

Instructor

Name: Josh Brunty, CHFI, SCERS, ACE, AME
Office: Prichard Hall 215
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 8:30AM-9:30AM, F 12:00-1:00PM
Twitter: [@joshbrunty](https://twitter.com/joshbrunty)
Facebook: [Marshall Digital Forensics & Information Assurance](#)
Skype: josh.brunty
Linkedin: <http://www.linkedin.com/in/joshbrunty>

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 (4) credit hour Network Forensics (CRN# 3749) 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

IST 264, IST 363, IST 449

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. In order to accommodate for this, I have set aside open laboratory hours in the Digital Forensics Lab (ML 121) that will be posted during the first week of classes.

All students are responsible for knowing the University Computing Services' Acceptable Use Policy available at <http://www.marshall.edu/ucs/CS/accptuse.asp>.

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 and MUOnline at least once a day. PLEASE ONLY SEND TO MY MARSHALL EMAIL ADDRESS FOR QUICK CORRESPONDENCE. Messages left on MUOnline 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 2-5, 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.	Mod 6, Classroom Discussion, 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 3-13, 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 3-13, 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 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 exam 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>		
Professionalism/Attendance Policy		
This class is predominately project based, with a good majority of our time devoted to class time computer work and hands-on tutorials with forensic tools and other plugins that are only available in the laboratory environment. . With that said, any missed classes will result in lost points for in-class lab exercises, put the student behind, and make it difficult to pick up with the next class lessons. However, in		

the event that you **MUST** miss class, it is the student's responsibility to meet with the instructor to discuss absences due to illness or other reasons. I understand that there are circumstances that may arise throughout the semester that prevent a student from attending class. Documentation of an excused absence can be obtained from the Dean of Student Affairs, MSC 2W38. Excused absences include: death or illness of an immediate family member, pre-approved university sponsored activity, athletics, academic activities, short-term military obligation, jury duty/court appointment, and/or religious holiday (see MU Undergraduate Catalog). Nonetheless, if you miss class it is your responsibility as a student to obtain any lecture notes or assignments that you missed on that day.

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.

Inclement Weather Policy

Students can find information concerning Marshall's policy regarding inclement weather regarding inclement weather online via <http://www.marshall.edu/ucomm/weather.html>. Please note that a two-hour delay means that classes that begin at 10:00 a.m. begin on time. Classes that begin at 8:30 a.m. meet at 10:00 a.m. and continue for the remaining period of that class.

Makeup Policy

The tentative dates for the exams and due dates of projects/reports are shown in the course schedule. If you have other plans on any of these dates, please make arrangements now to change them, or inform the instructor of your plans. If for any unforeseen reason you must miss an exam or project due date, you must have a University excused absence. If the instructor accepts the excuse you will be given a make-up exam on the date specified. Otherwise, you will be given a zero (0) grade for the missed exam and/or assignment.

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.

Project 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 @ 11AM) 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:

IST462_LastName_FirstInitial_Assignment Name.doc ("IST462_brunty_j_project1.doc")

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	50%
Midterm Exam	25%
Final Exam	25%

Example:

Midterm Exam (92%)	x .25 = 23
Final Exam (86%)	x .25 = 21.5
Laboratory Projects (80%)	x .50 = 40

	86.25 (86% B)

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 on Fridays @ 11AM). 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 Malware & Exploits	✓ Read Davidoff Ch. 1 ✓ Read ic3 Report ✓ Review Online Videos ✓ Lab Project 1 Distributed ✓ January 16, Friday Last day to add classes	Jan 12-16
Week 2 (Module 2) Technical Fundamentals-Introduction to Networking & Networking Concepts	✓ Read Davidoff Ch. 2 (pp. 23-44) ✓ Lab Project 1 Due ✓ Lab Project 2 Distributed ✓ Jan 19, Monday, MLK Holiday (University Closed) ✓ No Class 1/21 (OSAC Meeting) ✓ Jan 20, Tuesday "W" Withdrawal Period Begins	Jan 19-23
Week 3 (Module 3) Network Forensics Acquisition/Analysis/Examination-Introduction	✓ Read Davidoff Ch. 3 (pp.45-72) ✓ Lab Project 2 Due ✓ Lab Project 3 Distributed	Jan 26-30
Week 4 (Module 4) Network Forensics Acquisition/Analysis/Examination-Traffic Analysis	✓ Read Davidoff Ch. 4 (pp.73-157) ✓ Lab Project 3 Due ✓ Lab Project 4 Distributed	Feb 2-6
Week 5 (Module 5) Network Forensics Acquisition/Analysis/Examination-Statistical Flow Analysis	✓ Read Davidoff Ch. 5 (pp.159-196) ✓ Lab Project 4 Due ✓ Lab Project 5 Distributed	Feb 9-13
Week 6 (Module 6) Network Forensics & the Law- Legal Considerations	✓ No Class 2/18, 2/20 (AAFS Conference) ✓ Read Brunty Ch. 4 (pp. 71-86) ✓ Lab Project 5 Due ✓ Lab Project 6 Distributed	Feb 16-20
Week 7 (Module 7) Social Media Forensics	✓ Read Brunty Ch. 1,2,3,5 ✓ Lab Project 6 Due ✓ Lab Project 7 Distributed	Feb 23-27

Week 8 (Module 8) Wireless Network Forensics Midterm Review	✓ Read Davidoff Ch. 6 (pp. 199-255) ✓ Lab Project (In-Class) ✓ Lab Project 7 Due ✓ Lab Project (In-Class)	Mar 2-6
Week 9 Midterm Exam (Written & Practical)	✓ Monday 3/10- Midterm Exam-Written ✓ Wednesday 3/11- Practical Midterm Distributed	Mar 9-13
Week 10 Spring Break- No Class	✓ March 16, Monday -- March 20, Saturday Spring Break, Classes dismissed	Mar 16-20
Week 11 (Module 9) Investigation of Web/Internet Crimes	✓ Midterm Practical Due Fri. 3/27 ✓ Lab Project 8 Distributed ✓ Mar 28, Fri. Last Day to Drop a Full Semester Individual Course	Mar 23-27
Week 12 (Module 10) Internet Browser Forensics	✓ Lab Project 8 Due ✓ Lab Project 9 Distributed ✓ March 30, Monday -- May 1, Friday Complete withdrawal only from the university ✓ March 30, Monday Students should schedule appointments with advisors to prepare for advance registration. (Required for students who have mandatory advising holds)	Mar 30-Apr 3
Week 13 (Module 10) Advanced Internet Browser Forensics	✓ Lab Project 9 Due ✓ Lab Project 10 Distributed ✓ Apr 8, Tues. Assessment Day (Students receive assignments in class)	Apr 6-10
Week 14 (Module 11) Email Forensics	✓ Lab Project 10 Due ✓ Lab Project (In-Class) ✓ Apr. 14, Mon. – Apr. 25 Fri. Advance Registration for Fall Semester for Currently Enrolled Students	Apr 13-17
Week 15 (Module 12) File Sharing & Internet Chat Forensics	✓ Lab Project (In-Class)	Apr 20-24
Week 16 (Module 13) “Dead Week” Introduction to Python & Network Forensics Final Exam Review	✓ Lab Project (In-Class) ✓ May 1, Fri. Last Day to Completely Withdraw for Spring Semester	Apr 27- May 1

Week 17 Final Exam	Final Exam Time: Tuesday, May 5, 10:15AM-12:15PM	May 4-8
------------------------------	---	---------

"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