COURSE SYLLABUS
FSC 609- Network Forensics
CRN: 4316- 3 CR HRS.
Fall 2024

Instructor:	Dr. Josh Brunty GASF, CHFI, SCERS, CFVT, CCME, MCFE	**Class Meets:**	M 4:00-6:20PM
Office:	Forensic Science Ctr. W200G	**Classroom:**	WAEC 1232
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):

Teaches the basics of how computers and networks function, how they can be involved in crimes as well as used as a source of evidence.

More Description:

Although many concepts of network forensics are similar to those of any other digital forensic investigation, the network in of itself presents many nuances that require special attention. This course will teach digital forensics and incident response to network-based evidence. This course will also acclimate the student to the basic tools and techniques of the trade.

Course Format:

Class will meet on Monday each week from 4:00PM-6:20PM, 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 laboratory assignments, and take in-class quizzes and exams.

A midterm & final examination, along with a Final Practical Project will also be given in the course.

Required Texts, Additional Reading, & Other Materials:

- Davidoff, S., Ham, J. (2012) *Network Forensics- Tracking Hackers Through Cyberspace*. ISBN: 0132564718
- Brunty, J., Helenek, K. (2012). *Social Media Investigation for Law Enforcement.* ISBN: 1455731358

- You will be required to purchase a lab/code directly from the lab provider in order to complete the virtual lab exercises within course. These Linux virtual machines & labs are entirely HTML5-based and require no plugins to run. These labs can be completed from anywhere. Google Chrome is the supported browser for this lab-based environment. The Course ID for this lab course is: **RAFYVYRPWK**.
- 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, reading assignments, etc.) will be posted to the and a course OneDrive link (http://bit.ly/network-forensics-onedrive). Other content will be shared in MUOnline: http://www.marshall.edu/muonline

Desired Objectives/Outcomes:

This course is designed to build on the material learned foundational forensic courses and apply those concepts to a network environment. This course places a strong emphasis on digital forensic procedures, digital forensic tools, and legal issues relating to digital forensics in a network environment. This course uses advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators. Upon completion of this Network Forensics course, students will be able to:

Course Student Learning Outcome	How Practiced in This Class	How Assessed in This Course
Explain the various components of computer networks.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
Explain the significance of computer networks (i.e. internet, LAN, WAN) in an investigation.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
Convey privacy, security, and legal issues on computer networks and the internet.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
Utilize methods used to prevent, detect, and investigate network and internet-related crimes	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam

Collect and examine various types of digital evidence from computers and computer networks using forensically- sound techniques and/or technologies.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam

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.

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** via Teams. These due dates are outlined in the course schedule below & also available in Teams.

All electronic submissions MUST follow this file naming convention:
FSC609_LastName_FirstInitial_Assignment Name.doc ("FSC609_brunty_j_lab1.docx")

Course Requirements & Grading Policy:

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

Laboratory Exercises (45%) – Students will be required to complete fifteen (15) hands-on virtual lab exercises over the course of the semester. These labs will be essential for demonstrating how to conduct network forensics examinations and other digital forensics tasks that are commonly used in digital forensics and incident response. Laboratory exercises must be turned in via MUOnline on the date specified. Late or make-up lab exercises will not be accepted, except under special circumstances with written justification.

Final Practical Project (45%)- This examination will be handed out midway through the semester schedule and will be based upon the techniques covered in the course and completed in lab exercises. Students will be required to examine a mock case and prepare and submit a case report on the findings and methodologies of the case. Students will also be required to present the findings in their report to the professor and fellow student cohorts during a class period specified by the instructor.

In-Class Attendance/Participation (10%) – This portion will include active participation and attendance in in-class, instructor led lectures and exercises. Participation in these activities will significantly help in the completion of both virtual labs and Final Project exercises.

The above categories will be graded as follows:

Laboratory Exercises	45%
Final Practical Project	45%
In-Class Attendance/Participation	10%
Total	**100%**

Evaluation Category	Your Score (Out of 100)	Weight	Contribution to Final Grade
Laboratory Exercises (average)		X .45 =	
Practical Final		X .45 =	
In-Class Attendance Participation		X .10 =	
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 here. Ask questions. Participate.*

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

Course Schedule and Due Dates:

NOTE: This is a tentative schedule and it may change as the class progresses and/or classes are cancelled. Lab Projects, etc. are listed in the notes section. Virtual Labs & end of module quizzes must also be completed by 11:59PM on the Friday of the week as they appear on the schedule below.

