MARSHALL DIGITAL FORENSICS INFORMATION ASSURANCE	**Digital Forensics and Information Assurance 420** Incident Response Course Syllabus Spring, 2018

Spring 2018
M,W,F 1-1:50
WAEC 1232

Instructor – John Sammons
Office – WAEC 2003
Office Phone – 304-696-7241
eMail Address – john.sammons@marshall.edu

Office Hours:

Mon, Weds, Fri – 10:00 – 11:00
T/TH – 11:00 – 12:00

* Other times by appointment

Textbook

Incident Response and Computer Forensics 3rd Edition, Jason Luttgens, Matthew Pepe, McGraw-Hill, San Francisco, CA. ISBN 13: 978-0071798686

Required (and suggested) Materials

Each student must obtain a spiral-bound sketchbook 9”x 12”. We will be doing quite a bit of sketchnoting during this course. Your finished notebook will be submitted at the end of the semester.

You’re also encouraged to obtain a ruler, and some decent pens, pencils, highlighters, markers, etc. These will enhance with your sketchnoting experience. I am happy to provide some recommendations if you like.

Course Description

This course examines the forensic and investigative aspects of a network intrusion. Topics include pre-incident preparation, developing leads, scoping an incident, data collection and forensic duplication, evidence from hosts (Windows), Networks, Applications, and enterprise environments. We will also examine the steps and actions taken during remediation.

Credit

The course is three (3) credit hours.

Pre/co-requisites

DFIA 400 Introduction to Digital Forensics

Course Learning Objectives

Course Student Learning Outcomes	How students will practice each outcome in this Course	How student achievement of each outcome will be assessed in this Course
Students will effectively **explain** the incident response process.	PowerPoint/Prezi development, peer & instructor review, journal assignments, Quizlets, sketchnotes	Presentations, test questions, concept map, high stakes writing assignment, sketchnotes
Students will correctly **apply** the fundamental principles of incident response.	Case studies and practical exercises, journal assignments, peer teaching, Quizlets	Presentations, test questions, concept map, high stakes writing assignment
Students will **demonstrate** their ability to communicate effectively both orally and in writing.	PowerPoint/Prezi development, peer & instructor review, journal assignments, Quizlets, sketchnotes	Presentations, test questions, concept map, high stakes writing assignment, sketchnotes
Students will correctly **apply** investigative methodologies used when responding to a network intrusion.	Case studies and practical exercises, journal assignments	Presentations, test questions, concept map, high stakes writing assignment
Students will correctly ***locate***, ***preserve***, ***collect***, ***analyze***, and ***interpret*** common artifacts associated with a network intrusion.	Journal exercises, in-class team assignments, Quizlets, Practical exercises, journal assignments	Tests and practical assessments
Students will **arrange** key course content into a comprehensive, detailed concept map that clearly demonstrates the relationship of one concept to another.	Module concept maps	Mid-Term & Final Concept Maps

Blackboard

Unless otherwise stated, ALL assignments must be submitted on time through Bb. It's your responsibility to know how to do this. Late work will not be accepted without a verified or university approved excuse. Should you have some issue that prohibits you from doing meeting the deadline, you should email the assignment to me via my

MU email account. This should be before the due date as well. If not, it will not be accepted. You should collect proof that supports your reason for the work being late. Work that is not in Bb will likely not be graded.

Grade Appeals

Should you feel an assignment/test question was graded in error, you may appeal. However, your appeal MUST FOLLOW THIS PROCEDURE and FORMAT. You will submit the appeal through Bb email only. Appeals sent elsewhere will not receive a response. The subject line MUST say this "APPEAL – Test/Assignment Name." In the body of the email list the entire question, your answer, and why you think you deserve credit.

Instruction Method

There will be 3 contact hours of classroom instruction per week. Coursework will include classroom lectures, a learning journal, and exams along with a variety of low, med and high stakes writing assignments. You are expected to take an active role in your learning. Discussions and writing assignments play significant roles in the conduct of the course.

This course will be taught using active learning methodologies. This means that lectures, as a delivery method will be limited. For students, this means that you will be expected to complete all assigned "pre-work" before the start of class, participate in group assignments, and complete in-class exercises.

Evaluation method

Course grades will be based on a total points system. Your grade will be based on a percentage of the total points possible.

