# University of Oklahoma University of Oklahoma Polytechnic Institute CYBS 3743: Cyberforensics Fundamentals Spring 2025

## Course Format/Meeting Time: Tuesdays and Thursdays from 1:00 pm to 2:20 pm.

## Location: OU Tulsa Campus, Building 3 – 3100 or 3102

## Instructor: Dr. Sungbo Jung

**Contact:** [sungbo.jung@ou.edu](mailto:sungbo.jung@ou.edu), Administration Building, Room 1H27, (918) 660-3495

**About Your Instructor**: I am Dr. Sungbo Jung, holding a PhD in Computer Science and Engineering from the University of Louisville. My professional experience includes web service development, efficient data center design and operation, and constructing advanced cyber ranges. My research focuses on cryptography, hardening web servers, and cybersecurity education. I am dedicated to advancing both practical and theoretical aspects of computing, which will equip students to tackle the challenges of modern technology infrastructure.

### Student Support Hours: Monday and Wednesday from 1:30 pm to 4:30 pm CST or by appointment. Virtual student support hours are also available. These hours are dedicated to you, providing a space where you can ask questions about course content, engage in deeper discussions, voice any concerns you have about the class, and explore career or graduate school options in this field with me. Many students feel hesitant about interrupting my time, but I want to assure you that your visits are welcome and encouraged! These sessions are valuable not only for your learning but also for me to understand better the questions and needs of my students, allowing me to refine my teaching methods accordingly.

### Learning Management System/Website: All Materials (except the textbooks) will be available on Canvas. Log in with your OU ID (usually the first 4 letters of your last name followed by a 4-digit number). All assignments, deadlines, grades, announcements, and course documents will be posted to the CYBS 3743 Canvas page. It is your responsibility to regularly check for updates. You can confiture Canvas to email you notifications. Click this link to go to the class website: [https://canvas.ou.edu](https://canvas.ou.edu/).

## Course Prerequisites: CYBS 3123

## Course Description: This course introduces students to cyber forensics and cyber-crime scene analysis fundamentals. The various laws and regulations dealing with computer forensic analysis are discussed. Students are introduced to the emerging international standards for cyber forensic analysis and a formal methodology for conducting computer forensic investigations.

## Course Goals:

## Students will understand many aspects of the digital forensics techniques.

## Students will learn about evidence management, including data acquisition, remote network acquisition tools, and validating data acquisitions.

## Students will learn to gather data and perform analysis in various operating systems, including virtual and cloud-based systems.

## Students will learn to evaluate various digital forensics tools, validating and testing forensics software and evaluating their effectiveness.

## Students will learn to perform network, mobile, and cloud forensics.

## Students will learn to communicate with the evidence gathered.

## Students will develop an application or tool to analyze cyber forensics data.

## Learning Outcomes: Upon successful completion of the course, the student will be able to:

* Competent with a working knowledge of cyber forensics applications and tools.
* Recognize various laws and regulations on computer forensic analysis.
* Implement and maintain a chain of custody plan following the rules of evidence.
* Develop an application or tool for cyber forensics using Python or .Net Framework
* Demonstrate the fundamental concepts and methodologies of cyber forensics and crime scene analysis.

## ABET:

Students will increase their ability to meet the following ABET outcomes (which are outcomes tied to the accreditation of the bachelor of science degree in cybersecurity):

* Outcome 1: Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.
* Outcome 3: Communicate effectively in a variety of professional contexts.
* Outcome 5: Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.

## Texts and Materials:

Required: *None*

Optional:

Title: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory

Author: Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters

ISBN: 978-1118825099

Publisher: Wiley

Date: 07/28/2014

Title: File System Forensic Analysis

Author: Brian Carrier

ISBN: 978-0321268174

Publisher: Addison-Wesley Professional

Date: 03/17/2005

Title: The Practice of Network Security Monitoring: Understanding Incident Detection and Response

Author: Richard Bejtlich

ISBN: 978-1593275099

Publisher: No Starch Press

Date: 07/15/2013

Resources*:*

I will also provide open-access resources that will provide additional information on cyber forensics topics related to the class. These resources are optional, but are a great way for you to more thoroughly explore the topics covered in our course. This will include information from mainstream sources (e.g., news, social media) and articles from research journals that provide a more in-depth take on issues related to our class. These resources will be posted in the course documents portion of the class on Canvas and will provide you with a solid foundation for our class discussions and activities.

