

Syllabus for CSCE 5555.001 (10649)

COMPUTER FORENSICS

Meeting dates, times:

MoWe 8:30AM - 9:50AM

Meeting location:

NTDP K110

Instructor Information

Dr. Ervin Frenzel

Office E235B (Discovery Park – Engineering wing)

Ervin.frenzel@unt.edu

Office Hours: Monday - Wednesday
Friday

10:00 – 12:00; 14:00 – 16:00
13:00 – 15:00

Please reach out to identify if I have been called to other obligations – such as other student office hours before visiting.

Please keep all communications relating to class in the Canvas email, do not email me assignments (to my unt.edu or canvas email). Assignments will be counted as turned in when you complete them and turn them in through the Canvas turn-in. Assignments sent to my unt.edu or canvas email will not be counted as “submitted”, if the assignment is locked and you need to turn in the assignment (no later than 3 days following due date), it is your responsibility to contact me via email to set window for assignment turn-in. Understand that unless special circumstances exist, you will be docked points, the instructor will determine if you qualify for special permitting circumstances. **Communicate often and openly with your instructor.**

Connect with me through canvas email and/or by attending office hours. During busy times, my inbox becomes rather full, so if you contact me and do not receive a response within two business days, please send a follow up email. A gentle nudge is always appreciated. Office hours offer you an opportunity to ask for clarification or find support with understanding class material. I encourage you to connect with me via canvas email. Additional office hours, in person and virtually, will be offered as the semester concludes. Your success is our goal.

Instructor Values

I deeply value respect, integrity, honesty, and transparency. These values have served me well in my 30 + years in the field. I hope that you will consider incorporating these values so that they too can serve you well in your career. Grades are recorded based upon your activity and mastery of the subject matter. While I do not produce a “curve” for grades, I drop the lowest of each category of grade during evaluation, which will be discussed below.

*I value the perspectives students bring to my classroom and our campus. Please work with me to create a classroom culture of open communication, mutual respect, and belonging. All discussions should be respectful and civil. Although disagreements and debates are encouraged, personal attacks are unacceptable. Remember others have as much to a right to their opinion as you have to yours. **You do not have a right to photograph or otherwise record the class. First it is considered intellectual property of the instructor, second, it is a representation of other students – which means you may be liable for violating the privacy of others and possibly a FERPA (Family Educational Rights and Privacy Act) violation.** Together, we can ensure a safe and welcoming classroom for all. If you ever feel like this is not the case, please stop by my office and let me know. We are all learning together ([Code of Student Conduct](https://policy.unt.edu/policy/07-012)) (<https://policy.unt.edu/policy/07-012>).*

Honor Code: “I commit myself to honor, integrity, and responsibility as a student representing the University of North Texas community. I understand and pledge to uphold academic integrity as set forth by [UNT Student Academic Integrity Policy, 06.003](https://policy.unt.edu/policy/06-003) (<https://policy.unt.edu/policy/06-003>). I affirm that the work I submit will always be my own, and the support I provide and receive will always be honorable.”

To learn more about campus resources and information on how you can be successful at UNT, go to unt.edu/success and explore unt.edu/wellness. To get all your enrollment and student financial-related questions answered, go to scrappysays.unt.edu. [Course Description, Structure, and Objectives](#)

We have multiple sets of outcomes for this CSCE 4555 (Computer Forensics) and we will focus from very broad to very specific objectives within the course. In this 16-week (5 module) lecture/lab course, we will use a “flipped” classroom, meaning students are responsible for reading the assigned chapters prior to attending class (first meeting) so that they will be prepared for the class “notes” more importantly to ask pertinent questions to clarify content in a meaningful way. During the 2nd half of each module (second meeting), students should come to class having completed the labs, or have specific questions to clarify work within the labs. Discussion questions will be discussed in class to identify specific topics associated with various modular topics tied to forensics. We will focus on the catalog description as well as three NSA KU (Knowledge Units); Digital Forensics (DFS), Host Forensics (HOF), and Media Forensics (MEF).

CSCE 4555 (Computer Forensics)

Catalog Description:

Security goals, threats and vulnerabilities, Cryptography, program security and operating system security issues. Basic network security. Planning, policies, and risk analysis.

Credit Hours: 3

Prerequisites: CSCE 3600

Course Outcomes:

1. Demonstrate general knowledge and comprehension of computer forensics and computer investigations.
2. Describe and explain the Windows, Macintosh, and Unix/Linux operating systems data storage and methodologies.