Course Point Distribution

Assignment/Assessment	Points Possible
Midterm & Final Exam (Concept Map)	200
Projects & Assignments	200 (Approx. Subject to change based on progress)
Chapter Tests	500 (Approx. Subject to change based on progress)
Learning Journals	330 (Approx. Subject to change based on progress)
Sketchnotes	200 (Approx. Subject to change based on progress)
Total	**1430** (Approx. Subject to change based on progress)

Final letter grades are determined based on the following grading scale:

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

The instructor reserves the right to change these values depending on the overall class performance and/or extenuating circumstances. Please note that your final grade will be calculated by hand, NOT from the totals/weights that you may see on Bb. Grades will be posted as quickly as possible into Bb. However, please keep in mind that those times will vary.

Policy Statement

My Academic Dishonesty Policy
Academic Dishonesty is defined as any act of a dishonorable nature which gives the student engaged in it an unfair advantage over others engaged in the same or similar course of study and which, if known to the classroom instructor in such course of study, would be prohibited. Academic Dishonesty 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.

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

In this course, STUDENTS ARE NOT TO "COPY & PASTE" MATERIAL FROM A SOURCE INTO ANY ASSIGNMENT UNLESS SPECIFICALLY AUTHORIZED BY THE INSTRUCTOR.

If you are found cheating on projects or plagiarizing answers from the Internet or other sources (among other things), 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.

Your assignments may be analyzed using the anti-plagiarism suite of tools powered by Turnitin. Please visit http://turnitin.com for more information.

Assignments

The course includes a number of writing assignments. All assignments are due **BY THE BEGINNING OF CLASS** on their due date. **NO LATE ASSIGNMENTS WILL BE ACCEPTED**. There are VERY specific cutoff dates/times for submission. Please do not procrastinate. If you wait until the last night to start a writing assignment, chances are, you will fail. All (or the majority of) assignments MUST be submitted through Bb. Should some technical issue arise that makes this impossible submit the clearly labeled assignment through Bb email. If for some reason, you cannot submit the assignment through Bb email the instructors University email address will serve as a backup means of submission. Should submission prove to be impossible, students are expected to leave a voice mail on the Instructors office phone. In ALL instances, any email or voicemail MUST have a date/time stamp that is BEFORE the due date/time of the assignment. Submissions that do not will be rejected.

Assignments should be labeled as follows:

File Names: All electronic submissions must follow this file naming convention:
DFIA 420_Last Name_First Initial_Assignment Name.doc ("DFIA420_sammons_j_researchpaper.doc")

***Make-up Quizzes/Assignments and Late Penalty**:* Make-up exams will not be given except under unusual circumstances and with satisfactory written justification. Any student who misses a quiz/assignment due to an unexcused absence will receive a grade of zero with no opportunity for make-up or substitution. Only University excused absences or those occurring with a good reason (and that reason must be given prior to missing the quiz/assignment) will be accepted.

Make up quizzes/assignments must be taken within one week of the original scheduled date. The decision to allow a make-up quiz or accept late work rests with the instructor. Please note, your university excuse MUST be received by me within TWO weeks of the missed assignment/test. Excuses received after that time will not be accepted.

Attendance Statement & Policy

Attendance is absolutely vital to your success in this course and your ability to learn and retain this material. As such, attendance is mandatory. You will be permitted **TWO** unexcused absences for the entire semester. Each unexcused absence after that will result in a one letter reduction of your grade. Top Hat will be used to collect attendance every day in class.

Excused Absence

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

5. Religious Holidays

Unexcused Absences

· If you miss two classes, I will issue a warning.

· If you miss a third 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.

Student's Responsibility

· Provide appropriate documentation to Dean of Student Affairs for excused absence. Learn how the process works here: http://www.marshall.edu/student-affairs/excused-absence-form/

· 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**.

Top Hat
Students will need to create Top Hat user account and purchase a Top hat subscription plan for use within this course. Subscription plans vary from 4-month access, semester access, to lifetime access. Top Hat can either be purchased online or through MU Bookstore.

Top Hat will be used not just to track attendance, but for class quizzes, reviews, etc. The join code for this course is TBA and the course homepage is TBA. 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.

All students must have Tophat available for use by Monday, January 15, 2018.

Class Cancellation

There may come a time during the semester when class could be cancelled (illness, weather, etc). Should that occur, I will notify everyone through their official University email as well as post an announcement on Bb. You are responsible for checking these early and often to ensure that class will be held as scheduled. Should there be some technological issue that prevents me from doing that, a sign should be posted on the classroom door.

