Instructor
Name: 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 8:30-9:30AM, TR 8:00AM-9:30AM
Twitter: https://twitter.com/joshbrunty (@joshbrunty)
Facebook: Marshall Digital Forensics & Information Assurance
Linkedin: http://www.linkedin.com/in/joshbrunty

Required Text(s)
AccessData Forensics Training Manual- Academic Edition *(Avalable only @ Marshall University Bookstore)*

Recommended Texts
None

Resource Sites
http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk (Resource Site for FTK v6)
https://www.syntricate.com/computer-forensics-certification.html (Information & Resources on ACE)

Course Description
This two (3) credit hour Data Recovery & Analysis course (CRN #3745), through lecture, demonstration, and practical "hands-on" Training, is designed to provide students theories and techniques utilized to examine, analyze, and classify various types of digital evidence

Prerequisites
IST 264- Technology Foundations

Computer Requirements
Students will be required to complete assignments using AccessData's Forensic Toolkit v6 (FTK) and its complimentary suite of forensic tools (this software will be made available in the WAEC 1232 computer lab). Open lab hours will be posted later in the semester. In addition, the open lab hours will be available to practice and complete laboratory projects and assignments. These hours are usually posted in the ML Commons area the first week of the semester.

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 messages at least once a day. PLEASE ONLY SEND TO MY MARSHALL EMAIL ADDRESS FOR QUICK CORRESPONDENCE. Messages left on MUOnline or other social networking mediums may result in delayed responses.

The IST department maintains agreements with various software publishers to provide software for its computer labs as well as for its faculty, staff, and students. Students enrolled in IST department courses are eligible to receive a variety of software applications at no cost for use in their academic endeavors. This includes many of the same applications used in IST courses. You can find this information and more on the IST Web site at http://www.marshall.edu/isat/software/. |

Course Objectives/Outcomes
This course is designed to build on the material learned in previous foundational courses and apply those concepts. This course places a strong emphasis on utilization of advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators.

Upon completion of Data Recovery & Analysis course, students will be able to:		
Course Student Learning Outcome	How Practiced in This Class	How Assessed in This Course
Students will be knowledgeable in recovering evidence from various digital media types	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Practice Competency Exam, Final Exam
Students will be familiar with components of advanced hardware and software systems used in a digital forensics laboratory.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Practice Competency Exam, Final Exam
Students will be acquainted with advanced methods used to recover, examine, and complete case reports pertaining to digital evidence.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Practice Competency Exam, Final Exam
Students will be confident in analyzing and examining digital evidence that will stand up to standards required for criminal and/or civil cases.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Practice Competency Exam, Final Exam
Students will obtain knowledge that will allow successful completion of the AccessData Certified Examiner (ACE) certification.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Practice Competency Exam, Final Exam

This Data Recovery & Analysis course will meet every TR from 9:30am-10:45am in the Weisberg Applied Engineering Complex Room 1232 (Digital Forensics Laboratory). The class will consist of lecture/demonstration with accompanying labs and/or exercises. In addition to the required lab manual, materials and readings pertaining to the course will be provided by the instructor.

Students will be given multiple in-class instructor-lab exercises that focus on a variety of digital forensic methodologies. Students will also complete 4 hands-on practical laboratory projects throughout the semester that will enhance mastery of basic digital forensics concepts.

A practice competency exam is also available to take via MUOnline. This exam is equivalent to the AccessData Certified Examiner (ACE) certification exam in terms of structure and complexity. You will be allowed to take the exam as many times as you please during the semester. Your highest grade on the practice competency exam at the end of the semester will be used to calculate your final grade.

At the end of the semester, students will sit for the AccessData Certified Examiner (ACE) certification, which consists of approximately 50 multiple choice questions that covers all of the knowledge points covered throughout the semester. The score obtained in this examination will count as your final exam grade.

Lectures and course materials will be available from MUOnline as they become available. You can log into the course website using your 901 student number at the following address:
www.marshall.edu/muonline

MARSHALL UNIVERSITY
INTEGRATED SCIENCE & TECHNOLOGY DEPT.
Digital Forensics & Information Assurance
IST 449-201- Data Recovery & Analysis
Course Syllabus Outline- Spring 2016

DIGITAL FORENSICS
INFORMATION ASSURANCE

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 (attendance will be taken beginning in Week 2) will result in lost points (2 pt. per class), 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.

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

Social networking Policy

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 (@joshbrunty) and/or join my network on LinkedIn. You can also follow our department through our MU ISAT or MU Digital Forensics Facebook group pages.

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 verifiable, well-documented excuse. 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

Academic Dishonesty includes cheating, fabrication and falsification of data or information, plagiarism, bribes/favors/threats, and complicity (i.e., helping or attempting someone commit an act of dishonesty). As stated in the policy, "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

MARSHALL UNIVERSITY
INTEGRATED SCIENCE & TECHNOLOGY DEPT.
Digital Forensics & Information Assurance
IST 449-201- Data Recovery & Analysis
Course Syllabus Outline- Spring 2016

DIGITAL FORENSICS
INFORMATION ASSURANCE

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" (MU Undergraduate Catalog). If you are found cheating on projects or plagiarizing answers from the Internet or other sources there will be no second chance. In this course, STUDENTS ARE NOT TO "COPY & PASTE" MATERIAL FROM A SOURCE INTO ANY ASSIGNMENT UNLESS SPECIFICALLY AUTHORIZED BY THE INSTRUCTOR. 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 laboratory projects. All laboratory projects are due 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 Thursdays (lab days). 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:
IST449_LastName_FirstInitial_Assignment Name.doc ("IST449_brunty_j_labpractical1.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. 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. Practical 1, 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:

In-Class Exercises/Attendance	25%
Practical Labs (x4)	25%
Practice Competency Exam (x1)	25%
Final Exam (ACE Cert.)	25%

Example:
In-Class Exercises/Attendance (86%)   x .25 = 21.50
Practical Labs (93%)   x .25 = 23.25
Practice Competency Exam (87%)   x .25 = 21.75
ACE Exam-Final (84%)   x .25 = 21.00

87.50 (88% B)

In-Class Exercises/Attendance (25%)
This component factors any in-class hands-on activities for the semester. Attendance will be taken every class accounting to 2 points for each class. Any in-class quizzes, labs, etc. will also be factored into this percentage.

Practical Labs (25%)
There are a total of four (4) practical labs given this semester, each covering a specific component of the FTK Tools Suite. These labs will be due accordingly as outlined in the class schedule below. Each Lab Practical is worth 50 points and will be turned in via MUOnline

Practice Competency Exam (25%)
A practice competency exam is also available to take via MUOnline. This exam is equivalent to the AccessData Certified Examiner (ACE) certification exam in terms of structure and complexity. You will be allowed to take the exam as many times as you please during the semester. Your highest grade on the practice competency exam at the end of the semester will be used to calculate this percentage.

ACE Exam-Final (25%)
At the end of the semester, students will sit for the AccessData Certified Examiner (ACE) certification, which consists of approximately 50 multiple choice questions that covers all of the knowledge points covered throughout the semester. The score obtained in this examination will count as your final exam grade.

CLASS SCHEDULE	Marshall University Dates/ Important Dates/Notes	WEEK
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). Failure to do so will result in a **<u>zero</u>** 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 Module 1- Introduction to Data Recovery & Analysis Module 2: Working with FTK Imager	✓ January 15, Friday Last day to add classes	Jan 11-15

Week 2 Module 2: Working with FTK Imager (Cont.)	✓ January 18, Monday MLK Day - University Closed No Class 1/19, 1/21	Jan 18-22
Week 3 No Class	No Class (NIST OSAC Meeting)	Jan 25-29
Week 4 Module 3: Windows Registry		Feb 1-5
Week 5 Module 4: Registry Viewer	✓ Lab Practical 1 (FTK Imager) Due 2/12 @ 11:59PM ✓ Lab Practical 2 (RV) Distributed	Feb 8-12
Week 6 Module 5: Working with FTK-Part 1	✓ No Class 2/18- AAFS Conference ✓ Lab Practical 2 Due 2/20 @ 11:59PM	Feb 15-19
Week 7 Module 5: Working with FTK-Part 1		Feb 22-26
Week 8 Module 6: Working with FTK-Part 2		Feb 29- Mar 4
Week 9 Module 7: Processing the Case		Mar 7-11
Week 10 Module 8: Narrowing your Focus	✓ Mar 18 (Friday)- Last day to drop a full semester individual course	Mar 14-18
Week 11 No Class-Spring Break	✓ Complete Withdrawals Only (3/21-4/29)	Mar 21-25
Week 12 Module 9: Regular Expressions		Mar 28- Apr 1
Week 13 Module 10: Filtering the Case	✓ Lab Practical 3 (FTK) Lab Due 4/10 @ 11:59PM	Apr 4-8
Week 14 Module 13: Working with PRTK		April 11-15
Week 15 Module 11: The Recycle Bin Module 12: Common Windows Artifacts		Apr 18-22
Week 16 "Dead Week" ACE Exam Review Module 14: Encrypting File System (EFS) Module 15: Case Reporting	✓ Lab Practical 4 (PRTK) Due 4/29 @ 11:59PM ✓ Practice Competency Exam (MUOnline) Due 4/29 @ 11:59PM ✓ April 25-29,"Dead Week"	Apr 25-29

Week 17	✓ Final Exam Time: Tuesday, May 3rd 8:00AM-10:00AM	May 2-6
Final Exam (ACE)		

Syllabus meets requirements set forth by MUBOG Policy AA-14