BUSA 539: Cyber Forensics & Security

FALL 2023

Instructor: DR. ZAKI MALIK
Office Location: Dallas Location – Floor 20
Office Hours: By appointment or Thursday 8.30AM – 12PM
University Email Address: zaki.malik@tamuc.edu

Please use emails to ask me questions, and use BUSA-539 in the subject line of the email. This is the fastest way to reach me.

COURSE INFORMATION

Textbook & Labs

- Chuck Easttom. Digital Forensics, Investigation, and Response, Fourth Edition, Burlington, MA: Jones & Bartlett, 2022 (ISBN 9781284226065)
- You also need the Jones & Bartlett Cloud Labs Access. The textbook and labs package is around $125-$130. Check D2L for discounts before buying the bundle.

Course Description

This course offers an introduction to digital forensics, investigation, and response. Areas of study include procedures for investigating computer and cybercrime, and concepts for collecting, analyzing, recovering, and preserving forensic evidence.

Major Instructional Areas

1. Digital forensic investigations
2. Forensic environments and tools
3. Evidence collection and handling
4. Forensic reporting
5. Solving business challenges with forensic investigations

Student Learning Outcomes

Students learning topics include:

1. Summarize the basic principles of computer forensics.
2. Summarize important laws regarding computer forensics.
3. Describe various computer crimes and how they are investigated.
4. Describe digital forensic methodologies and evidence handling techniques.
5. Outline the proper approach to collecting, seizing, and protecting evidence.
6. Explain techniques for hiding and scrambling information as well as how data is recovered.
7. Summarize various types of digital forensics.
8. Describe contingency planning and incident response.
9. Explain how to perform network packet analysis.
10. Identify technical and legal trends in digital forensics.

COURSE REQUIREMENTS

Minimal Technical Skills Needed

- Be able to take screenshots and use MS. Word and PowerPoint, using presentation and graphics programs, etc.
- Be able to follow instructions in installing the required software.
- Be able to troubleshoot software problems (e.g., by consulting online sources using Google etc).

GRADING

Final grades in this course will be based on the following scale:

A = 90%-100%
B = 80%-89%
C = 70%-79%
D = 60%-69%
F = 59% or Below

Assessments

- **Project:** The project is divided in 4 parts, for a total of 20 points.

- **Quizzes**: 8 Quizzes covering the chapter texts covered in that week (one or two each week) will be given during the semester. You can get a maximum of 40 points for these.
- **Labs**: A total of 10 labs will provide hands-on experience for the materials covered in the text. You can get a maximum of 30 points for these.

- **Labs' Quizzes**: A total of 10 lab quizzes, that related to each lab will be given during the semester. You can get a maximum of 10 points for these.

Student Responsibilities/Tips for Success in the Course

1. Students are expected to:
    a. Read the text related to the topic listed for each week on D2L.
    b. Complete all required assignments as scheduled
    c. Watch any tutorial/recorded videos as posted
    d. Read the slides for each week/topic

2. This syllabus is tentative for the semester. Certain topics maybe stressed more, or less than indicated in the schedule. Depending on the class progress, certain topics may be omitted or added.

3. Behavior: "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 Book). During your collaboration with me and your fellow students online or in class, professionalism and respect will be expected.

4. Any form of cheating – copying, sharing files, submitting the work of another as your own – is not permitted. Students who participate (as givers/receivers) in any form of cheating will fail the course.

TECHNOLOGY REQUIREMENTS

The following information is provided to assist you in successfully using technology to complete the assignments and class activities:

- The course may require you to download and install open-source software. Specifically, you may be asked to install Virtual Machines. It is the student's responsibility to follow the given instructions and get the system ready in due time. You cannot come to the instructor only a few days before the assignment is due and say that you have NOT installed the required software. You WILL HAVE ample time for all tasks !

The *syllabus/schedule are subject to change.*

- To fully participate in online courses you will need to use a current Flash enabled internet browser.
- You will need regular access to a computer with a broadband Internet connection. The minimum computer requirements are:
    - 512 MB of RAM, 1 GB or more preferred o Broadband connection required courses are heavily video intensive o Video display capable of high-color 16-bit display 1024 x 768 or higher resolution
- You must have a:
    - Sound card, which is usually integrated into your desktop or laptop computer
    - Speakers or headphones.
    - *For courses utilizing video-conferencing tools and/or an online proctoring solution, a webcam and microphone are required.
- At a minimum, you must have Microsoft Office 2013, 2010, 2007 or Open Office. Microsoft Office is the standard office productivity software utilized by faculty, students, and staff. Microsoft Word is the standard word processing software, Microsoft Excel is the standard spreadsheet software, and Microsoft PowerPoint is the standard presentation software. Copying and pasting, along with attaching/uploading documents for assignment submission, will also be required. If you do not have Microsoft Office, you can check with the bookstore to see if they have any student copies.
- For additional information about system requirements, please see: https://secure.D2L.com/tamuc/index.learn?action=technical

LMS

All course sections offered by Texas A&M University-Commerce have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

LMS Requirements:
https://community.brightspace.com/s/article/Brightspace-Platform-Requirements

LMS Browser Support:
https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

YouSeeU Virtual Classroom Requirements:
https://support.youseeu.com/hc/en-us/articles/115007031107-Basic-System-Requirements

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu**.**

Note: Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student needs to have a backup method to deal with these inevitable problems. These methods might include the availability of a backup PC at home or work, the temporary use of a computer at a friend's home, the local library, office service companies, Starbucks, a TAMUC campus open computer lab, etc.

