MIDWESTERN STATE UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE

CMPS 5363/4663: Computer Forensics

Summer semester 2023

Instructor:	Dr. Nelson L. Passos	
Office	Bolin Science Hall 126B	
Office phone:	397-4129	
E-mail:	nelson.passos@msutexas.edu	
Webpage:	cs.msutexas.edu/~passos	
Office Hours:	MWTR	8:00 – 10:00 am
Class Hours:	MWTR	10:10 am - BO 320

Course Description:

Study of techniques used to identify attacks to computer systems and recover data to be used as evidence in any sort of investigation. Includes an introduction to criminal forensics, evaluation of security flaws, network attacks, information hiding, and protection tools. It also includes an introduction to PowerShell scripts and data communication.

Prerequisites:

Minimum grade of C in CMPS 2084 and CMPS 2143 or CMPS 3013

Text book:

Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 7, by Harlan Carvey.

Additional requirements:

Administrator access to a Windows system (version 7, 8, 10 or 11)

CMPS 5363: graduate students will be required to conduct research, analyze, run an experiment with PowerShell commands used as computer forensics tools.

CMPS 4663: undergraduate students will be required to report on testing a tool available on Microsoft sysinternals website or the use of an EZ tool.

Grading:

Tests and Final Exam:	20 %
Homeworks:	20 %
Project:	15 %
Class Participation:	5 %

Final grading letter:

90 to 100 pts = A, 80 to 89.99 pts = B, 70 to 79.99 pts = C, 60 to 69.99 pts = D, other = F

Additional and important information:

All students should refer to the current MSU Students Handbook and Activities Calendar for university policies related to class attendance, academic dishonesty, students responsibilities, rights and activities.

Disability needs: Inform the instructor if you are a student with a disability and need accommodations for this class.

Cell phones, etc.: Use of any electronic device is not allowed in the classroom. Exceptions must be approved by the instructor.

Student drops: If you wish to drop this course you must first contact your instructor. All students-initiated drops must be processed by **July 27, 2023**.

Attendance: Students are expected to attend all meetings of the classes in which they are enrolled. Attendance is rewarded by the participation points in the grading criteria.

Campus Carry: Senate Bill 11 passed by the 84th Texas Legislature allows licensed handgun holders to carry concealed handguns on campus, effective August 1, 2016. Areas excluded from concealed carry are appropriately marked, in accordance with state law. For more information regarding campus carry, please refer to the University's webpage on Campus Carry at https://msutexas.edu/police/policies-laws/index.php. If you have questions or concerns, please contact Interim MSU Chief of Police at steven.callarman@msutexas.edu.

Active Shooter: The safety and security of our campus is the responsibility of everyone in our community. Each of us has an obligation to be prepared to appropriately respond to threats to our campus, such as an active aggressor. Please review the information provided by MSU Police Department regarding the options and strategies we can all use to stay safe during difficult situations. For more information, visit Safety / Emergency Procedures. Students are encouraged to watch the video entitled "*Run. Hide. Fight.*" which may be electronically accessed via the University police department's webpage: *"Run. Hide. Fight."*

Assignments: Assignments will be made as scheduled and are expected to be completed by the specified due date. Grades will be given to the assignments handed in on time. Late assignments will be accepted until one class past the due date, however will have their maximum grade reduced by twenty points. Any assignment turned in after that period or not done will be graded zero points. Students in this course must demonstrate their competency in fundamentals math skills through homework assignments and tests.

Assistance: Please contact your instructor for extra help during this course. This includes class material clarification, expected absences from class due to any personal problem, etc.

Academic Honesty: The Department of Computer Science had adopted the following policy related to cheating (academic misconduct). The policy will be applied to all instances of cheating on assignments and exams as determined by the instructor of the course.

- 1st instance of cheating in a course: The student will be assigned a non-replaceable grade of zero for the assignment, project or exam. In addition, the student will receive a one-letter grade reduction in course.
- 2nd instance of cheating in a course: The student will receive a grade of F in course & immediately be removed from course.

All instances of cheating will be reported to the Department Chair and, in the case of graduate students, to the Department Graduate Coordinator. The MCOSME website provides information on the process for grade appeals or appeals of academic honesty sanctions. The Grade Appeal Checklist provides the timeline for appealing from the instructor to the next in line (dean of the college). The Academic Honesty Checklist describes the timeline for appealing from the instructor to the next in line (chair of department).

Testing Process: The Department of Computer Science has adopted the following policy related to testing:

- All bags, purses, electronics (turned off), books, etc. will be placed in the front of the room during exams, or in an area designated by the instructor.
- Unless otherwise announced by the instructor, nothing is allowed on the desk but pen/pencil/eraser and test papers.
- No student is allowed to leave the room during an exam and return
-

RECORDING OF CLASS LECTURES: Permission must be requested in writing & obtained from the instructor before recording of class lectures. If permission is granted, the recording may only be used by the student making the recording. Recordings may NOT be posted on any internet source without written permission of the instructor. Failure to adhere to the policy may result in removal from the course with a grade of F or other appropriate punishment.

Grades will be posted on D2L

Tentative agenda:

Jul 10-	Introduction to computer forensics - Ethics
Jul 11-	Fundamentals – Statistical data – Incident response
	Assignment #1
Jul 12-	History - Computer Security in the Enterprise
Jul 13-	File Systems – Introduction FAT and inodes
Jul 17-	File Systems – NTFS
	Assignment #2
Jul 18-	File Recovery – hidden data
Jul 19-	Network forensics – OSI and TCP/IP - addressing
	Assignment #3
Jul 20-	Perl and PowerShell – basic operations
Jul 24-	Perl and PowerShell - programming
Jul 25-	**Test # 1**
Jul 26-	Security incidents - logs Registry
Jul 27-	Hidden data – file signatures, ADS
	Assignment #4
Jul 31-	Steganography, recycle bin and prefetch files
Aug 1-	Rootkits and other clues - Scanners and Sniffers
Aug 2-	**Test # 2**
Aug 3-	E-mail headers
Aug 7-	Anticipating problems - policies
Aug 8-	Internal Systems
Aug 9-	Timeline
Aug 10-	**Final 10:10 AM**