**Teaching Philosophy**:

My goal is to create a class in which everyone is welcome, included, and able to learn and succeed. I anticipate that there will be a wide range of knowledge about the topics we will discuss, from students having no or limited knowledge, to students who have read more extensively or worked in the cybersecurity field in some capacity. We all have different learning preferences and I’ve designed this course so that you can learn from different types of sources, including news articles, peer-reivewe academic articles, discussion, lectures, and videos. learn in different ways, and I will seek to help you learn in the way that best facilitates your learning style. We will incorporate news articles, peer-reviewed academic articles, and videos. To make the learning process easiest on yourself, you need to do the assigned readings ahead of class time.

My expectation is that you give your attention to the discussion and contribute without dominating the discussion (i.e., everyone deserves a chance to express their thoughts and insights). I fully expect to learn from you as much as you learn from me and for us all to be respectful in our dialogue and discussion. You can ask probing or difficult questions, but it should be done in the spirit of learning or discovering new knowledge.

## Expectations:

## You can expect from me:

* To start and end class on time.
* To assign homework that covers the material and is relevant to the course.
* To reply to your emails in a timely manner.
* To keep regularly scheduled student hours and appointments.
* To provide opportunities for intellectual growth.

## Students are expected:

* To be present in all class meetings and inform me in a brief e-mail if you will be absent.
* To participate actively in class discussions; be attentive and engaged; ask questions.
* To spend an adequate amount of time on homework each week and projects so we can collectively discuss questions and share understandings.
* To seek help from me when needed; ask early which gives us time to make corrections, not at the end of the semester when options are more limited.

## Learning Activities, Assignments, and Assessments:

This course will engage you with various activities, assignments, and labs. You will read from the textbooks before class and actively participate in learning activities in class to help deepen your understanding of the content. There will be a collaborative project that will help deepen your critical thinking, demonstrate your understanding of the topic, and develop collaboration and communication skills – all of which are highly valued by employers.

## Assessments (Grading):

All assignments will be listed and explained in Canvas. I encourage you to keep that page handy or bookmarked and check it frequently. Additional instructions or explanations will be provided through the course as necessary.

Grading matrix:

|  |  |
| --- | --- |
| Grade | Points earned |
| A | 91% ≤ Yours |
| Dilemma Zone B | 89% < Youres < 91% |
| B | 81% ≤ Yours ≤ 89% |
| Dilemma Zone C | 79% < Youres < 81% |
| C | 71% ≤ Yours ≤ 79% |
| Dilemma Zone D | 69% < Youres < 71% |
| D | 59% < Yours ≤ 69% |
| F | Yours ≤ 59 |

Grading policy:

If you belong to the dilemma zone, your letter grade will be determined by

* Active participation
* Performance improvement
* Extra award

Quizzes 5%

Assignments ( Homeworks and Projects ) 50%

Test 1 15%

Test 2 15%

Test 3 15%

\* You have two excuses for any combinations of the assignments.

   Excused assignments will be replaced with your average points at the end of the semester.

Once an assignment is submitted, it will not be replaced with an excuse.

You’ll be asked to verbally participate in class through informal and formal presentations, class discussions, and in teamwork. My goal is to provide you a supportive environment where you can practice your public speaking. Our class discussions and informal presentations are there to help you build your confidence in advance of your final presentation, which you’ll do in a group. Working in a group and public speaking are two key skills identified by employers in our field. I know public speaking can cause some anxiety and I want you to know that there are resources available to help. You may find it beneficial to talk with counseling services, use their [self-help resources](https://www.ou.edu/ucc/resources/self-help), including [Anxiety and Stress](https://www.ou.edu/ucc/resources/anxiety-and-stress). You can also follow along with activities shown in videos, such as a [tapping exercise or](https://www.youtube.com/watch?v=75PUjUsGsQQ) [unilateral breathing](https://www.youtube.com/watch?v=7nHbLtBbvcY), to practice mindfulness before you participate in public speaking.

## Course Policies:

**Academic Integrity and Plagiarism:** Academic honesty is incredibly important within this course. Cheating is strictly prohibited at the University of Oklahoma, because it devalues the degree you are working hard to get. As a member of the OU community, it is your responsibility to protect your educational investment by knowing and following the rules. For specific definitions on what constitutes cheating, review the [Student’s Guide to Academic Integrity](http://integrity.ou.edu/students_guide.html).

The overall goal of this course is your learning. In order to demonstrate that you have reached this goal, the work you turn in needs to be your own. This includes putting written work into your own words and citing your sources, as appropriate, to avoid plagiarism. If you work in a group, seek assistance from a tutor, use a resource on campus, and/or use online resources (including AI software – see specific AI policy below), the work you turn in must be your own, demonstrating your own understanding of the material that you have gained through the learning process.

