**CMPS 355 Cyber Forensics**

**Credit: 3 hours**

**Catalog Description:** This course will cover the introduction to the various aspects in the field of Internet/cyber forensics such as the rules and integrity of evidence, legal processes, factual reporting of the information found, and providing expert opinion in a court of law or other legal administrative proceeding and contemporary methods in the preservation, identification, extraction, interpretation, presentation, and documentation of computer evidence.

**Instructor:** Dr. Mohammad Abdus Salam, Department of Computer Science, Henry Thurman Hall, Room E107, and Phone: (225) 771-4383, Email: md.salam@sus.edu.

**Office Hours:** MW: 9:00 am ~ 10:00 am, T: 9:00 am ~ 1:00 pm and by special appointment.

**Course Objectives and Learning Outcomes:**

Upon completion of the course, students will be able to understand the most popular forensics tools and provides specific guidance on dealing with civil and criminal matters relating to the law and technology. Students will be able to manage a digital forensics operation in today’s business environment.

**Textbook:** Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, Sixth Edition. Cengage Learning, 2018, ISBN-13: 978-1-337-56894-4.

**Topic Covered:**

Understanding the Digital Forensics Profession and Investigations

The Investigator’s Office and Laboratory

Data Acquisition

Processing Crime and Incident Scenes

Working with Windows and CLI Systems

Current Digital Forensics Tools

Linux and Macintosh File Systems

Recovering Graphics Files

Digital Forensics Analysis and Validation

Virtual Machine Forensics, Live Acquisitions, and Network Forensics

Email and Social Media

Mobile Device Forensics

Cloud Forensics

Report Writing for High Tech Investigations

Expert Testimony in High Tech Investigations

Ethics for the Investigator and Expert Witness.

|  |  |  |  |
| --- | --- | --- | --- |
| Tentative Schedule | | | |
| Week | Topics | Chapter  Readings | Exams |
| 1 | Understanding the Digital Forensics Profession and Investigations | Chapter 1 |  |
| 2 | The Investigator’s Office and Laboratory | Chapter 2 |  |
| 3 | Data Acquisition | Chapter 3 |  |
| 4 | Processing Crime and Incident Scenes | Chapter 4 |  |
| 5 | Working with Windows and CLI Systems | Chapter 5 |  |
| 6 | Current Digital Forensics Tools | Chapter 6 |  |
| 7 | Linux and Macintosh File Systems | Chapter 7 | Midterm Exam |
| 8 | Recovering Graphics Files | Chapter 8 |  |
| 9 | Digital Forensics Analysis and Validation | Chapter 9 |  |
| 10 | Virtual Machine Forensics, Live Acquisitions, and Network Forensics | Chapter 10 |  |
| 11 | Email and Social Media  Mobil Device Forensics | Chapter 11  Chapter 12 |  |
| 12 | Cloud Forensics | Chapter 13 |  |
| 13 | Report Writing for High Tech Investigations Expert Testimony in High Tech Investigations | Chapter 14 Chapter 15 |  |
| 14 | Ethics for the Investigator and Expert Witness | Chapter 16 | Final Exam |

**Prerequisite:** None.

**Classroom:** Henry Thurman Jr. Hall, Room 204 (HYBRID).

**Meeting time:** Monday, Wednesday, and Friday: 10:00 am to 10:50 pm.

**Evaluation and Grading:** Standard grading scale will be followed. Following is a tentative distribution of various components of the course:

|  |  |  |  |
| --- | --- | --- | --- |
| Points Distribution | | Grading | Midterm Grading:  10% Homework  10% Quizzes  80% Mid-term |
| Mid-term | 25% | A: 90-100% |
| Quizzes | 25% | B: 80-89% |
| Homework | 10% | C: 70-79% |
| Project and Presentation | 10% | D: 65-69% |
| Final Exam | 30% | F: below 65% |
| Total | 100% |  |

**Mid-term and final examination:**

There will be mid-term examination and final examination. It is mandatory that you take the mid-term and final. Make-up tests will be given in extenuating circumstances only. All tests and examinations missed due to illness or emergency require a written, verified excuse or a grade of zero will be assigned.

**Presentation and Report:**

Each student is required to select a particular research topic and study in-depth of that area. Each student need to make at least one oral presentation of typically 10 minutes duration and to submit a written report of about 5~7 pages long about his/her research topic. All research topics must be approved by the instructor. Each student must submit a brief project title that outlines project objectives. You are encouraged to discuss research topics with the instructor and to submit your research topics as early as possible.

**Quizzes:** Quizzes will be given in class at the discretion of the instructor. No make-up quizzes will be given. At any time without any advance notice, pop-up quiz should be expected.

**Homework:** Homework will be assigned and collected. Late assignments will not be accepted. Selected assignments will be graded. Other assignments will be returned with general comments. The intent of assigning and collecting homework is to evaluate the progress of the students in mastering the concepts presented. Use regular-size paper, staple the sheets together, and put your name, date of homework, homework number on the cover page.

**Attendance:** Students are responsible for all information covered in class. Attendance is strongly recommended, and 5% bonus will be assigned for attendance and class performance. Moodle will be used for attendance.

**Plagiarism:** Plagiarism in any course work (homework, quizzes, projects, exam, etc.) will not be tolerated. A course grade of "F" will automatically be assigned to anyone who cheats on assignments or examinations.

**Cellular Phones and Portable Electronic Devices:** Please use common courtesy when bringing cellular phones and other portable electronic devices into class. They should be set to a non-audible signaling mode. If it is absolutely necessary to answer a cellular phone or beeper call, please discretely exit the classroom and do so. Please use common sense as to what constitutes an absolute necessity. No electronic devices such as cellular phones, laptop computers are allowed without the permission of the instructor during test.

**Changes in Course Requirements**: Since all classes do not progress at the same rate, the instructor may wish to modify the above-mentioned requirements or their timing as circumstances dictate. For example, the instructor may wish to change the number and frequency of examinations, or the number and sequence of assignments. If such modification is needed, the student will be notified.

**Disability Statements:** Students with documented disabilities who believe that they may need accommodations in this class are encouraged to contact the Disability Services Coordinator in the Office of Disability Services, 246 A.C. Blanks Hall, 225-771-3546 (Voice), 225-771-3949 (Fax), as soon as possible to ensure that such accommodations are implemented in a timely fashion. Students who need accommodations must be registered with the Office of Disability Services. Students are responsible for informing the instructor of any instructional accommodations and/or special learning needs at the beginning of the semester. All discussions will remain confidential.