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:

https://community.brightspace.com/support/s/contactsupport

COMMUNICATION AND SUPPORT

- If you ask me questions by emails, I will reply within 48 hours. However, I usually answer them much faster than this.
- If you have questions about software operations, please be sure to include the screenshots of the questions in the emails.
- All assignment due dates, project deadlines, and exam time are central time in the United States.

COURSE AND UNIVERSITY POLICIES

COVID-19 Related

A&M-Commerce recommends the use of face-coverings in all instructional and research classrooms/laboratories. Students should not attend class when ill or after exposure to anyone with a communicable illness. Communicate such instances directly with your instructor. Faculty will work to support the student getting access to missed content or completing missed assignments.

Course Specific Procedures/Policies

The class schedule will be provided and updated in D2L. A tentative topics list with each week is listed at the end of this document. Each assignment will be listed with its due date. Since assignments make up the majority of your grade, you should make every effort to complete them on time. Late assignments are **highly** discouraged. For each day an assignment is late it will be deducted 20%. Under **NO** circumstances will I accept an assignment more than THREE DAYS late. Exceptions for sickness and accidents can be made – please consult.

Syllabus Change Policy

The syllabus is a guide. Circumstances and events, such as student progress, may make it necessary for the instructor to modify the syllabus during the semester. Any changes made to the syllabus will be announced in advance.

University Specific Procedures

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

TAMUC Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01.
http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf

Academic Integrity

Students at Texas A&M University-Commerce are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

Undergraduate Academic Dishonesty 13.99.99.R0.03

The *syllabus/schedule are subject to change.*

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf

Graduate Student Academic Dishonesty 13.99.99.R0.10

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/graduate/13.99.99.R0.10GraduateStudentAcademicDishonesty.pdf

ADA Statement

Students with Disabilities

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
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.

The *syllabus/schedule are subject to change.*

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployeesAndStudents/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.

COURSE CALENDAR (Tentative)

Grading Category	Activity Title	Quiz	Lab
Week 1: Introduction to Forensics and Computer Crime			
Required Readings	Chapter 1: Introduction to Forensics Chapter 2: Overview of Computer Crime	Quiz 1	
Week 2: Forensic Methods and Evidence Handling			
Required Readings	Chapter 3: Forensic Methods and Labs Chapter 4: Collecting, Seizing, and Protecting Evidence	Quiz 2	
Lab	Applying the Daubert Standard to Forensic Evidence	L. Quiz 1	Lab 1
Project	**Project Part 1**: Preparing for a Digital Forensic Investigation		
Week 3: Steganography and Data Recovery			
Required Readings	Chapter 5: Understanding Techniques for Hiding and Scrambling Information Chapter 6: Recovering Data	Quiz 3	
Lab	Recognizing the Use of Steganography in Image and Audio Files	L. Quiz 2	Lab 2
Lab	Recovering Deleted and Damaged Files	L. Quiz 3	Lab 3
Week 4: Incident Response and Windows Forensics			
Required Readings	Chapter 7: Incident Response Chapter 8: Windows Forensics	Quiz 4	
Lab	Conducting an Incident Response Investigation	L. Quiz 4	Lab 4
Lab	Conducting Forensic Investigations on Windows Systems	L. Quiz 5	Lab 5
Project	**Project Part 2**: Researching Forensic Best Practices and Creating Procedures		
Week 5: Linux and Mac OS Forensics			
Required Readings	Chapter 9: Linux Forensics Chapter 10: Mac OS Forensics	Quiz 5	
Lab	Conducting Forensic Investigations on Linux Systems	L. Quiz 6	Lab 6
Week 6: Email Forensics and Mobile Forensics			
Required Readings	Chapter 11: Email Forensics Chapter 12: Mobile Forensics	Quiz 6	
Lab	Conducting Forensic Investigations on Email and Chat Logs	L. Quiz 7	Lab 7
Lab	Conducting Forensic Investigations on Mobile Devices	L. Quiz 8	Lab 8

The *syllabus/schedule are subject to change.*

Grading Category	Activity Title	Quiz	Lab
Project	**Project Part 3**: Obtaining Evidence from an ISP		
Week 7: Network Forensics			
Required Readings	Chapter 13: Network Forensics	Quiz 7	
Lab	Conducting Forensic Investigations on Network Infrastructure	L. Quiz 9	Lab 9
Project	**Project Part 4**: Outlining Incident Response and Root Cause Analysis		
Week 8: Memory Forensics and Future Trends			
Required Readings	Chapter 14: Memory Forensics Chapter 15: Trends and Future Directions	Quiz 8	
Lab	Conducting Forensic Investigations on System Memory	L. Quiz 10	Lab 10

This is only a tentative class schedule. Updates will be communicated and maintained in D2L

The *syllabus/schedule are subject to change.*