Professionalism

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. Participating in class means that you are not on your cell phone or surfing the Internet. If you can't be in class, I expect you to let me know ahead of time. Your classroom language and demeanor should also be professional all times. Written communication with me must also be professional. You are expected to follow the guidelines in the "How to Email My Professor" article.

University Holidays & Key Dates

January 8, Monday
First Day of Classes

January 15, Monday
Martin Luther King, Jr. Holiday – University Closed

January 16, Tuesday
"W" Withdrawal Period Begins

March 16, Friday
Last day to drop an individual course

March 19, Monday – March 24, Saturday
Spring Break – Classes Dismissed

March 26, Monday
Classes resume

April 27, Friday
Last Class Day - Last Day to Completely Withdraw from Summer II

April 30, Monday – May 4, Friday
Final Exams

May 8, Tuesday, Noon
Final Grades Due

Expectations

1. Work/Think Hard
2. Participate
3. Act with Integrity
4. Embrace the Challenges
5. Tell Me if You Have a Problem
6. Own Your Mistakes and Shortcomings
7. Help Your Fellow Students
8. Be Willing to Work Outside Your Comfort Zone
9. Have FUN!
10. Treat Everyone with Respect
11. Read the Syllabus
12. Check Bb and Your Email Very Often
13. Check Bb for Due Dates and Assignment Specifics
14. Read All of the Assigned Materials

Technical Competencies

Students are expected to be proficient working with AD Forensic Toolkit, FTK Imager, Registry Viewer, Password Recovery Toolkit, and Microsoft Office products or their equivalent. In addition, students will need to an application to create concept maps. VUE, from Tufts University is the recommended tool for this purpose. Use of a different tool for creation of the concept map requires the instructors permission. It's a free, open source tool that works well on Windows or Macintosh computers. It can be downloaded here: http://vue.tufts.edu/. VUE is very simple to use with a very short learning curve. Students are also expected to be proficient using the Blackboard system (submitting assignments, navigating the class space, taking tests, etc.).

Topics and Methodology

The following outline delineates the tentative class schedule with topics to be addressed during the course.
It could vary based on class progress and performance.

Week	Dates	Lecture Topics	Reading
1	Jan 8-12	Intro, Module "0" Data Storage	Bb
2	Jan 15-19	Real World Incidents	Chap 1
3	Jan 22-26	Incident Response	Chap 2
4	Jan 29 – Feb 2	Pre-Incident Prep	Chap 3

5	Feb 5-9	Starting the Investigation	Chap 4
6	Feb 12-16	Developing Leads	Chap 5
7	Feb 19-23	Mid-Term	Chap
8	Feb 26 – Mar 2	Scoping the Incident	Chap 6
9	Mar 5-9	Live Data Collection	Chap 7
10	Mar 12 -16	Forensic Duplication	Chap 8
11	Mar 19-23	Spring Break	
12	Mar 26-30	Network Evidence	Chap 9
13	Apr 2-6	Investigating Windows	Chap 12
14	Apr 9-13	Investigating Enterprise Services	Chap 10
15	Apr 16-20	Malware Triage	Chap 15
16	Apr 23-27	Dead Week	
17	May 1 -5	Final Exams	Chap 17

Every student is responsible for all materials presented in class, including lectures, notes, and handouts. In case you are not present for a class, it is your responsibility to contact the instructor and receive information about the material presented in that class. Class attendance is VERY IMPORTANT.

Effort Required

This course requires significant effort both in and out of class. Outside of class students will be expected to keep pace with the reading/videos and come to class prepared. If you come to class unprepared it will negatively impact your ability to complete the lab exercises. For every one hour in class, the student is expected to put in an effort of at least 3 hours outside the class for studying and completing writing assignments. Depending upon background and preparedness, some students may have to put in additional effort. **DO NOT PROCRASTINATE.**

Prioritize, schedule, and take responsibility for your actions and you should do very well in this class. To be successful in this course, you **MUST** take an active role in the learning process. To be successful in the course, you must do the work. You must also manage your time effectively. Throughout the semester you may be given time in class to work on various assignments. I STRONGLY encourage you take full advantage of this opportunity.

