DIGITAL FORENSICS
INFORMATION ASSURANCE

COURSE SYLLABUS
FSC 609- Network Forensics
CRN: 2394-3 CR HRS.

Instructor:	Prof. Josh Brunty	**Class Meets:**	TR 8:00-9:15AM
Office:	WAEC 2001	**Classroom:**	WAEC 1232
Phone:	304-696-5602	**Office Hours:**	MWF 10:00-11:00AM
Email:	josh.brunty@marshall.edu		TR 9:30-11:00AM

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:

This three (3) credit hour Network Forensics course will provide an overview of the foundations of computer network security and discuss how criminals are using computers to commit crimes. This course will introduce the student to the principles of computer network communications & provide an overview of computer information security and digital forensics within a network and internet environment.

Course Format:

Class will meet on Tuesday and Thursday each week from 8:00-9:15AM, 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.

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 also be required to purchase a lab access code from the Marshall University Bookstore in order to complete the virtual laboratory exercises and access the Kali Linux & Windows sandbox virtual machines (VM's) used within course. These virtual labs & sandbox VM's are entirely HTML5-based and require no plugins to run. These labs can be completed from anywhere. We will also use these sandbox VM's for in-class practice labs. Google Chrome is the supported browser for this lab-based environment.

Assigned readings and laboratory exercises 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, lab exercises, etc.) will be posted to the 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 listed below. Please read the full text of each policy by going to www.marshall.edu/academic-affairs and clicking on "Marshall University Policies." Or, you can access the policies directly by going to http://www.marshall.edu/academic-affairs/policies/

Academic Dishonesty/ Excused Absence Policy for Undergraduates/ Computing Services Acceptable Use/ Inclement Weather/ Dead Week/ Students with Disabilities/ Academic Forgiveness/ Academic Probation and Suspension/ Academic Rights and Responsibilities of Students/ Affirmative Action/ Sexual Harassment

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 labs, etc.).

Assignment Submission & Late Policy:

Laboratory Exercises and other in-class labs 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 electronic submissions MUST follow this file naming convention:
DFIA462_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 (40%) – Students will be required to complete ten (10) hands-on 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 commony 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.

Practical Midterm Examination (20%)- This examination will be handed out 2 weeks prior to the due date in the schedule and will be based upon the material covered in the first half of the course. 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.

Exam #1- Written Midterm Examination (20%) – There will be written examinations that will be administered during at the midterm point of the semester (see schedule for exam date). This exam will cover materials of the first-half of the course. Any student who misses this exam due to an unexcused absence will receive a 0% for that exam (see make-up exam policy).

Exam #2- Written Final Examination (20%)- There will be a written final examination that will be given during finals week of the semester (see schedule for final exam date). This exam will be cumulative and cover all materials given over the course of the semester. Any student who misses this 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:

Laboratory Exercises	40%
Practical Midterm	20%
Exam #1	20%
Exam #2	20%
Total	**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.

<table>
<tr><th>Evaluation Category</th><th>Your Score (Out of 100)</th><th>Weight</th><th>Contribution to Final Grade</th></tr>
<tr><td>Laboratory Exercises (average)</td><td></td><td>X .40 =</td><td></td></tr>
<tr><td>Practical Midterm</td><td></td><td>X .20 =</td><td></td></tr>
<tr><td>Exam #1</td><td></td><td>X .20 =</td><td></td></tr>
<tr><td>Exam #2</td><td></td><td>X .20 =</td><td></td></tr>
<tr><td colspan="2">Final letter grades are calculated using the following scale:<table>
<tr><td>90-100</td><td>A</td></tr>
<tr><td>80-89</td><td>B</td></tr>
<tr><td>70-79</td><td>C</td></tr>
<tr><td>60-69</td><td>D</td></tr>
<tr><td>Below 60</td><td>F</td></tr>
</table></td><td><b>Final Grade (out of 100)</b></td><td></td></tr>
</table>

Communication:

I will post course content on MUOnline (e.g., syllabus, assignments, readings, etc.), so be sure to check for new materials regularly. Your MU e-mail address will be used to make any general announcements, last minute schedule changes, etc. I recommend that you monitor your MU email and MUOnline accounts 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.

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.

Date	Day	Topic	Notes
8/22	T	Module 1- Introduction to Network Forensics	Read Davidoff Ch. 1 Module 1 Lab
8/24	R	Module 1- Introduction to Network Forensics	
8/29	T	Module 2- Technical Fundamentals- Introduction to Networks & Networking Concepts	Read Davidoff Ch. 2 (pp. 23-44) Module 2 Lab
8/31	R	Module 2- Technical Fundamentals- Introduction to Networks & Networking Concepts	
9/5	T	Module 3- Network Forensics- Acquisition/Analysis/Examination	Read Davidoff Ch. 3 (pp. 45-72) Module 3 Lab #1
9/7	R		
9/12	T	Module 3- Network Forensics- Introduction to Wireshark	Watch Intro to TCPdump/Wireshark Video Module 3 Lab #2
9/14	R	Module 3- Network Forensics- Introduction to Wireshark	
9/19	T	**Conference Travel- No Class**	
9/21	R	Module 4- Network Forensics Traffic Analysis	Read Davidoff Ch. 4 (pp. 73-157) Module 4 Lab
9/26	T	Module 4- Network Forensics Traffic Analysis	Read Davidoff Ch. 5 (pp. 159-196)
9/28	R	Module 4- Network Forensics Traffic Analysis	
10/3	T	Module 5- Wireless Network Forensics	Read Davidoff Ch. 6

			(pp. 199-255) Module 5 Lab #1
10/5	R	Module 5- Wireless Network Forensics	
10/10	T	Module 5- Wireless Network Forensics (Search & Seizure Exercise)	Module 5 Lab #2
10/12	R	Module 5- Wireless Network Forensics (Search & Seizure Exercise)	
10/17	T	Exam #1	**Exam #1 (Midterm)- Covers chapters 1-5**
10/19	R	**Midterm Practical Distribution & Briefing**	
10/24	T	Module 6- Event Log Forensics	Read Davidoff Ch. 8 (pp. 291-333) Module 6 Lab
10/26	R	Module 6- Event Log Forensics	
10/31	T	Module 7- Malware Forensics	Read Davidoff Ch. 12 (pp. 461-516) Module 7 Lab
11/2	R	Module 7- Malware Forensics	
11/7	T	**Midterm Practical Presentations & Debriefing**	
11/9	R	Module 8- Legal Considerations in Network Forensics	Read Brunty Ch. 4
11/14	T	Module 9- Web/Internet Forensics	Read Brunty Ch. 1,2,3,5
11/16	R	Module 9- Web/Internet Forensics	
11/21	T	**Thanksgiving University Holiday- No Class**	
11/23	R	**Thanksgiving University Holiday- No Class**	
11/28	T	Module 10- Email Forensics	Module 10 Lab
11/30	R	Module 10- Email Forensics	
12/5	T	Exam #2 Review	
12/7	R	Exam #2 Review	
12/11	M	**Exam #2- Final Exam-** **Thursday 12/14 8:00AM-10:00AM**	**Exam #2 (Final)- Cumulative**