3. Describe and explain the methods used for digital evidence control, processing crime and incident scenes, and data acquisition for computer forensic analysis.

4. Demonstrate knowledge and comprehension of basic tools and techniques used in the field of computer forensics sciences.

5. Describe and explain writing investigation reports and being an expert witness.

Additional NSA KU's:

Digital Forensics (DFS)

The intent of the Digital Forensics Knowledge Unit is to provide students with the skills to apply forensics techniques throughout an investigation life cycle with a focus on complying with legal requirements.

Outcomes

To complete this KU, students should be able to:

1. Discuss the rules, laws, policies, and procedures that affect digital forensics
2. Use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.

Topics

To complete this KU, all Topics and sub-Topics must be completed:

1. Legal Compliance
 - a. Applicable Laws
 - b. Affidavits
 - c. How to Testify
 - d. Case Law
 - e. Chain of custody
2. Digital Investigations
 - a. E-Discovery
 - b. Authentication of Evidence
 - c. Chain of Custody Procedures
 - d. Metadata
 - e. Root Cause Analysis
 - f. Using Virtual Machines for Analysis

Host Forensics (HOF)

The intent of the Host Forensics Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a host in a network.

Outcomes

1. Describe what can/cannot be retrieved from various Operating Systems,
2. Describe the methodologies used in host forensics.

Topics

To complete this KU, all Topics must be completed:

(More than one operating system should be demonstrated).

1. File Systems and File System Forensics
2. Hypervisor Analysis
3. Cryptanalysis
4. Rainbow Tables
5. Known File Filters (KFF)
6. Steganography
7. File Carving
8. Live System Investigations
9. Timeline Analysis
10. Include samples of hands-on activities

Media Forensics (MEF)

The intent of the Media Forensics Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a particular media in context.

Outcomes

To complete this KU, students should be able to:

1. Students should be able to describe methods and approaches for forensic analysis on specified media.

Topics

To complete this KU, all Topics and sub-Topics must be completed:

1. Drive Acquisition
2. Authentication of Evidence
 - a. Verification and Validation
 - b. Hashes
3. Metadata
4. Live vs. Static Acquisition
5. Sparse vs. Full Imaging
6. Slack Space
7. Hidden Files/clusters/partitions
8. (must include hands-on activities)

Federal regulations state that students may apply only 3 fully-online semester credit hours (SCH) to the hours required for full-time status for [F-1 Visa \(PDF\)](#) holders. Full-time status for F-1 Visa students is 12 hours for undergraduates and 9 hours for graduate students.

Required/Recommended Materials

- Required Textbook information (title, author, date and edition, publisher, cost, where available)

Computer Networking with Access 8th edition; Kurose, Pearson.

- Optional/Supplementary materials and/or readings:

Other reading content required to complete training will be available in the Canvas shell (at no cost or through readily available weblinks).

- Technology requirements for courses with digital materials:

This course has digital components. To fully participate in this class, students will need internet access to reference content on the Canvas Learning Management System and [faculty member to include other required equipment or software such as a webcam, microphone, Adobe Photoshop, etc.]. If circumstances change, you will be informed of other technical needs to access course content. Information on how to be successful in a digital learning environment can be found at [Learn Anywhere \(https://online.unt.edu/learn\)](https://online.unt.edu/learn).

Assessing Your Work

Our grading scale is:

A	89.5	to	100
B	79.5	to	89.49
C	69.5	to	79.49
D	59.5	to	69.49
E	0	to	59.49

Weighted Work Percentages for final grades:

Discussion Questions (lowest dropped)	30%
Lab Assignments	10%
Participation	10%
Midterm Exam	25%
Final Exam	25%

Attendance and Participation

Research has shown that students who attend class are more likely to be successful. You should attend every class unless you have a university excused absence such as active military service, a religious holy day, or an official university function as stated in the [Student Attendance and](#)

[Authorized Absences Policy \(PDF\) \(https://policy.unt.edu/policy/06-039\)](https://policy.unt.edu/policy/06-039). If you cannot attend a class due to an emergency, please let me know. Your safety and well-being are important to me.

Because this course involves collaboration, participation is essential to learning. Our project-based activities require you to be actively engaged in discussions and group work. **Active participation will count for 10% of your final grade, this involves in-class participation during discussion question sessions and content presentation.** I understand tardiness and absences may occur. If you are late to class, please drop me an email to let me know the circumstances. If you must miss class, please let me know prior to your absence.

