DIGITAL FORENSICS
INFORMATION ASSURANCE

DFIA 400 Intro to Digital Forensics

Course Syllabus

Fall 2017

WAEC 1232
T/TH 11:00a-12:15p

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

Office Hours:

Monday	11:00am – 12:00pm
Tuesday	1:30pm – 2:30pm
Wednesday	11:00am – 12:00pm
Thursday	1:30pm – 2:30pm
Friday	11:00am – 12:00pm

All other times by appointments

* Please send me an email to schedule a meeting if possible. Sometimes I get pulled away even during office hours.

Textbooks

AccessData Training Manual. Academic Edition.

YOU MUST KEEP THIS MANUAL. YOU WILL NEED IT IN OTHER COURSES HERE AND AFTER YOU GRADUATE AS WELL. YOU CAN'T GET THIS BOOK OUTSIDE OF THE UNIVERSITY WITHOUT ATTENDING THE OFFICIAL TRAINING.

Course Description

DFIA 400 introduces students to core digital forensic concepts, including data storage, imaging, the digital forensics process, common Windows artifacts, and the fundamentals of the forensic examination of digital media using the AccessData suite of tools.

Credit

The course earns three (3) credit hours.

Pre/co-requisites

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 function of key Windows forensic artifacts.	Hands-on exercises, Journals, Sketchnotes, class discussions, PowerPoint presentation.	Module Tests, Final Exam
Students will correctly **locate, identify,** and **interpret** Windows artifacts using FTK.	Hands-on exercises, Journals, Sketchnotes,	Module Tests, Final Exam
Students will correctly **image** a piece of digital evidence using FTK IMAGER.	Hands-on exercises, Journals, Sketchnotes,	Module Tests, Final Exam
Students will correctly **interpret** common Windows artifacts as they relate to the facts and circumstances of a particular investigation.	Hands-on exercises, Journals, Sketchnotes,	Module Tests, Final Exam
Students will **understand** how learning occurs and **apply** best practices to their own learning in this course.	Journal assignment, Sketchnotes, discussion, Quizlet	Test questions

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 completing the assignment on Bb by 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. This course will be taught using active learning and "flipped classroom" 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. Students are expected to watch the module videos on the AccessData Learning Management system **BEFORE** starting on module in class. This is predominantly a hands-on class. Students will often work individually at their own pace. Students are expected to take an active role in their own learning.

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
Assignments	100 (Approx. Subject to change based on progress)
Midterm & Final	200
Quizzes	100
Total	**400** (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 the Bb system as quickly as possible. 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.

College of Science IT Student Conduct Agreement

In order to complete this course, you must read, sign, and comply with the COS IT conduct agreement. The agreement is available online here: http://www.marshall.edu/cosweb/agreements/?a=j3qw3

This code of conduct **MUST** be read and signed by you no later than **Friday, August 25, at 5:00 PM.** If you fail to sign this agreement, your access to the computers in WAEC 1232 will be **REVOKED** until you do.

Assignments

The course includes a number of writing assignments. All assignments are due **by the date and time noted in Bb**. **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, the instructors University email address will serve as the secondary 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. If you have an extenuating circumstance that prevents you from submitting an assignment by the due date/time you will need to contact the instructor prior to the due date to explain the circumstance and obtain permission for a late assignment. Failure to contact the instructor prior to the due date with result in a zero on the assignment.

All assignments must follow the format described in the assignment instructions in Bb. Failure to follow the specific formatting and naming instructions could result in a zero for the assignment.

File Names

All electronic submissions must follow this file naming convention:

DFIA400_Last Name_First Initial_Assignment Name.doc ("dfia400_sammons_j_researchpaper.doc")

Make-up Quizzes/Assignments and Late Penalty

Make-up exams will not be given except under unusual circumstances and 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 348338 and the course homepage is http://app.tophat.com/e/348338. 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.

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 and 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. Once class begins University computers you use are intended for classroom work and not for personal use. This includes checking Facebook, other social media sites, and surfing the Web. 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.

