the associated grading item. For the 2nd violation, the student will receive a fail grade for this course.

KSU Statements on COVID-19

Face Masks in The Classroom
As mandated by the University System of Georgia, the university requires the use of face masks in the classroom and in KSU buildings to protect you, your classmates, and instructors. Per the University System of Georgia, anyone not using a face covering when required will be asked to wear one or must leave the area. Repeated refusal to comply with the requirement may result in discipline through the applicable conduct code.

Reasonable accommodations may be made for those who are unable to wear a face covering for documented health reasons. Please contact Student Disability Services at sds@kennesaw.edu for student accommodation requests.

Shifting Modalities
Please note that the university reserves the right to shift teaching modalities at any time during the semester, if health and safety guidelines require it to do so. Some teaching modalities that may be used are F2F, Hyflex, Hybrid, or online, both synchronous and asynchronous instruction.

Staying Home When Sick
If you are ill, please stay home and contact your health professional. In that case, please email the instructor to say you are missing class due to illness. Signs of illness include, but are not limited to, the following:

- Cough
- Fever of 100.4 or higher
- Runny nose or new sinus congestion
- Shortness of breath or difficulty breathing
- Chills
- Sore Throat
- New loss of taste and/or smell

Seating Plans
Students will sit in the same seat for every F2F class so that the instructor can use a seating plan for contact tracing if a student contracts Covid-19.

Student Resources

This link contains information on help and resources available to students: KSU Student Resources for Course Syllabus