Course Summary:

Dates are tentative and subject to change in the event of inclement weather. You will be notified by Eagle Alert if there is a campus closing that will impact your class. [Emergency Notifications and Procedures Policy \(https://policy.unt.edu/policy/06-049\)](https://policy.unt.edu/policy/06-049).

Course Summary:		
Date	Details	Due
Mon Aug 21, 2023	Page (1) Module 3 & 5 (combined) - to do list	to do: 11:59pm
Thu Aug 24, 2023	Discussion Topic Module 0 (Welcome and understanding the class information)	due by 11:59pm
	Discussion Topic Module 3 - (Week 1; 21-26 Aug 2023) Chapter 1 Understanding The Digital Forensics Profession and Investigations	due by 11:59pm
Thu Aug 31, 2023	Discussion Topic Module 3 - (Week 2; 27 Aug 2023 - 2 Sep 2023) Chapter 2 The Investigator's Office and Laboratory	due by 11:59pm
Thu Sep 7, 2023	Discussion Topic Module 3 - (Week 3; 3-9 Sep 2023) Chapter 4 Processing Crime and Incident Scenes	due by 11:59pm
Thu Sep 14, 2023	Discussion Topic Module 1 - Demonstrate general knowledge and comprehension of computer forensics and computer investigations.	due by 11:59pm
	Discussion Topic Module 3 - (Week 4; 10-16 Sep 2023) Chapter 11 E-mail and Social Media Investigations	due by 11:59pm
	Discussion Topic Module 5 - Describe and explain writing investigation reports and being an expert witness.	due by 11:59pm
Thu Sep 21, 2023	Discussion Topic Module 3 - (Week 5; 17-23 Sep 2023) Chapter 14 Report Writing for High-Tech Investigations	due by 11:59pm
Thu Sep 28, 2023	Discussion Topic Module 3 - (Week 6; 24-30 Sep 2023) Chapter 15 Expert Testimony in Digital Investigations & Chapter 16 Ethics for the Expert Witness	due by 11:59pm
Sun Oct 1, 2023	Page (2) Module 2 - to do list - Describe and explain the Windows, Macintosh, and Unix/Linux operating systems data storage and methodologies.	to do: 11:59pm
Thu Oct 5, 2023	Discussion Topic Module 2 - (Week 7; 1-7 Oct 2023) Chapter 5 Working with Windows and CLI Systems	due by 11:59pm

Mon Oct 9, 2023	Quiz Midterm Exam	due by 11:59pm
Thu Oct 12, 2023	Discussion Topic Module 2 - (Week 8; 8-14 Oct 2023) Chapter 7 Linux and Macintosh File Systems	due by 11:59pm
	Assignment Overview of Data Acquisition - Lab 1 (Create a disk image file of a hard disk partition)	due by 11:59pm
	Assignment Overview of Data Acquisition - Lab 2 (Acquire RAM from Windows Workstation)	due by 11:59pm
	Assignment Overview of Data Acquisition - Lab 3 (Acquire volatile information from a live windows system)	due by 11:59pm
	Assignment Overview of Data Acquisition - Lab 4 (Analyze file system of a linux image using autopsy)	due by 11:59pm
	Assignment Performing Evidence Analysis - Lab 1 (View contents of forensic image file)	due by 11:59pm
Thu Oct 19, 2023	Discussion Topic Module 2 - (Week 9; 15-21 Oct 2023) Chapter 12 Mobile Device Forensics and the Internet of Anything	due by 11:59pm
Sun Oct 22, 2023	Page (3) Module 1 - to do list - Students should be able to describe methods and approaches for forensic analysis on specified media.	to do: 11:59pm
Thu Oct 26, 2023	Discussion Topic Module 1 - (Week 10; 22-28 Oct 2023) Chapter 10 Virtual Machine Forensics, Live Acquisitions, and Network Forensics	due by 11:59pm
Sun Oct 29, 2023	Page (4) Module 4 - to do list - Demonstrate knowledge and comprehension of basic tools and techniques used in the field of computer forensics sciences.	to do: 11:59pm
Thu Nov 2, 2023	Discussion Topic Module 4 - (Week 11; 29 Oct 2023 - 4 Nov 2023) Chapter 3 Data Acquisition	due by 11:59pm
Thu Nov 9, 2023	Discussion Topic Module 4 - (Week 12; 5-11 Nov 2023) Chapter 6 Current Digital Forensics Tools	due by 11:59pm
Thu Nov 16, 2023	Discussion Topic Module 4 - (Week 13; 12-18 Nov 2023) Chapter 8 Recovering Graphics Files	due by 11:59pm
Thu Nov 30, 2023	Discussion Topic Module 4 - (Week 14; 26 Nov 2023 - 2 Dec 2023) Chapter 9 Digital Forensics Analysis and Investigation & Chapter 13 Cloud Forensics	due by 11:59pm
Sun Dec 10, 2023	Assignment Certification Exam or Written report for Graduate Student only.	due by 11:59pm
Mon Dec 11, 2023	Quiz Final Exam	due by 11:59pm
	Assignment Roll Call Attendance	

How to Succeed in this Course / Required Notices

Academic Integrity Standards and Consequences

According to UNT Policy 06.003, Student Academic Integrity, academic dishonesty occurs when students

engage in behaviors including, but not limited to cheating, fabrication, facilitating academic dishonesty, forgery, plagiarism, and sabotage. A finding of academic dishonesty may result in a range of academic penalties or sanctions ranging from admonition to expulsion from the University.

Plagiarism will not be tolerated. Plagiarism or strictly using AI used to answer Discussion Questions or homework assignments will result in an automatic grade of "0" (zero) for the assignment, for a second confirmed use a "0" (zero) for all assignments in the category. All assignments will have plagiarism and AI checks enabled (behind the scenes to detect use of plagiarized or artificially created content).

ADA Accommodation Statement

UNT makes reasonable academic accommodation for students with disabilities. Students seeking accommodation must first register with the Office of Disability Accommodation (ODA) to verify their eligibility. If a disability is verified, the ODA will provide a student with an accommodation letter to be delivered to faculty to begin a private discussion regarding one's specific course needs. Students may request accommodations at any time; however, ODA notices of accommodation should be provided as early as possible in the semester to avoid any delay in implementation.

Note: that students must obtain a new letter of accommodation for every semester and must meet with each faculty member prior to implementation in each class. For additional information see the ODA website at <http://disability.unt.edu>

Course Safety Procedures (for Laboratory Courses)

While working in laboratory sessions, students enrolled in CSCE 3530 - Introduction to Computer Networks are required to follow proper safety procedures and guidelines in all activities requiring lifting, climbing, walking on slippery surfaces, using equipment and tools, handling chemical solutions and hot and cold products. Students should be aware that **UNT is not liable for injuries or damage to personal computers** incurred while students are participating in class activities. All students are encouraged to secure adequate insurance coverage in the event of accidental injury (**there should be no more than average computer usage during this course**). Students who do not have insurance coverage should consider obtaining Student Health Insurance. Brochures for student insurance are available in the UNT Student Health and Wellness Center. Students who are injured during class activities may seek medical attention at the Student Health and Wellness Center at rates that are reduced compared to other medical facilities. If students have an insurance plan other than Student Health Insurance at UNT, they should be sure that the plan covers treatment at this facility. If students choose not to go to the UNT Student Health and Wellness Center, they may be transported to an emergency room at a local hospital. Students are responsible for expenses incurred there.

Emergency Notification & Procedures

UNT uses a system called Eagle Alert to quickly notify students with critical information in the event of an emergency (i.e., severe weather, campus closing, and health and public safety emergencies like chemical spills, fires, or violence). In the event of a university closure, please refer to the UNT Learning Management System (LMS) for contingency plans for covering course materials.

Instructor expectations and explanations:

Email the instructor primarily through Canvas, allow 24-48 business hours for response, this is your primary means of communication with the instructor. The instructor does not typically respond on the weekends. Grades will automatically reflect as a "0" if an assignment has not been turned in by the due date. **Homework does not count as having been turned in until you physically submit it via "Canvas", it cannot be emailed to the instructor or TA to count for credit.** If it is late and the Canvas turn-in has closed, then you must contact the instructor to open the assignment, at which point late points will be

assessed. **It will not be accepted more than 3 days late, without extenuating circumstances, at the discretion of the instructor (not the TA).**

Once grades are posted please contact the instructor within 7 days if you have a question or concern about the grade - we can discuss to identify what is right or wrong with the assignment as it was or was not turned in.

You will receive training in Basic Networking, in addition to the NSA topics listed under the following KU (Basic Networking-BNW). **You will be responsible for checking announcements 3 times a week (I recommend Monday, Wednesday, and Friday).** It will not be sufficient to take a certification exam without external study.