If you have questions about academic integrity or plagiarism, please ask: my aim is to foster an environment where you can learn and grow, while also maintaining academic honesty and a clear representation of your learning and ideas. Penalties for serious offenses include a zero on the assignment and egregious offenses can even result in expulsion from the university, so it is important to understand expectations.

Plagiarism as defined by the [OU Integrity Office](https://www.ou.edu/integrity/students#OU-and-Integrity) includes:

• Copying words and presenting them as your own writing.

• Copying words, even if you give the source, unless you also indicate that the copied words are a direct quotation

• Copying words and then changing them a little, even if you give the source.

• Even if you express it in your own words, it is plagiarism to use someone else’s idea as your own.

Visit the [OU Integrity Office](https://www.ou.edu/integrity/students#OU-and-Integrity) for more information on what constitutes plagiarism.

**Artificial Intelligence Policy**: I hope that this course aids you in a creative exploration of Generative AI tools and how they can be used to assist you in accomplishing the goals of this course. In this course, you:

* May use any **free** Generative AI tools, including those provided to you by the university. This will allow everyone in the course to have the same access to Generative AI. Using AI does not negate or change the Academic Integrity and Plagiarism guidance.
* Must appropriately acknowledge its use and provide a statement describing how and why it was used, and how you verified the accuracy of its output. You are expected to cite your usage of Generative AI, including any direct quotes or paraphrasing of ideas/content generated by AI. But remember, AI can be wrong, so verify the output.
* **Cannot** use it to write any papers and submit as your own work. You can use it to give you ideas; however, I will be asking you to explain your work and I will ask questions about the topic – studying the material is the only way to really learn.

Usage of generative AI without appropriate acknowledgment will be considered a violation of the academic integrity policy for this course.

### Absences and Make-up Policy: Students must attend classes to keep up with the course material. If you miss class, you are expected to contact me. For this course, you have excused absence for appropriate reasons, such as emergencies, lifetime events, or illness. You have two excuses for any combination of the assignments. Excused assignments will be replaced with your average earned points at the end of the semester. Once an assignment is submitted, it will not be replaced with an excuse. Any assignments that are due on the day would still need to be completed in accordance with the late work policy. Makeup tests are given only if solid evidence of a medical or serious emergency prevents the student from participating in the exam.

### In addition to your excused absence, I will also excuse additional absences due to accommodations, as communicated with Accessibility and Disability Resource Center (ADRC), medical emergencies (including mental or physical, with a doctor’s, counselor’s, or ADRC note), illness or death in a close relation, and university sponsored activities. If you have childcare/eldercare or other issues that may prevent you from being as active of a participant during class discussion as you normally would be, please notify me so that we can discuss another way in which you can demonstrate your participation that day.

### If in doubt on whether an absence would be excused or not, I want you to talk with me. Additional excused absences are at my discretion. If you have three or more unexcused absences in the course, you may receive a reduction in your final letter grade of ten points (e.g. a C would become a D) since active in-class participation is an expectation of the course. The final exam will not have a makeup test and must be taken. Failure to take the final exam will result in an automatic F.

## Land Acknowledgement Statement Provided by OU’s Tribal Liaison office:

Long before the University of Oklahoma was established, the land on which the University now resides was the traditional home of the “Hasinais” Caddo Nation and “[Kirikirʔi:s](http://www.wichitatribe.com/media/18910/wichita.mp3)” (audio available when opened in Chrome) Wichita & Affiliated Tribes. We acknowledge that this territory once also served as a hunting ground, trade exchange point, and migration route for the Apache, Comanche, Kiowa, and Osage nations.  Today, 39 tribal nations dwell in the state of Oklahoma due to settler and colonial policies designed to assimilate Native people. The University of Oklahoma recognizes our university's historical connection with its indigenous community. We acknowledge, honor and respect the diverse Indigenous peoples connected to this land. We fully recognize, support, and advocate for the sovereign rights of all of Oklahoma’s 39 tribal nations. This acknowledgment is aligned with our university’s core value of creating a diverse and inclusive community. It is an institutional responsibility to recognize and acknowledge the people, culture, and history that make up our entire OU Community.

## University Policies

### Mental Health Support Services

Support is available for any student experiencing mental health issues that are impacting their academic success.  Students can either been seen at the University Counseling Center (UCC) located on the second floor of Goddard Health Center or receive 24/7/365 crisis support from a licensed mental health provider through [TELUS](https://www.ou.edu/ucc/online-therapy) Health.  To schedule an appointment or receive more information about mental health resources at OU please call the UCC at 405-325-2911 or visit  [University Counseling Center](https://www.ou.edu/ucc). The UCC is located at 620 Elm Ave., Room 201, Norman, OK 73019. Given we are in Tulsa, please contact Student Affairs in the Founders Student Center, or email them at TulsaSA@ou.edu, or call them at 918-660-3100.