The official MU Academic Calendar can be found at: https://www.marshall.edu/academic-calendar/

August 19th **Module 1: Introduction to Network Forensics**	
Required Readings	• Davidoff Chapter 1 (pp. 3-22)
Lab	• No Lab Due
August 26th **Module 2: Technical Fundamentals**	
Required Readings	• Davidoff Ch. 2 (pp. 23-44)
Lab(s)	• Lab #1- TCP/IP Utilities Lab
Week of 9/2 – 9/6 - No Class- Labor Day	
Week of 9/9 – 9/13 **Module 3- Network Forensics- Acquisition/Analysis/Examination**	
Required Readings	• Davidoff Ch. 3 (pp. 45-72)
Lab	• No Lab Due

Week of 9/16 – 9/20 **Module 3 Cont.- Network Forensics- Introduction to Packet Capture/Analysis using TCPDump & Wireshark**	
Required Readings	• Watch Hack3rCon “Intro to TCPdump & Wireshark” Video
Lab	• Lab #2- Performing A Denial of Service Attack from the WAN • Lab #3- Capturing & Analyzing Traffic Using a Sniffer
Week of 9/23 – 9/27 **Module 4- Network Forensics- Traffic Analysis**	
Required Readings	• Davidoff Ch. 4 (pp. 73-157) • Watch Hack3rCon “Network Forensics Using SANS SIFT” Video
Lab	• Lab #4- The OSI Model • Lab #5- TCP/IP Protocols- The Core Protocols • Lab #6- TCP/IP Protocols- The Other Key Protocols
Week of 9/30 – 10/4 **Module 4- Network Forensics- Traffic Analysis Cont.**	
Required Readings	• Davidoff Ch. 5 (pp. 159-196)
Lab	• Lab #7- Deep Dive in Packet Analysis- Using Wireshark & Network Miner
Week of 10/7 – 10/11 **Module 5- Wireless Network Forensics**	
Required Readings	• Davidoff Ch. 6 (pp. 199-255)
Lab	• Lab #8- Examining Wireless Networks
Week of 10/14 – 10/18 **Module 6- Event Log Forensics**	
Required Readings	• Davidoff Ch. 8 pp. 291-333
Note	• Lab #9- Log Analysis • Lab #10- Intrusion Detection Using Snort • Lab #11- Log Analysis in Linux & Splunk
Week of 10/21 – 10/25 **Final Project Briefing**	
Note	• No Class 10/17 • Final Project Briefing & Release (Thursday 10/19)
Week of 10/28 – 11/1 **Module 7- Threat Hunting Part I- Static & Dynamic Malware Analysis**	
Required Readings	• Davidoff Ch. 12 (pp. 461-516)
Lab	• Lab #12- Static & Dynamic Malware Analysis

Week of 11/4 – 11/8 **Module 8- Threat Hunting Part II- Malicious Indicators & Network Compromise**	
Required Readings	• Memory Forensics Lecture/PowerPoint
Lab	• Lab #13- Finding Malicious Indicators • Lab #14- Investigating & Network Compromise
Note	• Final Report ***Rough Draft*** Due (Friday 11/8) @ midnight
Week of 11/11 – 11/15 **Module 9- Legal Issues in Network Forensics**	
Required Readings	• Brunty Ch. 4 • Electronic Essentials Webinar (NCSTL)- MUOnline
Lab	• No Lab Due

Week of 11/18 – 11/22 **Module 10- Communication Artifacts**	
Required Readings	• Communication Artifacts Handouts & Slides • Brunty Ch. 1,2,3 & 5
Lab	• Lab #15- Communication Artifacts
Fall Break No Class 11/25 – 11/29	
Week of 12/2 – 12/6) **Dead Week**	
Note	• No Formal Class Meetings
Week of 12/9 – 12/13 **Final Exam Week**	
Note	• Final Practical Project DUE Sunday 12/8 @ Midnight via MUOnline • Final Project Class Meeting & Debrief Monday 12/9 at 4PM in WAEC 1232

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