FORENSIC SCIENCE

COURSE SYLLABUS
FSC 632- Foundations & Fundamentals of Digital Evidence
CRN: 2295- 3 CR HRS.
Fall 2024

Instructor:	Dr. Josh Brunty GASF, CHFI, SCERS, CFVT, CCME, MCFE	**Class Meets:**	MW 8:00-9:15AM
Office:	Forensic Science Ctr. W200G	**Classroom:**	WAEC 2237
Phone:	304-691-8962	**Office Hours:**	MWF 0930-1100hrs & 1230PM-2PM
Email:	josh.brunty@marshall.edu		Book a Teams Meeting with Me

Course Description (from catalog):

The course provides fundamental information to lay the foundation for the Digital Forensics Area of Emphasis. A range of topics includes laws and regulations relating to stored digital data, quality assurance and ethics in a digital laboratory, basic terminology, computer hardware and various storage media, software, including operating and file systems, and basics concepts of computer security. The course is taught primarily in a lecture format. Class discussions and participation in practical exercises supplement lectures.

More Description:

This course will give a fundamental foundation for students new to the digital forensics field. This course will discuss what digital forensics is, the methodologies used, key technical concepts, and the tools needed to perform examinations. Details on digital forensics for computers, networks, the internet, the cloud, and mobile devices are also discussed.

Course Format:

Class will meet on Monday and Wednesday each week from 8-9:15AM in WAEC 2237 (Advanced Cyber Forensics & Security Laboratory) unless otherwise specified by the instructor or course schedule. Materials will be presented using lectures, in-class discussions, and class projects and presentations. Students will be expected to attend class and participate in class discussions, complete written assignments, and take in-class quizzes and exams.

Required Texts, Additional Reading, & Other Materials:

Required texts:

- Easttom, C. (2021). *Digital Forensics, Investigation, and Response. 4th Edition.* Burlington, MA: Jones and Bartlett Learning. ISBN: 9781284226065

Assigned readings are an essential component of this course and provide students with a baseline of knowledge that will be expanded upon through more detailed and complex in-class lectures and discussions. Students will be required to complete assigned readings prior to the class period in which the material will be discussed. Supplemental course materials (e.g., handouts, PPTs, reading assignments, etc.) will be posted to the MUOnline (Blackboard) and a course OneDrive link (https://bit.ly/de-foundations-onedrive) to share in-class labs and other large files.

Desired Objectives/Outcomes:

Course Student Learning Outcome	How Practiced in This Class	How Assessed in This Course
Provide core knowledge necessary for students to have a basic understanding of Digital Forensics & the value of digital evidence in solving crimes **(objective)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3
Students will be able to evaluate digital devices for evidence important in solving criminal & civil cases **(expectation)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3
Provide concepts & knowledge to students who decide to further their understanding of Digital Forensics by pursuing this area of emphasis and, possibly, as a future career **(objective)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3
Students will actively participate & discuss the topics at hand during class and implement them in in-class lab exercises **(expectation)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3
Students will gain an understanding of laws governing search & seizure of digital evidence & laws that govern access to stored data will be analyzed. Factors that allow & impact the admissibility of evidence will be explored & debated **(objective)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3

Students will gain understanding that federal & state laws are in flux & court decisions related to privacy and the availability of digital data to law enforcement is currently being decided. State & county courts differ on such interpretations so students will be expected to understand how these laws will impact cases involving digital evidence **(expectation)**	In-class lecture & hands on laboratory exercises.	Classroom Discussion, Laboratory Exercises, Exams 1-3

University Policies

By enrolling in this course, you agree to the University Policies. Please read the full text of each policy (listed below) by going to MU Academic Affairs: University Policies. (URL: http://www.marshall.edu/academic-affairs/policies/)

