MARSHALL

DIGITAL FORENSICS
INFORMATION ASSURANCE

COURSE SYLLABUS
DFIA 462- Network Forensics
CRN: 2884- 4 CR HRS.

Instructor:	Prof. Josh Brunty	**Class Meets:**	MWF 11:00-10:50AM M 12:00-12:50PM
Office:	WAEC 2001	**Classroom:**	WAEC 1232
Phone:	304-696-5602	**Office Hours:**	MWF 9:00-10:00AM
Email:	josh.brunty@marshall.edu		TR 9:30-11:00AM

Course Description (from catalog):

Examination of techniques and tools used to investigate, search, collect, analyze, and report on network based breaches and events.

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:

This Network Forensics course will meet every MWF from 11:00am-11:50am & M from 12:12:50PM in the Weisberg Applied Engineering Complex (WAEC) Room 1232 (Digital Forensics Laboratory).

Students will be given lecture and multiple in-class, instructor-led lab exercises that focus on a variety of Network Forensics methodologies. Students will also complete ten (10) hands-on, virtual laboratory exercises and challenge labs throughout the course of the semester. Students will also be quizzed on content at multiple points during the semester via Top Hat.

A midterm (written & practical) and final examination 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 from either the Marshall University Bookstore or you can purchase a lab code directly from the INFOSECLEARNING 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.

- Students will need to create Tophat user account and purchase a Top Hat subscription plan for use within this course. Top Hat can either be purchased online or through MU Bookstore with different subscription options based upon your needs. Subscription plans vary from 4 month access, semester access, to lifetime access. However, if you are a full-time student in the DFIA program I would recommend that you purchase the lifetime subscription as this software will be used in your future DFIA coursework. Top Hat will be used to track attendance, class quizzes, reviews, etc. The join code for this course is 233438 and the course homepage is https://app.tophat.com/e/233438 Top Hat 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.

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	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class

investigate network and internet-related crimes		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:

Regular attendance in this class is crucial to your success as a student. The only way to benefit from class discussions and hands-on learning activities is to be here. Being present and on time for all class meetings is expected. Period. Excused absences include: 1) University-sponsored academic activities (performing arts, debate and individual events, honors classes, ROTC); official athletic events; other university activities (student government). 2) Student Illness or Critical Illness/Death in the Immediate Family:" Immediate Family" is defined as a spouse/life partner, child, parent, legal guardian, sibling, grandparent or grand- child. *Routine doctor appointments are not excused. Appointments should be scheduled around your classes. 3) Short-Term Military Obligation. 4) Jury Duty or Subpoena for Court Appearance and 5) Religious Holidays. It is the student's responsibility to provide appropriate documentation to Dean of Student Affairs or the instruction for excused absence. Learn how the process works here: http://www.marshall.edu/student-affairs/excused-absence-form/ The student should also request opportunity to complete missed work immediately upon return to class. Be aware that excessive absences—whether excused or unexcused—may affect your ability to earn a passing grade. Regardless of the nature of the excused absence, you are responsible for completing all coursework prior to the end of the semester.

Because this course is an interactive class, students who miss class due to University-excused activities will be provided with an alternative assignment that connects to the activities in the missed class session. For unexcused absences, if you miss ***two (2)*** classes, I will issue a warning. If you miss a **third (3rd)** class: You will receive an automatic **one letter grade deduction** in the course. We will conference to discuss your standing and develop a plan of improvement. If you meet its criteria, you may have the chance to earn back the letter grade deduction. If you miss a fourth class, the previous letter grade deduction stands, regardless of improvement plan results. Subsequent missed classes will result in an additional letter grade deduction for each absence. Regardless, students will earn 1 point for each class attended and 1 point for each in-class quiz taken. The points for these can **ONLY** be made up if an excused absence is provided.

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 obtain a written excused absence form.

All electronic submissions MUST follow this file naming convention:
FSC609_LastName_FirstInitial_Assignment Name.doc (“DFIA101_brunty_j_lab1.docx”)

Course Requirements & Grading Policy:

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

Top Hat Attendance & In-Class Quizzes (10%)- Attendance will be taken each day of class via Top Hat. It is the student’s responsibility to make sure that attendance is properly recorded for that class Each class will be worth 1 point and will be calculated as a composite score at the end of the semester. Any in-class quizzes given by the instructor via Top Hat will also earn 1 point for participation for each quiz completed. This will also factor into this weighted percentage calculation.

Virtual Laboratory Exercises (25%) – 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 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.

