Instructor

Professor Josh Brunty, ACE, SCERS, CHFI, 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 8:00AM-10:00AM
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 four (4) credit hour Network Forensics (CRN# 2908) 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

DFIA 363, DFIA 400

Computer & Software Requirements

Due to the nature of the course, the student will be required to complete laboratory projects using forensic tools & software that is only available in the laboratory environment. Open lab hours will be posted later in the semester. These hours are usually posted the first week of the semester.

The College of Science maintains agreements with various software publishers to provide software for its computer labs as well as for its faculty, staff, and students. Students currently enrolled in COS courses are eligible to receive, via the COS Software Store, a variety of software applications at no cost for use in their academic endeavors. This includes many of the same applications used in COS courses (including the virtual platforms used in this course). All students currently enrolled in COS courses are eligible for the program, regardless of his/her major, as long as he/she is currently enrolled in at least one COS course.
http://www.marshall.edu/cos/software.

Students will need to create Tophat user account and purchase a Tophat subscription plan for use within this course. Subscription plans vary from 4 month access, semester access, to lifetime access. Tophat will be used to track attendance, class quizzes, reviews, etc. The join code for this course is 552219 and the course homepage is https://app.tophat.com/e/552219 Tophat can be used from either a PC or via the Android/iOS app on a mobile device. Students can also text-in answers to +1 (315) 636-0905 via SMS. This is ideal for poor wifi or older mobile devices.

Students will receive emails via Marshall email (Please setup your Marshall account 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 or email service may result in delayed responses.

Course content (labs, slides, exams, etc) will be distributed via MUOnline as they become available. You can log into the course homepage at the following address: www.marshall.edu/muonline

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.	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 In-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

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 MWF 11:00AM-11:50AM in the Weisberg Applied Engineering Complex (WAEC) Room 1232 (Digital Forensics Lab) with accompanied lab scheduled on Mondays from 12:00PM-12:50PM. 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.

Daily knowledge-based quizzes and attendance will also be administered via Tophat. These quizzes can be used as study material for the final and midterm examination.

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 be 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

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

Professionalism/Attendance Policy

This class is predominately lab and task based, with much of our time devoted to class time computer work and hands-on tutorials with forensic tools and other utilities that may only available in the laboratory environment. With that said, any missed classes will result in lost points (5 pts per class), put the student behind, and make it difficult to pick up with the next class lessons. Attendance is tracked and maintained electronically via Tophat. In the event that you MUST miss class, it is the student's responsibility to meet with the professor to discuss absences due to illness or other reasons. Any excused absences must adhere to the University's excused absence policy. In this course you will be treated as professionals and will be expected to behave and perform as such. As professionals, you will be expected to attend class, be on time, complete all of your assignments, meet deadlines, ask questions when you don't understand, and participate. Your classroom language and demeanor should also be professional. Also, please set your mobile devices to "Vibrate Only" mode (or turn it off) during class.

Academic Dishonesty Policy

As described in the Marshall University Creed, Marshall University is an "Ethical Community reflecting honesty, integrity and fairness in both academic and extracurricular activities. "Academic Dishonesty is something that will not be tolerated as these actions are fundamentally opposed to "assuring the integrity of the curriculum through the maintenance of rigorous standards and high expectations for student learning and performance" as described in Marshall University's Statement of Philosophy. A student, by voluntarily accepting admission to the institution or enrolling in a class or course of study offered by Marshall University accepts the academic requirements and criteria of the institution. It is the student's responsibility to be aware of policies regulating academic conduct, including the definitions of academic dishonesty, the possible sanctions and the appeal process. For the purposes of this policy, an academic exercise is defined as any assignment, whether graded or ungraded, that is given in an academic course or must be completed toward the completion of degree or certification requirements. This includes, but is not limited to: Exams, quizzes, papers, oral presentations, data gathering and analysis, practical and creative work of any kind.

If you are found cheating on projects or plagiarizing answers from the Internet or other sources (e.g. other students) there will be no second chance. Your penalty is that you will receive a failing grade for the course. In those cases in which the offense is particularly flagrant or where there are other aggravating circumstances, additional, non-academic, sanctions may be pursued through the Office of Judicial Affairs. Notice of an act of academic dishonesty will be reported to the Department Chair, Dean of the College of Science, and to the Office of Academic Affairs. Please refer to the Marshall University Undergraduate Catalog for a full definition of academic dishonesty.

Lab Submission Guidelines

The course includes a number of hands-on laboratory projects. All laboratory projects are due BY THE BEGINNING OF CLASS (generally it is Friday @ 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:
DFIA462_LastName_FirstInitial_Assignment Name.doc ("DFIA462_brunty_j_lab5_1.docx")

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	40%
Attendance/Participation	10%
Midterm Exam (Written & Practical)	25%
Final Exam	25%

Example:

Midterm Exam (92%)	x .25 = 23
Final Exam (86%)	x .25 = 21.5
Laboratory Projects (80%)	x .40 = 32
Attendance/Participation (85%)	x .10 = 8.5

	85.00 (85% B)

CLASS SCHEDULE	Marshall University Dates/ Important Dates/Notes	WEEK
NOTE: 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 (Module 1) -Introduction to Network Forensics (Course Introduction)	✓ Read Davidoff Ch. 1	Jan 9-13
Week 2 (Module 2) Technical Fundamentals-Introduction to Networking & Networking Concepts	✓ Read Davidoff Ch. 2 (pp. 23-44) ✓ Jan 16, Monday, MLK Holiday (University Closed)	Jan 16-20
Week 3 (Module 3) Network Forensics Acquisition/Analysis/Examination	✓ Read Davidoff Ch. 3 (pp.45-72)	Jan 23-27
Week 4 (Module 3) Network Forensics Introduction to Wireshark	✓ Read Intro to TCPdump/Wireshark PowerPoint & Video	Jan 30-Feb 3
Week 5 (Module 4) Network Forensics Traffic Analysis	✓ Read Davidoff Ch. 4 (pp.73-157) ✓ Read Davidoff Ch. 5 (pp.159-196)	Feb 6-10
Week 6 (Module 4) Network Forensics Traffic Analysis- Cont.		Feb 13-17
Week 7 (Module 5) Wireless Network Forensics	✓ Read Davidoff Ch. 6 (pp. 199-255)	Feb 20-24
Week 8 (Module 5) Wireless Network Forensics- Cont.		Feb 27-Mar 3
Week 9 Midterm Exam (Written & Practical)	✓ Monday 3/6- Midterm Exam- Written ✓ Wednesday 3/8- Practical Midterm Distributed	Mar 6-10
Week 10 (Module 6) Event Log Forensics	✓ Read Davidoff Chapter 8 (pp. 291-333)	Mar 13-17
Spring Break- No Class		Mar 20-24
Week 11 (Module 7) Malware Forensics	✓ Practical Midterm DUE 3/31 @ 11:59PM ✓ Read Davidoff Chapter 12 (pp. 461-516)	Mar 27-31
Week 13 Module 8) Network Forensics- Legal Considerations	Read Brunty Ch. 4	Apr 3-7

Week 14 (Module 9) Web/Internet Forensics	✓ Read Brunty Ch. 1,2,3,5	Apr 10-14
Week 15 No Class	✓ Apr 17-21- No class- Professor out for OSAC Meeting	Apr 17-21
Week 16 (Module 10) Email Forensics	✓ "Dead Week"	Apr 24-28
Week 17 Final Exam	✓ Final Exam Time: Tuesday, May 2, 10:15AM-12:15PM	May 1-5

Syllabus meets requirements set forth by MUBOG Policy AA-14