- Academic Dishonesty Policy
- Academic Dismissal Policy
- Academic Forgiveness Policy
- Academic Probation and Suspension Policy
- Affirmative Action Policy
- Dead Week Policy
- D/F Repeat Rule
- Excused Absence Policy for Undergraduates
- Inclement Weather Policy
- Sexual Harassment Policy
- Students with Disabilities (Policies and Procedures)
- University Computing Services Acceptable Use Policy

Generative Artificial Intelligence (AI) Policy for Use in this Course

Students are allowed, and even encouraged, to use Generative AI on any assignment in this course with the appropriate citation. Keep in mind that any content produced by generative AI can "hallucinate" (produce false information), so students are responsible for ensuring the accuracy of any AI-generated content. For information on citing AI, please see MU Library's citation website (URL: https://libguides.marshall.edu/plagiarism-AI/cite). Students should not use generative AI in any way that would violate the Student Code of Conduct (URL: https://www.marshall.edu/student-conduct/).

Health and Safety Information

All members of the Marshall University community are expected to always observe health and safety protocols. This includes general health and safety protocols as well as specific protocols that might emerge in response to community and campus health conditions.

Campus Carry Policy

University Policy, UPGA-12 (Campus Carry Policy) derives its authority from West Virginia State law, including the Campus Self-defense Act (W. Va. Code § 18B-4-5b). It pertains to the exercise of Concealed Carry on Marshall University's campus, except in designated areas, by individuals with a valid permit to Conceal Carry.

Individuals who choose to Conceal Carry are responsible for knowing and understanding all applicable federal, state, and local laws and Marshall University Board of Governors Rules, University Policies, and Administrative Procedures. University Policy, UPGA-12 applies to areas of campus and buildings that are directly under the possession or control of Marshall University.

Concealed Handguns are not observable to others and must be holstered and concealed on the body of the permit holder or in a personal carrier, such as a backpack, purse, or other bag that remains under the exclusive and uninterrupted control of the permit holder. This includes wearing the personal carrier with a strap, carrying or holding the personal carrier, or setting the personal carrier next to or within your immediate reach at all times. If your participation in class activities impedes your ability to maintain constant control of your Handgun, please make alternate arrangements prior to coming to class.

Attendance Policy and Make-up Work:

In-class participation is an essential component of this course and students will be expected to attend each class unless they have a valid university-approved excuse (see university excused absence policy). I will be happy to meet with students who miss class with a valid excuse to discuss course material and how missed work can be made up. However, I will not re-lecture to students who miss class during office hours, and it will be the students' responsibility to catch up on missed material (e.g., readings, in- class exercises, etc.).

Assignment Submission & Late Policy:

All homework & in-class issued assignments/labs must be turned in on the specified due date. Except under special circumstances with written justification, assignments turned in after the due date will be penalized with a 10% reduction in points for each day late, including Saturdays and Sundays (i.e., one day late = 90% highest possible score, two days late = 80% highest

possible score, etc.). Assignments will not be accepted more than one week after the original due date.
In-class quizzes and lab assignments will not be accepted late (i.e., there will be no opportunity to make up any missed in-class quizzes or lab exercises), except under special circumstances with written justification and prior approval. If your absence is unexcused, you will not be given an opportunity to make up any missed in-class assignments. In order to receive an excused absence, you must visit the office of academic affairs to obtain a written excused absence form. All virtual laboratory assignments are generally due on **Friday's at 11:59PM**. These due dates are outlined in the course schedule below.

Course Requirements & Grading Policy:

Students will be evaluated in this course based on their performance in the following categories:

Participation – Students will be required to complete several instructor-led, hands-on lab exercises during class. These labs will be essential for demonstrating how to conduct digital forensics examinations in a laboratory environment. Lab exercises must be handed in during class. Late or make-up labs will not be accepted, except under special circumstances with written justification.

Examinations – There will be three (3) written examinations that will be administered during specified class periods this semester (midterm and final examination). Any student who misses an exam due to an unexcused absence will receive a 0% for that exam (see make-up exam policy).

