Syllabus
CSCI 597– Digital Forensics
Texas A&M University Commerce
Spring 2018

Instructor: Dr. Omar El Ariss
Office Location: JOUR 238
Email: Omar.El.Ariss@tamuc.edu
Phone: 903-886-5403
Office Hours:

Day	Time
Tuesday	2:30 pm - 5:30 pm
Thursday	1:00 pm - 4:00 pm
By appointment	

There are many ways to reach me. There is no substitute for face-to-face communication which often leads to more refined and focused questions resulting in your improved understanding. I strongly encourage you to take advantage of my office hours. Questions during class or immediately after class are always welcomed. Email is an easy way to ask questions outside of class but is not productive as face-to-face communication.

Meeting Time and Place

Tuesday, 11:00 am to 2:10 pm, JOUR 204

Recommended Textbooks

- *File System Forensic Analysis*, by Brian Carrier, Addison-Wesley, ISBN 0321268172, *2005*.
- *Handbook of Digital Forensics and Investigation*, by Eoghan Casey, Academic Press, ISBN 0123742676, 2009.

Course Objectives

This course presents an overview of the principles and practices of digital investigation. The objective of this class is to emphasize the fundamentals and importance of digital forensics. Students will learn different techniques and procedures that enable them to perform a digital investigation. This course focuses mainly on the analysis of physical storage media and volume analysis. It covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in hard disks and random access memory.

The objective of this class is to emphasize the importance of digital forensics, and to prepare students to conduct a digital investigation in an organized and systematic way. This course will provide theoretical and practical knowledge, as well as current research on Digital Forensics. Upon completion of the course, students can apply open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.

Topics:

Topics to be covered (as time permits):

- Overview of digital investigation and digital evidence
- Data Acquisition of physical storage devices
- Study of file systems with a main focus on Microsoft Windows & Linux Systems
- File System Analysis & file recovery
- File carving & document analysis
- Information hiding & steganography
- Time, registry & password recovery
- Email & database forensics
- Memory acquisition

Course Outcomes

Upon completion of this course:

- Students will explain and properly document the process of digital forensics analysis.
- Students will gain an understanding of the tradeoffs and differences between various forensic tools.
- Students will be able to describe the representation and organization of data and metadata within modern computer systems.
- Students will understand the inner workings of file systems.
- Students will be able to create disk images, recover deleted files and extract hidden information.
- Students will be introduced to the current research in computer forensics. This will encourage them to define research problems and develop effective solutions.

Homework Assignments & Project

There will be a number of written assignments and programming assignments. Homework assignments must be done individually. A research project will be assigned, two students can work on the project.

Grading

- Homework: 30% of grade
- Research Project: 20% of grade
- Midterm Exam: 20% of grade
- Final Exam: 30% of grade

Letter grades will be determined using a standard percentage of points scale:

Letter Grade	Cut-off Score
A	90%
A-	88%
B+	85%
B	80%

B-	78%
C+	75%
C	70%
D	60%
F	Below 60%

Class attendance, doing all your project and homework will help the borderline cases. Check your grades often. Any score may be disputed up to seven (7) days after the score is posted. After 7 days the score remains as-is.

Methods of Instruction

This syllabus contains an overview of what will be covered in class; for specific information, students are referred to the class web page maintained on eCollege course management system. Information on eCollege will be updated frequently so it is a good idea to check it regularly. Assignments are posted on eCollege and should be submitted through eCollege. Class attendance, doing all your project and homework will help the borderline cases. Check your grades often. Any score may be disputed up to seven (7) days after the score is posted. After 7 days the score remains as-is.

Attendance

You are expected to attend every class. If you must miss a class, it is your responsibility to make up for the work that you missed. If you are going to be absent from class please notify the instructor in advance.

Late Submissions Policy

All work submitted electronically must be submitted by midnight of the due date. Late work will be deducted 10% for each day past the due date. Assignment will not be accepted after three days from the due date.

Tentative Course Outline

Week	Content
1	Introduction
2	Computer Foundations
3	Computer Foundations & Data Acquisition
4	Data Acquisition
5	Volume Analysis
6	Spring Break
7	Midterm Exam
8-10	Volume Analysis & File System Analysis
11, 12	Steganography & Document Analysis
13	Time, registry & email forensics
14	Final Exam

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook. http://www.tamuc.edu/admissions/registrar/documents/studentGuidebook.pdf
Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum: Netiquette http://www.albion.com/netiquette/corerules.html

Academic Honesty

"All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (See Student's Guide Handbook, Policies and Procedures, Conduct). It is the policy of the University, that no form of plagiarism or cheating will be tolerated. Plagiarism is defined as the deliberate use of another's work and claiming it as one's own. This means ideas as well as

text or code, whether paraphrased or presented verbatim (word-for-word). Cheating is defined as obtaining unauthorized assistance on any assignment. Proper citation of sources must always be utilized thoroughly and accurately. If you are caught sharing or using other people's work in this class, you will receive a 0 grade and a warning on the first instance. A subsequent instance will result in receiving an F grade for the course, and possible disciplinary proceedings. If you are unclear about what constitutes academic dishonesty, ask.

Special Needs

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services
Texas A&M University-Commerce
Gee Library- Room 132
Phone (903) 886-5150 or (903) 886-5835
Fax (903) 468-8148
Email: Rebecca.Tuerk@tamuc.edu
Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

Texas A&M University-Commerce will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

Campus Concealed Carry Statement

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in Texas A&M University-Commerce buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and A&M-Commerce Rule 34.06.02.R1, license holders may not carry a concealed handgun in restricted locations.

For a list of locations, please refer to the Carrying Concealed Handguns On Campus document and/or consult your event organizer.

Web url:
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployees AndStudents/34.06.02.R1.pdf

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all A&M-Commerce campuses. Report violations to the University Police Department at 903-886-5868 or 9-1-1.