

Instructor		
Professor Josh Brunty, ACE, SCERS, CJHFI, CCME Office: Weisberg Applied Engineering Complex (WAEC) 2001 Office Phone: 304-696-5602 (takes messages) Dept. Fax: 304-696-6533 Email: josh.brunty@marshall.edu Office Hours: MWF 8:00-9:00AM, TR 9:30AM-11:00AM Twitter: @joshbrunty @MuDigForensics Facebook: Marshall Digital Forensics & Information Assurance		
Required Text(s)		
-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		
Recommended Texts		
None		
Course Description		
This three (3) credit hour Network Forensics (CRN# 2308) 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.		
Prerequisites		
FSC 632 & FSC 634 (recommended)		
Computer & Software Requirements		
For laboratory exercises outside of class, it is recommended that the student setup their own functioning Linux distribution (for this course we will be using and learning SIFT, the SANS Investigative Forensic Toolkit available at http://digital-forensics.sans.org/community/downloads). I would highly recommend that the student setup this Linux distribution on a portable virtual machine (i.e. VM on a portable hard drive) for better experiences in in and out-of-class lab exercises.		
All students are responsible for knowing the University Computing Services' Acceptable Use Policy available at http://www.marshall.edu/academic-affairs/?page_id=802		
Students will receive emails via Marshall email (Please setup your Marshall account(s) if you have not done so). E-mail will be used to make any general announcements, last minute changes, etc. It is mandatory that you monitor both your email at least once a day. PLEASE ONLY USE MY MARSHALL EMAIL ADDRESS FOR QUICK CORRESPONDENCE. Messages left on MUOnline or any other social media may result in delayed responses.		
Course 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.	Mod 1-2, 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.	Mod 2-6, Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
Convey privacy, security, and	In-class lecture & hands on	Mod 9, Classroom Discussion,

legal issues on computer networks and the internet.	laboratory exercises.	End of 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.	Mod 3-14, 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.	Mod 3-14, Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
A variety of methods will be used to evaluate learning of each of the above outcomes. These include: classroom discussion, in-class case studies and exercises, and in-class and out-of-class laboratory projects. This 4 hour Network Forensics course will meet every Tuesday and Thursday from 8:00AM-9:15AM in the Weisberg Applied Engineering Complex (WAEC) Room 1232 (Digital Forensics Lab). Our journey of knowledge will consist of lecture with accompanying lab projects. There will be one (1) midterm examination consisting of both a written and practical segment. The final exam will consist of a written and multiple choice practical segment that will be completed in class. Lectures and course materials will be available from MUOnline as they become available. You can log into the course website using your student credentials at the following address: www.marshall.edu/muonline		
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/?page_id=802 <i>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</i>		
Project Submission Guidelines		
The course includes a number of hands-on laboratory projects. All laboratory projects are due at the end of the next module week (Friday's at 11:59PM) on their due date and must be submitted through via MUOnline (unless otherwise noted by the instructor). NO LATE ASSIGNMENTS WILL BE ACCEPTED. These assignments will usually be distributed and due on Fridays (start of class). Please see the instructor if extenuating circumstances exist that may merit an extension or modification of the assignment. Please do not procrastinate in working on your assignments or trying to submit through MUOnline as many others have done in the past. If you wait until the last night to start on the project or the last minute to submit, chances are, you will fail. All electronic submissions MUST follow this file naming convention: <i>FSC609_LastName_FirstInitial_Assignment Name.doc ("FSC609_bruntj_j_project1.doc")</i> Assignments MUST be submitted in the format specified by the instructor for a given assignment. I WILL NOT accept projects submitted in non-approved formats or naming conventions (e.g. Open Office & proprietary formats).		

Assignments & projects must convey information in a clear, concise, and technical matter; hence obvious grammatical mistakes will be deducted. Projects will be available for download & submitted via MUOnline unless otherwise noted by the instructor.

All course assignments will:

- 1) Be completed on time
- 2) Meet guidelines and scoring rubrics for the assignment

Grading Policy

Student materials and grades will be returned as soon as graded to the student and can be viewed via MUOnline. Should you wish to appeal a grade, test question, etc, you need to follow this procedure. You should send an email to me. The title of the email must read "GRADE APPEAL – Assignment Name" (i.e. Midterm, Project 2, etc). The body of the email must include the question, question number, your answer, and why you think you deserve credit. For tests and quizzes in MUOnline, this should be done immediately after completion, before you leave class. You can copy and paste this information to make things simple. I will get back to you as soon as possible.

Grading

Final letter grades will be based on the following scale:

90-100	A
80-89	B
70-79	C
60-69	D
0-59	F

Percentage of grades will be distributed as follows:

Laboratory Projects	25%
Midterm Exam (Practical)	50%
Final Exam	25%

Example:

Midterm Practical (83%)	x .50= 41.5
Final Exam (88%)	x .25 = 22
Laboratory Projects (80%)	x .25 = 20

	83.5 (84% B)

End of Module Lab Exercises (25%)

There are laboratory exercises that are to be completed and submitted MUOnline at the end of each Module. These will be released at the end of the Module week and will be due the following week. The due dates for each lab exercise can be found in MUOnline. The Lab exercises themselves and instructions on how to complete them can be found within the assignment posted in MUOnline. Point value can vary based upon the complexity of the step and/or specifications of the lab exercise, but is generally 25 points per lab.