Blackboard and Module 0

Your first assignment is to complete Module 0. This module is located on Bb. Part of this module is a quiz that you are expected to complete the first week of class. This quiz covers course administration, procedures, rules, policies, etc. Module 0 lays the groundwork for the rest of the semester. You are expected to read and familiarize yourself with all the material in Bb and its location. You should go through Bb and see what resources and information are available to you. From time to time, you may find assignments, etc. that are left over from a previous semester. Check the dates. Unless the dates are current, those assignments aren't applicable. You may also ask me for clarification. In regard to due dates, they should be clearly listed in Bb. The date in Bb is the date we will go by. If you need to know when something is due, check Bb. I don't commit to memory every due date for every assignment in all the classes I teach.

Learning Journal

As part of this course, each student must maintain a learning journal. This journal will contain a variety of low stakes assignments, many to be done in class. It is your responsibility to keep it current. It will be turned in at the end of each learning module as a single document. Do NOT procrastinate. The journals are graded **ALL OR NONE**. If you complete all entries, you will receive full credit. **ANY** missing entries will result in a 0.

You will need your journal during almost every class therefore you must ensure it's available when you need it. It is your responsibility to ensure that it's kept safe. You would be wise to make frequent back-ups of your journal. You may want to consider using Dropbox (www.dropbox.com) or Google Drive.

Tests & Readings

The number of quizzes/tests will vary, depending on class progress, participation, and how well students keep up with assignments, readings, etc. Generally, there will be a quiz for each module. Students are expected to keep up with all reading assignments and come to class prepared to discuss the material.

Communication

Private E-mail will be used to make any general announcements, last minute changes, etc. It is **mandatory** that you monitor your email messages at least once a day. PLEASE ONLY USE MY MARSHALL EMAIL ADDRESS FOR URGENT CORRESPONDENCE. Urgent messages left on Blackboard will result in extremely delayed/no response. Bb email should be used for correspondence related to assignments. Please read and follow the guidelines outlined in the "How to Email Your Professor" article. There is a link to it posted on Bb.

All written communications, including discussion postings, emails and written assignments Format, structure, organization, tone, clarity, spelling and punctuation all contribute to effective communications and are expected in all student communications. Any communication not deemed an appropriate business communication may be disregarded by the instructor or points may be taken off, at the sole discretion of the instructor. Students are expected to thoroughly proofread all communications

Using my University email for urgent communication ensures you get a response and the course run smoothly. During periods of inclement weather, check your email and Bb the night before, and the morning of class to see if it has been cancelled.

There is a great deal of information in Bb regarding the conduct of the course, additional resources, etc. You are expected to read and navigate through this material.

Note about cell phones and Internet in class

Please set your cell phone ringer to "Vibrate Only" mode (or turn it off) before you enter the classroom. While in class, you will be expected to work on class related materials/assignments. Please do not surf the Internet and work on other assignments unless authorized by the instructor.

During tests, cell phones MUST be put away. No exceptions.

Disclaimer

The instructor reserves that right to modify the course schedule and evaluation system should it become necessary for the effective conduct of the course.

Extra Credit

Extra credit MAY be offered during the semester. These assignments would be considered optional. Do NOT count on extra credit to save you from a failing grade.

Social Networking

I often receive friend requests from students via Facebook. It is my policy however, not to accept these requests from current students. This is absolutely nothing personal, so please do not take it as such. You are welcome to follow me on Twitter and or join my network on Linked-In. Please join us on the MU Digital Forensics Facebook page. There is lots of good information there including job and internship opportunities.

Please participate in our social media channels:

Facebook - Marshall Digital Forensics & Appalachian Institute of Digital Evidence

Twitter - @ MUDigForensics & @AppyIDE

Instagram - MarshallUDigForensics

Join the student chapter of Appalachian Institute of Digital Evidence - http://www.appyide.or

Get Involved!

There are tremendous opportunities here beyond your coursework. The student chapter of AIDE (Appalachian Institute of Digital Evidence), internships, and research are just some of the possibilities. Involvement in these activities is what can separate your resume from the others. Do not miss this opportunity. See me for details. Also, get to know the faculty. Introduce yourself, stop by and see us. The more we communicate and get to know you, the more we can help you.

Recommendations

I am very happy to write recommendations for students. My only requirement is that you give me a basis/foundation for a recommendation. Here's what I mean. If you don't get involved, earn average grades, show up late for class, do the bare minimum, don't do research, etc. I have nothing to write about.

NOTES: