Introduction to Computer Forensics

Texas A&M University - Central Texas

CIS 3361-110 , 10374 Intro to Computer Forensics

INSTRUCTOR AND CONTACT INFORMATION

Instructor: Dr. Deepti Gupta

Classroom Location: T, TH 2:00PM - 3:15PM, FH- 413

Phone: 254-501-5819 , you can reach me out through email or canvas inbox

Email: d.gupta@tamuct.edu

Office Hours: Tuesday 1:00 pm – 2:00 pm, location: 323N

We can always schedule the appointment.
Mode of instruction and course access:

This course is a hybrid course and uses the TAMUCT Canvas Learning Management System: https://tamuct.instructure.com,

Here is full information:

Date	Tuesday	Thursday
17th, 19th Jan	In person	In person
24th, 26th Jan	In person	Online - cloud lab video
31st Jan, 2nd Feb	In person	In person
7th, 9th Feb	In person	In person
14th, 16th Feb	In person	In person
21st, 23rd Feb	In person	In person
28th Feb, 2nd March	In person	In person
7th, 9th March	In person	In person
21st, 23rd March	In person	Online
28th, 30th March	Mid-term exam Online	Upload video-Online
4th, 6th April	In person	Online
11th, 13th April	In person	Online
18th, 20th April	In person	Online
25th, 27th April	In person	Online
2nd, 4th May	In person	In Person

Student-instructor interaction:

Contact me via Canvas Inbox, if you do not hear back from me within 48 hours, please contact me via email.

WARRIOR SHIELD

Emergency Warning System for Texas A&M University-Central Texas
Warrior Shield is an emergency notification service that gives Texas A&M University-Central Texas the ability to communicate health and safety emergency information quickly via email, text message, and social media. All students are automatically enrolled in Warrior Shield through their myCT email account.

Connect to Warrior Shield by 911Cellular [https://portal.publicsafetycloud.net/Account/Login] to change where you receive your alerts or to opt out. By staying enrolled in Warrior Shield, university officials can quickly pass on safety-related information, regardless of your location.

COVID-19 SAFETY MEASURES

To promote public safety and protect students, faculty, and staff during the coronavirus pandemic, Texas A&M University-Central Texas has adopted policies and practices to minimize virus transmission. All members of the university community are expected to adhere to these measures to ensure their own safety and the safety of others. Students must observe the following practices while participating in face-to-face courses, course-related activities (office hours, help sessions, transitioning to and between classes, study spaces, academic services, etc.) and co-curricular programs:

- Self-monitoring—Students should follow CDC recommendations for self-monitoring. Students who have a fever or exhibit symptoms of COVID-19 should participate in class remotely and should not participate in face-to-face instruction. Students required to quarantine must participate in courses and course-related activities remotely and must not attend face-to-face course activities. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities.
- Face Coverings— Face coverings must be worn inside of buildings and within 50 feet of building entrances on the A&M-Central Texas Campus. This includes lobbies, restrooms, hallways, elevators, classrooms, laboratories, conference rooms, break rooms, non-private office spaces, and other shared spaces. Face coverings are also required in outdoor spaces where physical distancing is not maintained. The university will evaluate exceptions to this requirement on a case by case basis. Students can request an exception through the Office of Access and Inclusion in Student Affairs.

o If a student refuses to wear a face covering, the instructor should ask the student to leave and join the class remotely. If the student does not leave the class, the faculty member should report that student to the Office of Student Conduct. Additionally, the faculty member may choose to teach that day's class remotely for all students.

- Physical Distancing—Physical distancing must be maintained between students, instructors, and others in the course and course-related activities.
- Classroom Ingress/Egress—Students must follow marked pathways for entering and exiting classrooms and other teaching spaces. Leave classrooms promptly after course activities have concluded. Do not congregate in hallways and maintain 6-foot physical distancing when waiting to enter classrooms and other instructional spaces.

The university will notify students in the event that the COVID-19 situation necessitates changes to the course schedule or modality.

COURSE INFORMATION

Course Overview and Description:

The course focuses on clear and authoritative instructions about the field of computer forensics as it applies to the investigative process; from the collection of digital evidence to the presentation of Computer Forensic Examination findings in a court of law. Upon successful completion of the course, students will have a basic understanding of the computer forensic process, the scientific procedure involved in accounting, law enforcement, and computer sciences. Topics also include the science of computer forensics and how it relates to and is utilized within the judicial system of the United States.

Course Objective:

This course focuses on the use of the most popular forensics tools and provides specific guidance on dealing with civil and criminal matters relating to the law and technology. Includes discussions on how to manage a digital forensics operation in today's business environment.

Student Learning Outcomes:

After completing this course, students will:

- Understand the basic concepts of the forensic process
- Understand the types of computer crimes likely to lead to forensic investigations
- Learn certain specific approaches to forensic investigation and lab setup requirements
- Understand specific and practical steps when seizing evidence, imaging drives, and preparing suspect drives for analysis
- Understand techniques for hiding and scrambling information
- Review steps used to recover deleted data
- Examine email forensics
- Learn how to perform a forensic examination of a Windows computer
- Learn how to perform a forensic examination of a Linux computer
- Learn how to perform a forensic examination of a Mac computer
- Learn how to perform a forensic examination of mobile devices

Competency Goals Statements (certification or standards):

- Ability to understand basic concepts, hardware, networking, and laws of computer forensics
- Ability to describe common computer crimes, approaches to said crimes, and appropriate strategies for said crimes
- Ability to understand forensic methodologies, lab setup, and major forensic software
- Ability to properly seize a suspect computer, examine it, and analyzing drives
- Ability to understand steganography and cryptography
- Ability to recover deleted data in Windows, Linux, and Macintosh
- Ability to analyze emails and the laws related to email investigations
- Ability to understand the Windows operating system and examine it for evidence
- Ability to understand the Linux operating system and examine it for evidence
- Ability to understand the Macintosh operating system and examine it for evidence
- Ability to understand mobile concepts and terminology and how to seize evidence from mobile devices

Required Reading and Textbook(s):

Digital Forensics, Investigation, and Response

Fourth Edition, Book and Cybersecurity Cloud Labs

Author: Chuck Easttom

Navigate eBook for Digital Forensics, Investigation, and Response + Cloud Labs, Fourth Edition
ISBN: 9781284244502

Labs:

https://www.jblearning.com

You will need to register to the JB Learning website using the Access Code with your book. Then you will need to provide this class code:

Navigate eBook for Digital Forensics, Investigation, and Response + Cloud Labs, Fourth Edition
ISBN: 9781284244502
class code: 738AD4

Here is the link for all students to use to purchase the eBook/lab bundle if needed:

https://info2.jblearning.com/easttom4e-fdoc

The students can use Coupon Code: **TXAMCYBR25** which will give them 25% off.

You will then have access to the labs for the course. Grades for the labs are not automatically transferred to Canvas so you will not see the grade-book reflect it until I manually input your grades from the labs.

This is my first semester using the labs so please be patient with me should any issues occur. There is a "Before You Begin" section as well as a "System Checker" section when you log into the labs. Please follow these before proceeding. If there are technical issues, JB Learning does provide support.

Course Requirements:

- All assignments needs to be submitted via canvas assignment to receive the
- All assignments, labs, discussion board, quizzes, midterm and final exam have scheduled due dates.
  Assignments after the due date will NOT be accepted and will receive a grade of
- Missed examinations will receive a grade of zero. Only students who present a compelling and documented explanation MAY arrange for a make-up examination.

Grading Criteria Rubric and Conversion

Assignments	300 points
Labs	200 points
Quizzes	250 points
Midterm	100 points
Final	150 points

TOTAL: 1000 points

Course Grade Calculation

Grade	**A**	**B**	**C**	**D**	**F**
Percent	90-100%	80-89%	70-79%	60-69%	0-59%
Points	900-1000	800-899	700-799	600-699	0-599

Posting of Grades:

- All student grades will be posted on the Canvas Grade book and students should monitor their grading status through this tool.
- Grades for quizzes and exams will be posted as soon as they are completed. All other assignments will have their grades posted no later than two weeks after the assignment due date.

COURSE OUTLINE AND CALENDAR

Complete Course Calendar

	Chapter(s)	Assignments	Due Date
Week 1	**Chapter 1 & 2** - Understand the basic concepts of forensics - Maintain the chain of custody - Understand the basic hardware and networking knowledge needed for forensics - Know the basic laws related to computer forensics - Describe common computer crimes	Chapter-1 Assessments— Labs 1 Quizzes for Chapter 1	29th Jan
Week 2	- Understand varying forensic approaches to different crimes - Apply the appropriate forensic strategy based on the specific crime	Chapter-2 Assessments Labs 2 Quizzes for Chapter 2	
Week 3	**Chapter 3** - Understand major forensic methodologies - Set up a computer forensic lab	Chapter Assessment for Chapter 3	5th Feb, 12th feb