The above categories will be graded as follows:

Participation	10%
Exam #1	30%
Exam #2	30%
Exam #3	30%
Total	**100%**

Evaluation Category	**Your Score (Out of 100)**	**Weight**	**Contribution to Final Grade**
Participation		X .10 =	
Exam #1		X .30 =	
Exam #2		X .30 =	
Exam #2		X .30 =	
Final letter grades are calculated using the following scale: 90-100 A 80-89 B 70-79 C 60-69 D Below 60 F		**Final Grade (out of 100)**	

This class will employ a weighted grading system. To determine your grade in this course, fill in your percentage score for each evaluation category below, multiply each score by its weight, and then add the values in the final grade column to find your overall grade out of 100. In addition to handing graded assignments back to you in class, I will post grades for individual assignments and exams on blackboard. However, please remember that you **must** use the weighted grading system shown below to determine an accurate portrayal of your overall course grade. I am happy to meet with you to discuss your course progress/grade during office hours throughout the semester.

There will be a number of out-of-class labs and hands-on assignments as part of this course. As such, you will be given 24/7 access privileges to the Digital Forensics Laboratory (WAEC 1232) to work on assignments and practice labs when classes aren't in session. Open lab schedules will be posted during the first or second week of classes. If you do not have an RFID-enabled access card you can obtain your first one free-of-charge from the campus ID office located on the first floor of Drinko Library. You can also visit the ID office to enable RFID access on a companion mobile device (i.e. Apple Watch or iPhone) if compatible. In addition, you will also need to complete the required COS IT Conduct form before the end of the first week of classes online by visiting https://netapps.marshall.edu/cosweb/agreements/?a=cositconduct Usage of the computers and

course files will not be permitted until the online form is completed.

Communication:

I will post course content Teams (e.g., syllabus, assignments, readings, etc.), so be sure to check for new materials regularly. MUOnline & your MU email address will be used to make any general announcements, last minute schedule changes, etc. I recommend that you monitor your MU email and Teams at least once a day. Also, I will only respond to emails that you send me from your official MU email address – it is the only way for me to be sure that I am responding to you (and not someone else pretending to be you).

Classroom Learning Environment:

To foster the best possible environment for learning, we will follow "Brunty's Maxims" They are as follows:

- Don't Lie…
- Don't Cheat…
- Don't Steal…
- Don't play on your cellphone unless directed to do so.
- Don't have conversations that distract the class.
- Don't disparage other students- Treat everyone with respect.
- Don't be late for class.
- ALWAYS be professional. Take advantage of your time in here. Ask questions. Participate

Students who violate these maxims will be asked to leave class.

Academic Calendar

For beginning, ending, and add/drop dates, see the Marshall University Academic Calendar (URL: http://www.marshall.edu/academic-calendar/)

Course Schedule and Due Dates:

NOTE: This is a tentative schedule and it may change as the class progresses. Chapter readings should be completed prior to class.

Week 1- Introduction to Forensics (8/19-8/23)	
Required Readings	• Chapter 1- Introduction to Forensics (pp. 1-36)
Week 2- Forensic Methods & Labs (8/26-8/30)	
Required Readings	• Chapter 3- Forensic Methods & Labs (pp. 65-87) • Chapter 3 Supplemental Readings
Week 3- Collecting, Seizing, and Protecting Evidence. (9/2-9/6)	
Required Readings	• Chapter 4- Collecting, Seizing, and Protecting Evidence (pp. 91-118) • Chapter 4 Supplemental Readings
Note	• No Class 9/2- Labor Day
Week 4- Recovering Data (9/9-9/13)	
Required Readings	• Chapter 6- Recovering Data (pp. 151-171) • Chapter 6 Supplemental Readings
Week 5- Overview of Computer Crime & Incident Response (9/16-9/20)	
Required Readings	• Chapter 2- Overview of Computer Crime (pp. 39-63) • Chapter 7- Incident Response (pp. 173-189) • Chapter 2 & 7 Supplemental Readings
Week 6- Exam #1 & Windows Forensics (9/23-9/27)	
Required Readings	• Chapter 8- Windows Forensics (pp. 193-209) • Chapter 8 Supplemental Readings
Note	• Exam #1 Monday 9/23 (Covers Chapters 1-4, 6 & 7)