Practical Midterm Examination (25%)- This examination will be handed out 1 ½ 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 a written examination that will be administered 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:

Attendance & Participation	10%
Laboratory Exercises	25%
Practical Midterm	25%
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>Top Hat Attendance/Participation</td><td></td><td>X .10 =</td><td></td></tr>
<tr><td>Laboratory Exercises (average)</td><td></td><td>X .25 =</td><td></td></tr>
<tr><td>Practical Midterm</td><td></td><td>X .25 =</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>

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 card access 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. 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 http://www.marshall.edu/cosweb/agreements/?a=j3qw3 Usage of the computers and course files will not be permitted until the online form is completed.

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).

If you need to schedule an office-hours appointment with me (career guidance, help with lab projects, etc.) you can stop by during my office hours or you can schedule an appointment with me anytime by visiting: https://calendly.com/joshbrunty/studentmeeting

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 must also be completed by 11:59PM on the Friday of the week as they appear on the schedule below.

Module 1: Introduction to Network Forensics (1/8-1/12)	
Required Readings	Davidoff Chapter 1
Lab	Module 1 Lab- Using SET (Social Engineering Toolkit)
Module 2: Technical Fundamentals (1/15-1/19)	
Required Readings	Davidoff Ch. 2 (pp. 23-44)
Lab(s)	Module 2 Lab- TCP/IP Utilities
Note:	No Class 1/15 (MLK Day)
Module 3- Network Forensics- Acquisition/Analysis/Examination (1/22-1/26)	
Required Readings	Davidoff Ch. 3 (pp. 45-72)
Lab	Module 3 Lab #1- Performing a DoS Attack from the WAN
Module 3- Network Forensics- Introduction to Wireshark (1/29-2/2)	
Required Readings	Watch Hack3rCon “Intro to TCPdump & Wireshark” Video
Lab	Module 3 Lab #2- Capturing & Analyzing Network Traffic Using a Sniffer
Module 4- Network Forensics- Traffic Analysis (2/5-2/9)	
Required Readings	Davidoff Ch. 4 (pp. 73-157)
Lab	No Lab Due
Module 4- Network Forensics- Traffic Analysis Cont. (2/12-2/16)	
Required Readings	Davidoff Ch. 5 (pp. 159-196)
Lab	Module 4 Lab: Deep Dive in Packet Analysis - Using Wireshark and Network Miner
Module 5- Wireless Network Forensics (2/19-2/23)	
Required Readings	Davidoff Ch. 6 (pp. 199-255)
Lab	Module 5 Lab #1- Breaking WEP and WPA and Decrypting the Traffic
Note	No Class 2/21 (W) and 2/23 (F) due to AAFS conference
Module 5- Wireless Network Forensics (Search & Seizure) (2/26-3/2)	
Required Readings	No Reading Assigned
Lab	Module 5 Lab #2- Examining Wireless Networks
Midterm Exam- Written & Practical (3/5- 3/9)	
Required Readings	No Reading Assigned
Lab	No Lab Assigned

Note	Written Exam covering Modules 1-5 (Monday 3/5), Practical Exam Distributed & Briefing (Wednesday 3/7)
Module 6- Event Log Forensics (3/12- 3/16)	
Required Readings	Davidoff Ch. 8 (pp. 291-333)
Lab	No Lab Due
Note	Midterm Practical Reports Due @ 11:59PM (3/16)
Spring Break (3/19-3/23)- No Class	
Module 7- Malware Forensics (3/26- 3/30)	
Required Readings	Davidoff Ch. 12 (pp. 461-516)
Lab	Module 6 Lab- Log Analysis Module 7 Lab- Memory Analysis
Module 8- Legal Issues in Network Forensics (4/2- 4/6)	
Required Readings	Brunty Ch. 4
Lab	No Lab Due
Module 9- Web/Internet Forensics (4/9- 4/13)	
Required Readings	Brunty Ch. 1,2,3 & 5
Lab	No Lab Due
Module 10- Communication Artifacts Cont. (4/16- 4/20)	
Required Readings	Communication Artifacts Handouts & Slides
Lab	No Lab Due
Module 10- Communication Artifacts Cont. (4/23- 4/27)	
Required Readings	No Required Readings
Lab	Module 10 Lab- Communication Artifacts
Note	Dead Week Final Exam Review- (Fri 4/27)
Final Exam Week (4/30- 5/4)	
Final Exam	Exam Covers Modules 6-10 Exam Time: Tuesday, May 1st 10:15AM-12:15PM