	- Demonstrate an understanding of major forensic software	Lab 3	
Week 4		Quiz for Chapter 3	
Week 5	**Chapter 4** - Properly seize a suspect computer - Prepare that computer for forensic examination - Understand the various storage formats - Image a drive - Acquire RAID drives	Chapter Assessment for Chapter 4 Lab 4	19th, 26th feb
Week 6		Quiz for Chapter 4	
Week 7	**Chapter 5 & 6** - Understand steganography - Use steganography - Detect stenography - Understand basic cryptography - Utilize basic cryptography - Understand general cryptanalysis techniques	Chapter Assessment for Chapter 5 & 6 Lab 5	5th, 12th March
Week 8	- Recover deleted files in Windows - Recover deleted files in Linux - Recover deleted files in Macintosh - Recover files from damaged drives	Quiz for Chapter 5 & 6	
	Midterm Exam		28th March
Week 9	**Chapter 7 & 8** - Understand the functionality of email and email protocols - Obtain the full email headers for a variety of email clients - Read and understand the contents of email headers	Chapter Assessments for Chapter 7 Labs 6	2nd, 9th April

Week 10	- Trace email to its origin - Work with email servers - Understand the laws related to email investigations - Understand the workings of the Windows operating system - Gather evidence from the Registry - Retrieve evidence from logs - Examine directories for evidence - Check the index.dat file for evidence	Quizzes for Chapter 7 Chapter Assessments for Chapter 8 Labs 7---Nov 02 Quizzes for Chapter 8	
Week 11	**Chapter 9** - Understand the Linux operating system - Retrieve logs from Linux - Utilize important shell commands	Chapter Assessment for Chapter 9 Lab 8	16th, 23rd April
Week 12	- Understand what directories are important in a Linux forensic investigation - Undelete files from Linux	Quiz for Chapter 9	
Week 13	**Chapter 10** - Understand the basics of Macintosh and its history - Know where to find logs in a Macintosh system	Chapter Assessment for Chapter 10 Lab 9	30th April
Week 14	- Examine the virtual memory of a Macintosh - Undelete Macintosh files	Quiz for Chapter 10	

	Chapter 11 & 12 - Understand cellular concepts and terminology - Understand what evidence to look for on mobile devices - Seize evidence from an iPhone, iPod, or iPad - Seize evidence from an Android phone - Seize evidence from a BlackBerry	Chapter Assessments for Chapter 11 & 12 Lab 10	
Week 15			
Week 16	- Understand network packets - Perform network analysis - Analyze routers for forensic evidence - Examine firewall logs for evidence	Quiz for Chapter 11 & 12	N/A
	Review Chapter and Prep for Final -No Assignments **Final Exam**		

INSTRUCTOR POLICIES

Examinations & Quizzes missed, will receive a grade of zero.
Students who present a compelling reason in ADVANCE may schedule a make-up Quiz or an Exam.

Copyright Notice.

Students should assume that all course material is copyrighted by the respective author(s). Reproduction of course material is prohibited without consent by the author and/or course instructor. Violation of copyright is against the law and Texas A&M University-Central Texas' Code of Academic Honesty. All alleged violations will be reported to the Office of Student Conduct.

Copyright. (2017) by (Daya Nand) at Texas A&M University-Central Texas, (Computer Information System); 1001 Leadership Place, Killeen, TX 76549; 254-213-4740; Fax 254-634-3998 daya.nand@tamuct.edu

TECHNOLOGY REQUIREMENTS AND SUPPORT

Technology Requirements.

This course will use the A&M-Central Texas Canvas learning management system.

Logon to A&M-Central Texas Canvas [https://tamuct.instructure.com].

Username: Your MyCT username (xx123 or everything before the "@" in your MyCT e-mail address) Password: Your MyCT password

Canvas Support

Use the Canvas Help link, located at the bottom of the left-hand menu, for issues with Canvas. You can select "Chat with Canvas Support," submit a support request through "Report a Problem," or call the Canvas support line: 1-844-757-0953.

For issues related to course content and requirements, contact your instructor.

Online Proctored Testing

A&M-Central Texas uses Proctorio for online identity verification and proctored testing. This service is provided at no direct cost to students. If the course requires identity verification or proctored testing, the technology requirements are: Any computer meeting the minimum computing requirements, plus web camera, speaker, and microphone (or headset). Proctorio also requires the Chrome web browser with their custom plug in.

Other Technology Support

For log-in problems, students should contact Help Desk Central.

24 hours a day, 7 days a week:

Email: helpdesk@tamu.edu

Phone: (254) 519-5466

Web Chat: [http://hdc.tamu.edu]

Please let the support technician know you are an A&M-Central Texas student.