Week 7- Windows Forensics Cont. (9/30-10/4)	
Required Readings	• Chapter 8-Windows Forensics (pp. 210-222) • Chapter 8 Supplemental Readings (Cont.)
Week 8- Linux Forensics (10/7-10/11)	
Required Readings	• Chapter 9- Linux Forensics (pp. 223-252) • Chapter 9 Supplemental Readings
Week 9- Mac OS Forensics (10/14- 10/18)	
Required Readings	• Chapter 10- Mac OS Forensics (pp. 253-270) • Chapter 10 Supplemental Readings
Week 10- Email Forensics (10/21- 10/25)	
Required Readings	• Chapter 11- Email Forensics (pp. 271-289)
Week 11- Exam #2 & Mobile Forensics (10/28-11/1)	
Required Readings	• Chapter 12- Mobile Forensics (pp. 291-312) • Chapter 12 Supplemental Readings
Note	• Exam #2 10/23 (Covers Chapters 8-10)
Week 12- Network Forensics (11/4- 11/8)	
Required Readings	• Chapter 13- Network Forensics (pp. 313-342) • Chapter 13 Supplemental Readings
Week 13- Memory Forensics (11/11- 11/15)	
Required Readings	• Chapter 14- Memory Forensics (pp. 343-360) • Chapter 14 Supplemental Readings

Week 14- Trends and Future Directions (11/18-11/22)	
Required Readings	• Chapter 15- Trends & Future Directions (pp. 361-374) • Chapter 15 Supplemental Readings • Exam #3 Review (11/20)
Fall Break- No Classes (11/25 - 11/29)	
Week 15- Dead Week & Mock Digital Scene (12/2 -12/6)	
	• Mock Digital Crime Scene @ Marshall Crime Scene House (CSH) • Time & Date TBA
Week 16- Final Exam Week- Exam #3- (12/9 -12/13)	
	• Exam #3 Covers Chapters 12-15 & Supplemental Readings ○ Exam Time: Monday, December 9th 8:00AM-10:00AM

About Your Professor:

I am an Associate Professor in the Department of Criminal Justice, Criminology, & Forensic Sciences at Marshall University and have been since 2012. My teaching & research expertise is in digital forensics, mobile device forensics, network forensics, and multimedia forensics. I currently serve as Head Coach of the US Cyber Team. I am a Fellow of the American Academy of Forensic Sciences (AAFS), an appointed member & Executive Secretary of the NIST Organization of Scientific Area Committee (OSAC) on Digital Evidence, & a member of ASTM E30 Committee on Forensic Sciences. I am also an Editorial Board Member of the Journal of Forensic Sciences & Elsevier's Forensic Science International: Digital Investigation journal. Prior to entering academia, I managed digital forensic casework & research laboratories at the Marshall University Forensic Science Center and also worked as an examiner with the West Virginia State Police's Digital Forensic Unit at the Marshall University Forensic Science Center. I also worked as a Technical Assessor for the ANAB assessing various digital forensics laboratories throughout the US seeking ISO accreditation. I am a LEVA Certified Forensic Video Technician (CFVT), a graduate of the FLETC Seized Computer Evidence Recovery Specialist (SCERS) program, a certified Computer Hacking Forensic Investigator (CHFI), a Magnet Certified Forensics Examiner (MCFE), a GIAC Advanced Smartphone Analyst (GASF), & a Cellebrite Certified Mobile Examiner (CCME).

A more detailed background, including my past work & research, can be found at: www.solo.to/joshbrunty

Feel free to follow me on Twitter @joshbrunty & on LinkedIn