When sending correspondence to the instructor it is expected that your language and content of your correspondence be clear, professional and polite. You should view this correspondence as a business communication and not a personal communication. Correspondence that is unclear, rude and unprofessional will not be responded to.

University Holidays & Key Dates

September 4, Monday
Labor Day – University Closed

October 19, Monday
Midterm grades due

October 27, Friday
Last Day to Drop

November 20, Monday – November 25, Saturday
Thanksgiving Break – Classes Dismissed

November 27, Monday
Classes Resume

December 4, Monday – December 8, Friday
Dead Week

December 8, Friday
Last Class Day

December 11, Monday – December 15, Friday
Final Exams

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
15. Refrain from personal cell phone and computer use in class.

Technical Competencies

Students are expected to be proficient working with Microsoft Office products or their equivalent. In addition, students will need to an VUE to create concept maps. VUE is a free, open source tool that woks 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. Using other tools to create concept maps requires permission from the instructor. 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.
Please note this schedule is tentative.

Week	Dates	Topics	Reading	LMS Video
1	Aug 21- 25	Learning/Digital Forensics Process	Bb	N/A
2	Aug 28 – Sept 1	Data Storage/FTK Imager	Bb/Mod 2	Introduction Working with FTK Imager (Due 9-2-16)

3	Sept 4 - 8	Windows Registry/ Registry Viewer	Mod 3	
4	Sept 11 - 15	Windows Registry/ Registry Viewer	Mod 3	Introduction to Registry Viewer (Due 9-16-16)
5	Sept 18 - 22	Working with FTK Part 1 (DerbyCon)	Mod 5	
6	Sept 25 – 29	Working with FTK Part 1	Mod 5	Working with FTK Part 1 (Due 9-30-16)
7	Oct 2 - 6	Working with FTK Part 2	Mod 6	Working with FTK Part 2 (Due 10-7-16)
8	Oct 9 - 13	Midterm/Flex		
9	Oct 16 - 20	Processing the Case Narrowing Your Focus	Mod 7 Mod 8	Processing the Case (Due 10-21-16)
10	Oct 23 - 27	Filtering the Case	Mod 10	Filtering the Case (Due 10-28-16)
11	Oct 30 – Nov 3	Recycle Bin	Mod 11	Narrowing your Focus (Due 11-4-16)
12	Nov 6 - 10	Common Windows Artifacts Windows System Artifacts	Mod 12	Common Windows XP Artifacts (Due 11-11-11)
13	Nov 13 - 17	Common Windows Artifacts Windows System Artifacts	Mod 12	Regular Expressions (Due 11-18-16)
14	Nov 20 - 24	Thanksgiving Break	N/A	N/A
15	Nov 27 – Dec 1	Working with PRTK Anti-forensics	Mod 13	Working with PRTK Decrypting EFS (Due 12-2-16)
16	Dec 4 - Dec 8	Case Reporting Legal/ Last week of class	Mod 15	Case Reporting

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 and part of professionalism grade for this course.

Effort Required

This course requires significant effort both in and out of class. As you can see by the size of the manual, there is a huge amount of material. 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.

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 of the classes I teach.

Tests & Readings

At the end of the semester you will have the opportunity to take the AccessData Certified Examiner test. It is given online and consists of both knowledge based questions as well as a practical using the tools and actual evidence. This is a timed test so it's imperative that you spend as much time during the semester using the tools so that you're not fumbling around during the test.

Communication

Private E-mail (Marshall email) 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 CORRESPONDENCE. Messages left on Blackboard will result in extremely delayed/no response. 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 should be professional and courteous. Format, structure, organization, tone, clarity, spelling and punctuation all contribute to effective communication 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 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.

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.

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.org

Get Involved!

There are tremendous opportunities here beyond your coursework. The student chapter of AIDE (Appalachian Institute of Digital Evidence), internships, CCDC, 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.

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.