Basic Networking (BNW)

The intent of the Basic Networking Knowledge Unit is to provide students with basic understanding of how networks are built and operate, and to give students some experience with basic network analysis tools. Students are exposed to the concept of potential vulnerabilities in a network.

Outcomes:

To complete this KU, students should be able to:

1. Describe the fundamental concepts, technologies, components and issues related to communications and data networks.
2. Design a basic network architecture given a specific need and set of hosts/clients.
3. Track and identify the packets involved in a simple TCP connection (or a trace of such a connection).

4. Use a network monitoring tools to observe the flow of packets (e.g., Wireshark).
5. Perform network mapping (enumeration and identification of network components) (e.g., Nmap).
6. Describe common network vulnerabilities.

Topics:

To complete this KU, all Topics and sub-Topics must be completed:

1. Networking models (OSI and IP).
2. Network media (wired, optical, and wireless)
3. Network Architectures and topologies (PAN, LAN/WAN, DMZ, Enclaves, VLAN, NAT, subnetting, super netting)
4. Common Network Devices and their role in the network. (Routers, Switches, Hosts, VPNs, Firewalls)
5. Network Protocols introduction (IP, TCP, UDP, ICMP)
6. Network Services and protocol's introduction (DNS, NTP, VLAN, etc.).
7. Network Applications and protocol's introduction (SMTP, HTTP, VoIP, SSH, etc.).
8. Use of basic network administration tools.
9. Overview of Network Security Issues

For those who take and pass a certification exam. If you choose to take a certification exam in lieu of taking a final exam, a passed certification exam will count as a replacement for the in-class final exam (Undergraduate students).

For those taking this course for **Undergraduate credit (CSCE 4555)** - **enrolled through the registrar's office for undergraduate credit:**

Final Exam:

Will consist of 200 (randomly chosen) questions worth .5 points apiece. You will have 3.5 hours to complete the exam in class, during the scheduled time for the Midterm, all materials are drawn from the book that we are using in the course itself (without supplemental materials) for chapters 1 - 16. Questions will be randomly pulled from chapters to this point in the semester with shuffled answers (no one will receive the same questions in the same order or with answers in the same order).

The 200 questions will focus on the work from the 2nd 8 weeks (120 Questions) but include questions from the 1st 8 weeks (80 Questions).

or

Acceptable forensic certification exam replacements include:

EC Council's Computer Hacking Forensic Investigator (CHFI)

Or

ISC2 SSCP (System Security Certified Practitioner)

Or

Access Data Certification

Or

Paraben Forensic Certification

For those taking this course for **Graduate credit (CSCE 5555)**- enrolled through the registrar's office for graduate credit.

You must notify the instructor of your decision through email no later than 4 weeks from the initial start date of the class - failure to notify the instructor indicates you will be completing the (1) In Class final exam **without a replacement certification option or the (2) Report **with** certification option:**

(1) Written Graduate Report **with either the final exam **or** a passed industry certification:**

(Either way must take this) The final report at the end of the semester will consist of an **integrative literature review** of 10 identified network protocol errors, the paper must consist of 10 or more APA 7.0 formatted pages (sans or Times new roman font size 12, double spaced, one-inch margins). It will exclude the cover page, reference pages, and abstract page if you choose to write one. It must be your own original work and will be checked for AI creation through inclusive Turnitin reporting and must contain at least 15 unique credible sources (authoritative), **no wikis, blogs (unless the wikis or blogs are seminal sources), or AI generated material will be counted within the paper for sources.**

And

The in class final exam.

Will consist of 200 (randomly chosen) questions worth .5 points apiece. You will have 3.5 hours to complete the exam in class, during the scheduled time for the Midterm, all materials are drawn from the book that we are using in the course itself (without supplemental materials) for chapters 1 - 16. Questions will be randomly pulled from chapters to this point in the semester with shuffled answers (no one will receive the same questions in the same order or with answers in the same order).

The 200 questions will focus on the work from the 2nd 8 weeks (120 Questions) but include questions from the 1st 8 weeks (80 Questions).

or

Completion of:

Acceptable forensic certification exam replacements include:

EC Council's Computer Hacking Forensic Investigator (CHFI)

Or

ISC2 SSCP (System Security Certified Practitioner)

Or

Access Data Certification

Or

Paraben Forensic Certification

Discussion Questions (and how to maximize the grading)

Initial Discussion Question responses (Due every Thursday of the even weeks at 23:59): These questions will not be reopened after they close. A single discussion question (lowest grade) will be dropped at the end of the semester.