### Title IX Resources and Reporting Requirement

The University of Oklahoma faculty are committed to creating a safe learning environment for all members of our community, free from gender and sex-based discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking, in accordance with Title IX. There are resources available to those impacted, including: speaking with someone confidentially about your options, medical attention, counseling, reporting, academic support, and safety plans. If you have (or someone you know has) experienced any form of sex or gender-based discrimination or violence and wish to speak with someone confidentially, please contact [OU Advocates](https://www.ou.edu/gec/gender-based-violence/advocates)(available 24/7 at 405-615-0013) or [University Counseling Center](http://ou.edu/ucc) (M-F 8 a.m. to 5 p.m. at 405-325-2911)

Because the University of Oklahoma is committed to the safety of you and other students, and because of our Title IX obligations, I, as well as other faculty, Graduate Assistants, and Teaching Assistants, are mandatory reporters. This means that we are obligated to report gender-based violence that has been disclosed to us to the Institutional Equity Office. This includes disclosures that occur in: class discussion, writing assignments, discussion boards, emails and during Student/Office Hours. You may also choose to report directly to the Institutional Equity Office. After a report is filed, the Title IX Coordinator will reach out to provide resources, support, and information and the reported information will remain private. For more information regarding the University’s Title IX Grievance procedures, reporting, or support measures, please visit [Institutional Equity Office](https://www.ou.edu/eoo)at 405-325-3546.

### Reasonable Accommodation Policy

The University of Oklahoma (OU) is committed to the goal of achieving equal educational opportunity and full educational participation for students with disabilities. If you have already established reasonable accommodations with the Accessibility and Disability Resource Center (ADRC), please [submit your semester accommodation request through the ADRC](https://www.ou.edu/adrc/students/adrc-registered-students/accommodation-request) as soon as possible and contact me privately, so that we have adequate time to arrange your approved academic accommodations.

If you have not yet established services through ADRC, but have a documented disability and require accommodations, please complete [ADRC’s pre-registration form](https://forms.office.com/pages/responsepage.aspx?id=neB9nDSQwUS0YsRk_s4gSiXtB4DC5XxJhwAGd7Un1f5UNFU2WDE3UEVENTFIMkgyWFkzV0lGM1NPVCQlQCN0PWcu) to begin the registration process.  ADRC facilitates the interactive process that establishes reasonable accommodations for students at OU.  For more information on ADRC registration procedures, please review their [Register with the ADRC](https://www.ou.edu/adrc/about/registering-with-the-adrc) web page.  You may also contact them at (405)325-3852 or [adrc@ou.edu](mailto:adrc@ou.edu), or visit [www.ou.edu/adrc](http://www.ou.edu/adrc) for more information.

Note: disabilities may include, but are not limited to, mental health, chronic health, physical, vision, hearing, learning and attention disabilities, pregnancy-related.  ADRC can also support students experiencing temporary medical conditions.

### Religious Observance

It is the policy of the University to excuse the absences of students that result from religious observances and to reschedule examinations and additional required classwork that may fall on religious holidays, without penalty.

[[See Faculty Handbook 3.15.2]](https://apps.hr.ou.edu/FacultyHandbook/#3.15.2)

### Adjustments for Pregnancy/Childbirth Related Issues

Should you need modifications or adjustments to your course requirements because of documented pregnancy-related or childbirth-related issues, please contact the Accessibility and Disability Resource Center at 405/325-3852 and/or the Institutional Equity Office at 405/325-3546 as soon as possible. Also, see the Institutional Equity Office [FAQ on Pregnant and Parenting Students’ Rights](https://www.ou.edu/content/dam/eoo/documents/faqs/faqs-pregnant-and-parenting-students.pdf) for answers to commonly asked questions.

### Final Exam Preparation Period

Pre-finals week will be defined as the seven calendar days before the first day of finals. Faculty may cover new course material throughout this week. For specific provisions of the policy please refer to OU’s [Final Exam Preparation Period policy](https://apps.hr.ou.edu/FacultyHandbook#4.10).

### Emergency Protocol

During an emergency, there are official university [procedures](https://www.ou.edu/campussafety/policy-and-procedures) that will maximize your safety.