Midterm Practical (50%)

The "Midterm Practical" is a real-world, out-of-class case scenario that will gauge mastery of the material covered before midterm. Generally, the time-frame to complete the practical once distributed is 2-weeks and requires submission and presentation of your forensic "report." This report will not only be scrutinized by your professor, but you may be "cross-examined" on your case methodology and reporting. Don't fret, however, it's a great learning experience.

Final Exam (25%)

Your final exam will be taken during the week of finals and will be presented in a traditional multiple choice, T/F, fill in the blanks, short essay kind of written exam, with the exception that it will include a little more practical-based component(s). You will be given 2 hours to complete this exam and will cover comprehensively cover all modules in the course. The exact date of the final exam can be found in the schedule below. We will be reviewing for this exam and I will prepare a study guide to help with this exam.

CLASS SCHEDULE	Marshall University Dates/ Important Dates/Notes	WEEK CLASS DATE
NOTE: When projects are assigned for a week, the due date will be reflected within the posted assignment via MUOnline. It is expected of the student to submit the project to MUOnline prior to the due date/cutoff time (which is usually the beginning of class). Failure to do so will result in a zero for the project. Please see the instructor if extenuating circumstances exist that may merit an extension or modification of the assignment. Late, incomplete or poorly organized assignments will result in point deductions. The following outline delineates the tentative class schedule with topics to be addressed during the course. Please note this is a tentative schedule and it may change upon class progress:		
Week 1 (Modules 0 & 1) -Introduction to Network Forensics (Course Introduction) -Introduction to Network Forensics Programming Using Python	✓ Read Davidoff Ch. 1 ✓ Review Online Videos	Aug 22-26
Week 2 (Module 2) Technical Fundamentals-Introduction to Networking & Networking Concepts	✓ Read Davidoff Ch. 2 (pp. 23-44) ✓	Aug 29-Sept 2
Week 3 (Module 3) Network Forensics Acquisition/Analysis/Examination-Introduction	✓ Read Davidoff Ch. 3 (pp.45-72) ✓ September 5 (Monday)- Labor Day- No Class	Sept 5-9
Week 4 (Module 4) Network Forensics Acquisition/Analysis/Examination-Traffic Analysis	✓ Read Davidoff Ch. 4 (pp.73-157)	Sept 12-16
Week 5 (Module 5) Network Forensics Acquisition/Analysis/Examination-Statistical Flow Analysis	✓ Read Davidoff Ch. 5 (pp.159-196)	Sept 19-23
Week 6 (Module 6) Wireless Network Forensics	✓ Read Davidoff Ch. 6 (pp. 199-255)	Sept 26-30
Week 7 (Module 7) Malware Forensics	✓ Read Davidoff Ch. 12 (pp. 461-516)	Oct 3-7
Week 8 (Module 8) Event Log Forensics	Read Davidoff Chapter 8 (pp. 291-333)	Oct 10-14
Week 9 Midterm Exam (Practical)	✓ Practical Midterm Distributed 10/18	Oct 17-21
Week 10 (Module 9) Network Forensics & the Law- Legal Considerations	✓ Read Brunty Ch. 4 (pp. 71-86) ✓ Oct 28 (Friday)- Last day to drop a full semester individual course	Oct 24-28
Week 11 (Module 10) Practical Midterm Presentations	✓ Practical Midterm Due 10/31 @ 11:59PM	Oct 31-Nov 4

Open Source Network Forensics Part 1 (Social Media)	✓ Presentations Tuesday 11/1	
Week 12 (Module 11) Open Source Network Forensics Part 2 (Web/Internet Forensics)	✓ Read Brunty Ch. 1,2,3,5	Nov 7-11
Week 13 (Module 12) Internet Browser Forensics	✓ SecureWV/HackerCon (Nov 18-20) in Charleston, WV	Nov 14-18
Week 14 No Class	✓ Thanksgiving/Fall Break- 11/21-11/25	Nov 21-25
Week 15 (Module 13) Email Forensics		Nov 28-Dec 2
Week 16 (Module 14) Internet Chat & File sharing Forensics Final Exam Review	✓ "Dead Week"	Dec 5-9
Week 17 Final Exam (Written & Practical)	✓ Final Exam Time: Thursday, December 15, 8:00AM-10:00AM	Dec 12-16

"To Start Press Any Key'. Where's the ANY key? I see Esk, Catarl, and Pig-Up. There doesn't seem to be any ANY key. Whew! All this computer hacking is making me thirsty. I think I'll order a TAB."



*Syllabus meets requirements set forth by MUBOG Policy AA-14

-Homer Simpson