All discussion questions for weekly class discussion question credit will require that you will provide an initial answer to **ALL** weekly discussion questions by Thursday evening of the assigned week (no later than 23:59). This initial response should equate to 250 words and have a significant contribution to the weekly topic. You will only receive a notice for the Thursday due date, but it has three components - the Initial response due Thursday, and two peer responses due by Saturday at 23:59. **This initial response counts for 50 of the 100 points for the discussion question prompt.**

Attendance will be taken each week in class, additionally topic in class participation and will count as 10% of the course overall grade.

Part 2 (Due by Saturday of every week at 23:59)

You must complete 2 significant peer responses per week by Saturday evening at Midnight to receive the full credit for the weekly discussion questions (again by 23:59). These peer responses should equal another 250 words. Peer responses should have 1-3 (in-text) cited sources with a reference section properly formatted in APA 7.0. **These peer responses each count for 25 points of the 100 points for the discussion question prompt.**

Understand there will be external work (equating to a flipped classroom through external work and research), there will be increased writing from the regular classes, and there will be a requirement to submit a written protocol analysis and submit an integrated literature review briefing (involving multiple protocol threats against discussed layer of the TCP/IP protocol stack) before the end of the semester (these submissions will be your final exam for the class). **Homework does not count as having been turned in until you physically submit it via "Canvas", it cannot be emailed to the instructor or TA to count for credit.** If it is late and the Canvas turn-in has closed, then you must contact the instructor to open the assignment, at which point late points will be assessed. **It will not be accepted more than 3 days late, without extenuating circumstances, at the discretion of the instructor (not the TA).**

Discussion questions are not a reason to attack someone for their beliefs or statements, and that if you disagree with someone's statement, you should first seek to understand (through civil online discussion and conduct). Realize you cannot demand another person change their way of thinking but rather recognize it is their right to think the way they believe they should. If you believe you are in danger because of expressed views - reach out to your instructor (ervin.frenzel@unt.edu) for guidance. **Do not be surprised if you are referred to someone who can provide support from the school level, not just the classroom level.**

The instructor is not required to accept late work. Students are responsible for completing work by the assigned due date and time, there can be pre-approved exceptions (provided you have communicated with your instructor). In many cases students will have the option of completing work the week before to ensure they have sufficient time to complete work. If you have an emergency (or believe a situation to be an emergency), contact the instructor and let the instructor know the circumstance. **This is for emergencies as the instructor sees them, not as you see them. If in doubt about a circumstance, contact the instructor.**

AI (Artificial Intelligence) is a very creative tool which often misreports information when queried (and often introducing bias as the tool is designed to draw from like material once you find a result that you

agree with). You may use AI to generate thoughts, but you cannot turn in AI generated responses to your discussion question without first researching and generating original thoughts that you as an individual have created. As such, confirmed using of AI to answer Discussion Questions or homework assignments will result in an automatic grade of "0" (zero) for the assignment, a second confirmed academic integrity violation the instructor reserves the right to fail the student with a "0" for the course.

The lowest grade of the semester discussion question grades will be dropped at the end of the semester. The lowest grade of class participation will be dropped at the end of the semester. The lowest grade of the "assignments" grades grouping will be dropped at the end of the semester. The Final exam report will follow APA 7.0 formatting - and will have checks completed to ensure it is authentic and original to the student submitting it.

Academic Integrity Standards and Consequences

According to UNT Policy 06.003, Student Academic Integrity, academic dishonesty occurs when students engage in behaviors including, but not limited to cheating, fabrication, facilitating academic dishonesty, forgery, plagiarism, and sabotage. A finding of academic dishonesty may result in a range of academic penalties or sanctions ranging from admonition to expulsion from the University.

Plagiarism will not be tolerated. Plagiarism or strictly using Artificial Intelligence or AI (without it being part of the assignment) used to answer Discussion Questions or homework assignments will result in an automatic grade of "0" (zero) for the assignment, a second confirmed academic integrity violation the instructor reserves the right to fail the student with a "0" for the course.

All assignments will have plagiarism and AI checks enabled (behind the scenes to detect use of plagiarized or artificially created content. **There is mandatory reporting by faculty for suspected academic integrity violations.**