UNIVERSITY RESOURCES, PROCEDURES, AND GUIDELINES

Drop Policy

If you discover that you need to drop this class, you must complete the Drop Request Dynamic Form through Warrior Web.

[https://dynamicforms.ngwebsolutions.com/casAuthentication.ashx?InstID=eaed95b9-f2be-45f3-a37d-46928168bc10&targetUrl=https%3A%2F%2Fdynamicforms.ngwebsolutions.com%2FSubmit%2FForm%2FStart%2F53b8369e-0502-4f36-be43-f02a4202f612].

Faculty cannot drop students; this is always the responsibility of the student. The Registrar's Office will provide a deadline on the Academic Calendar for which the form must be completed. Once you submit the completed form to the Registrar's Office, you must go into Warrior Web and confirm that you are no longer enrolled. If you still show as enrolled, FOLLOW-UP with the Registrar's Office immediately. You are to attend class until the procedure is complete to avoid penalty for absence. Should you miss the drop deadline or fail to follow the procedure, you will receive an F in the course, which may affect your financial aid and/or VA educational benefits.

Academic Integrity

Texas A&M University -Central Texas values the integrity of the academic enterprise and strives for the highest standards of academic conduct. A&M-Central Texas expects its students, faculty, and staff to support the adherence to high standards of personal and scholarly conduct to preserve the honor and integrity of the creative community. Academic integrity is defined as a commitment to honesty, trust, fairness, respect, and responsibility. Any deviation by students from this expectation may result in a failing grade for the assignment and potentially a failing grade for the course. Academic misconduct is any act that improperly affects a true and honest evaluation of a student's academic performance and includes, but is not limited to, working with others in an unauthorized manner, cheating on an examination or other academic work, plagiarism and improper citation of sources, using another student's work, collusion, and the abuse of resource materials. All academic misconduct concerns will be referred to the university's Office of Student Conduct. Ignorance of the university's standards and expectations is never an excuse to act with a lack of integrity. When in doubt on collaboration, citation, or any issue, please contact your instructor before taking a course of action.

For more information regarding the Student Conduct process, [https://www.tamuct.edu/student-affairs/student-conduct.html].

If you know of potential honor violations by other students, you may submit a report, [https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=0].

Academic Accommodations

At Texas A&M University-Central Texas, we value an inclusive learning environment where every student has an equal chance to succeed and has the right to a barrier-free education. The Office of Access and Inclusion is responsible for ensuring that students with a disability receive equal access to the university's programs, services and activities. If you believe you have a disability requiring reasonable accommodations please contact the Office of Access and Inclusion, WH-212; or call (254) 501-5836. Any information you provide is private and confidential and will be treated as such.

For more information please visit our Access & Inclusion Canvas page (log-in required) [https://tamuct.instructure.com/courses/717]

Important information for Pregnant and/or Parenting Students

Texas A&M University-Central Texas supports students who are pregnant and/or parenting. In accordance with requirements of Title IX and related guidance from US Department of Education's Office of Civil Rights, the Dean of Student Affairs' Office can assist students who are pregnant and/or parenting in seeking accommodations related to pregnancy and/or parenting. Students should seek out assistance as early in the pregnancy as possible. For more information, please visit Student Affairs [https://www.tamuct.edu/student-affairs/index.html]. Students may also contact the institution's Title IX Coordinator. If you would like to read more about these requirements and guidelines online, please visit the website [http://www2.ed.gov/about/offices/list/ocr/docs/pregnancy.pdf].

Title IX of the Education Amendments Act of 1972 prohibits discrimination on the basis of sex and gender–including pregnancy, parenting, and all related conditions. A&M-Central Texas is able to provide flexible and individualized reasonable accommodation to pregnant and parenting students. All pregnant and parenting students should contact the Associate Dean in

the Division of Student Affairs at (254) 501-5909 to seek out assistance. Students may also contact the University's Title IX Coordinator.

Tutoring

Tutoring is available to all A&M-Central Texas students, on a remote online basis. Visit the Academic Support Community in Canvas to view schedules and contact information. Subjects tutored on campus include Accounting, Advanced Math, Biology, Finance, Statistics, Mathematics, and Study Skills. Tutors will return at the Tutoring Center in Warrior Hall, Suite 111 in the Fall 2020. Student success coaching is available online upon request.

If you have a question regarding tutor schedules, need to schedule a tutoring session, are interested in becoming a tutor, success coaching, or have any other question, contact Academic Support Programs at (254) 501-5836, visit the Office of Student Success at 212F Warrior Hall, or by emailing studentsuccess@tamuct.edu .