**Severe Weather:** If you receive an OU Alert to seek refuge or hear a tornado siren that signals severe weather.

1. Look for severe weather refuge location maps located inside most OU buildings near the entrances.
2. Seek refuge inside a building. Do not leave one building to seek shelter in another building that you deem safer. If outside, get into the nearest building.
3. Goto the building’s severe weather refuge location. If you do not know where that is, go to the lowest level possible and seek refuge in an innermost room. Avoid outside doors and windows.
4. Get in, Get Down, Cover Up
5. Waitfor official notice to resume normal activities.

Additional [Weather Safety Information](https://www.ou.edu/campussafety/divisions#management) is available through the Department of Campus Safety.

### The University of Oklahoma Active Threat Guidance

### The University of Oklahoma embraces a Run, Hide, Fight strategy for active threats on campus. This strategy is well known, widely accepted, and proven to save lives. To receive emergency campus alerts, be sure to update your contact information and preferences in the account settings section at [one.ou.edu](http://one.ou.edu/).

### RUN: Running away from the threat is usually the best option. If it is safe to run, run as far away from the threat as possible. Call 911 when you are in a safe location and let them know from which OU campus you’re calling from and location of active threat.

### HIDE: If running is not practical, the next best option is to hide. Lock and barricade all doors; turn of all lights; turn down your phone’s volume; search for improvised weapons; hide behind solid objects and walls; and hide yourself completely and stay quiet. Remain in place until law enforcement arrives. Be patient and remain hidden.

### FIGHT: If you are unable to run or hide, the last best option is to fight. Have one or more improvised weapons with you and be prepared to attack. Attack them when they are least expecting it and hit them where it hurts most: the face (specifically eyes, nose, and ears), the throat, the diaphragm (solar plexus), and the groin.

### *Please save OUPD’s contact information in your phone.*

### NORMAN campus:  *For non-emergencies call (405) 325-1717. For emergencies call (405) 325-1911 or dial 911.*

### TULSA campus:*For non-emergencies call (918) 660-3900. For emergencies call (918) 660-3333 or dial 911.*

### Fire Alarm/General Emergency

If you receive an OU Alert that there is danger inside or near the building, or the fire alarm inside the building activates:

1. *LEAVE* the building. Do not use the elevators.
2. *KNOW* at least two building exits
3. *ASSIST* those that may need help
4. *PROCEED* to the emergency assembly area
5. *ONCE safely outside, NOTIFY first responders of anyone that may still be inside building due to mobility issues.*
6. *WAIT* for official notice before attempting to re-enter the building.

[*OU Fire Safety on Campus*](https://vimeo.com/125093634)

### Office of Access and Opportunity’s Belonging Statement

Why You Belong at the University of Oklahoma: The University of Oklahoma, fosters an inclusive culture of respect and civility, belonging, and access, which are essential to our collective pursuit of excellence and our determination to change lives. The unique talents, perspectives, and experiences of our community enrich the learning, and working environment at OU, inspiring us to harness our innovation, creativity, and collaboration for the advancement of people everywhere.

### Course Reflection Survey

You’ll receive a Course Reflection Survey at the end of each semester for each course that you are enrolled in. I strongly encourage you to complete this survey. Your feedback can help me adjust my class for future semesters to help other students be successful. Your feedback is confidential, and I will only receive it after final grades are due. Course Reflection Survey results may also factor into teaching evaluations and annual performance reviews and are shared with department and program chairs.

### Copyright Statement

Sessions of this course may be recorded or live-streamed. These recordings are the intellectual property of the individual faculty member and may not be shared or reproduced without the explicit, written consent of the faculty member. In addition, privacy rights of others such as students, guest lecturers, and providers of copyrighted material displayed in the recording may be of concern. Students may not share any course recordings with individuals not enrolled in the class or upload them to any other online environment.

## Tentative Schedule (Subject to Change):

|  |  |
| --- | --- |
| Week | Topic |
| 0 | Understanding the Computing Devices and Digital Forensics; |
| 1 | Digital Evidence and Data Acquisition; |
| 2 | Processing Crime and Incident Scenes; |
| 3 | Current Digital Forensics Tools; |
| 4 | Recovering Graphics Files: Control Plane; |
| 5 | Digital Forensics Analysis and Validation; |
| 6 | Virtual Machine Forensics Live Acquisitions and Network Forensics; |
| 7 | Email and Social Media Investigations; |
| 8 | Mobile Device Forensics; |
| 9 | Spring Vacation; |
| 10 | Cloud Forensics; |
| 11 | Report Writing for HighTech Investigations; |
| 12 | Expert Testimony in Digital Investigations; |
| 13 | Ethics for the Expert Witness; |
| 14 | Advanced Topics; |
| 15 | Project Presentation; |