Chat live with a tutor 24/7 for almost any subject from on your computer! Tutor.com is an online tutoring platform that enables A&M-Central Texas students to log in and receive online tutoring support at no additional cost. This tool provides tutoring in over 40 subject areas except writing support. Access Tutor.com through Canvas.

University Writing Center

The University Writing Center (UWC) at Texas A&M University–Central Texas (TAMUCT) is a free service open to all TAMUCT students. For the Fall 2020 semester, all services will be online as a result of the COVID-19 pandemic. The hours of operation are from 10:00 a.m.-5:00 p.m. Monday thru Thursday with satellite hours online Monday thru Thursday from 6:00-9:00 p.m. The UWC is also offering hours from 12:00-3:00 p.m. on Saturdays.

Tutors are prepared to help writers of all levels and abilities at any stage of the writing process. By providing a practice audience for students' ideas and writing, our tutors highlight the ways in which they read and interpret students' texts, offering guidance and support throughout the various stages of the writing process. While tutors will not write, edit, or grade papers, they will assist students in developing more effective composing practices. Whether you need help brainstorming ideas, organizing an essay, proofreading, understanding proper citation practices, or just want a quiet place to work, the UWC is here to help!

Students may arrange a one-to-one session with a trained and experienced writing tutor by making an appointment via WCOnline [https://tamuct.mywconline.com/]. In addition, you can email Dr. Bruce Bowles Jr. at bruce.bowles@tamuct.edu if you have any questions about the UWC and/or need any assistance with scheduling.

University Library

The University Library provides many services in support of research across campus and at a distance. We offer over 200 electronic databases containing approximately 250,000 eBooks and 82,000 journals, in addition to the 85,000 items in our print collection, which can be mailed to students who live more than 50 miles from campus. Research guides for each subject taught at A&M-Central Texas are available through our website to help students navigate these resources. On campus, the library offers technology including cameras, laptops, microphones, webcams, and digital sound recorders.

Research assistance from a librarian is also available 24 hours a day through our online chat service, and at the reference desk when the library is open. Research sessions can be scheduled for more comprehensive assistance, and may take place on Skype or in-person at the library. Assistance may cover many topics, including how to find articles in peer-reviewed journals, how to cite resources, and how to piece together research for written assignments.

Our 27,000-square-foot facility on the A&M-Central Texas main campus includes student lounges, private study rooms, group work spaces, computer labs, family areas suitable for all ages, and many other features. Services such as interlibrary loan, TexShare, binding, and laminating are available. The library frequently offers workshops, tours, readings, and other events. For more information, please visit our Library website [http://tamuct.libguides.com/index].

For Fall 2020, all reference service will be conducted virtually. Please go to our Library website [http://tamuct.libguides.com/index] to access our virtual reference help and our current hours.

OPTIONAL POLICY STATEMENTS

A Note about Sexual Violence at A&M-Central Texas

Sexual violence is a serious safety, social justice, and public health issue. The university offers support for anyone struggling with these issues. University faculty are mandated reporters, so if someone discloses that they were sexually assaulted (or a victim of Domestic/Dating Violence or Stalking) while a student at TAMUCT, faculty members are required to inform the Title IX Office. If you want to discuss any of these issues confidentially, you can do so through Student Counseling (254-501-5955) located on the second floor of Warrior Hall (207L).

Sexual violence can occur on our campus because predators often feel emboldened, and victims often feel silenced or shamed. It is incumbent on ALL of us to find ways to actively create environments that tell predators we don't agree with their behaviors and tell survivors we will support them. Your actions matter. Don't be a bystander; be an agent of change. For additional information on campus policy and resources visit the Title IX webpage [https://www.tamuct.edu/compliance/titleix.html].

Behavioral Intervention

Texas A&M University-Central Texas cares about the safety, health, and well-being of its students, faculty, staff, and community. If you are aware of individuals for whom you have a concern, please make a referral to the Behavioral Intervention Team. Referring your concern shows you care. You can complete the referral online [https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=2].

Anonymous referrals are accepted. Please see the Behavioral Intervention Team website for more information [https://www.tamuct.edu/student-affairs/bat.html]. If a person's behavior poses an imminent threat to you or another, contact 911 or A&M-Central Texas University Police at 254-501-5800.

OTHER POLICIES

Copyright Notice

Students should assume that all course material is copyrighted by the respective author(s). Reproduction of course material is prohibited without consent by the author and/or course instructor. Violation of copyright is against the law and Texas A&M University-Central Texas' Code of Academic Honesty. All alleged violations will be reported to the Office of Student Conduct.