



#### Instructor

Name: Joshua L. Brunty, ACE, AME, SCERS, CHFI  
Office: Prichard Hall 215  
Office Phone: 304-696-5602 (takes messages)  
Dept. Fax: 304-696-6533  
Email: [josh.brunty@marshall.edu](mailto:josh.brunty@marshall.edu)  
Office Hours: M, W, F (0900-1000hrs) Thurs (0900-Noon)

#### Required Text(s)

AccessData Forensics Training Manual- Academic Edition (3/9/11 Edition) (*Marshall University Bookstore*)

#### Recommended Texts

None

#### Resource Sites

<http://www.accessdata.com/> (Resource Site for Forensic Toolkit-FTK v5)  
<http://www.accessdata.com/training/certifications> (Information & Resources on ACE certification)  
<http://www.accessdata.com/training/online-learning-center-lms> (FTK Certification LMS Login)

#### Course Description

This two (3) credit hour Data Recovery & Analysis course (CRN #2810), 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 v5 (FTK) and its complimentary suite of forensic tools (this software will be made available in the ML121 computer lab).

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

Students will receive emails via MUOnline & 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 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, Midterm 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, Midterm 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 In-Class Laboratory Exercises, Midterm 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, Midterm 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, Midterm Exam, Final Exam
<p>This Data Recovery &amp; Analysis course will meet every MWF from 11:00am-11:50am in Morrow Classroom 121 (Digital Forensics Teaching Lab). The class will consist of lecture/demonstration with accompanying labs and/or exercises. Each student will receive required course materials and readings pertaining to the course.</p> <p>Students will be given multiple in-class instructor-lab exercises that focus on a variety of digital forensic methodologies. Students will also complete various practical laboratory exercises throughout the semester.</p> <p>At the end of the semester, students will sit for the AccessData Certified Examiner (ACE) certification, which consists of approximately thirty-eight (38) 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.</p> <p>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:  <a href="http://www.marshall.edu/muonline">www.marshall.edu/muonline</a></p>		
<b>University Policies</b>		
<p>By enrolling in this course, you agree to the University Policies listed below. Please read the full text of each policy by going to <a href="http://www.marshall.edu/academic-affairs">www.marshall.edu/academic-affairs</a> and clicking on "Marshall University Policies." Or, you can access the policies directly by going to <a href="http://www.marshall.edu/academic-affairs/?page_id=802">http://www.marshall.edu/academic-affairs/?page_id=802</a></p> <p><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></p>		



### 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, 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. Any excused absences must adhere to the University's excused absence policy.

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 by going to [www.marshall.edu/academic-affairs](http://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](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*

### Professionalism/Attendance Policy

This class is considered a hands-on involved course, with some of our time devoted to exploring different types of technology. With that said, any missed classes will result in lost points, 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. Any excused absences must adhere to the University's excused absence policy.

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.

### 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

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.

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

If you are found cheating on projects or plagiarizing answers from the Internet or other sources 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 laboratory projects. All laboratory projects are due BY THE BEGINNING OF CLASS 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\_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.

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 via MUOnline 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	<b>A</b>
80-89	<b>B</b>
70-79	<b>C</b>
60-69	<b>D</b>
0-59	<b>F</b>

Percentage of grades will be distributed as follows:

Practical Labs/Exams	50%
Final Exam (ACE)	50%

#### Example:

ACE Exam-Final (82%)	x .50 =41
Practical Labs/Exams (91%)	x .50 =45.5
	-----
	86.5 (86% B)

CLASS SCHEDULE	Marshall University Dates/ Important Dates/Notes	WEEK CLASS DATE
<b>NOTE:</b> 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). 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:		
<b>Week 1</b> Module 1: Introduction to Data Recovery & Analysis		Aug. 26 <sup>th</sup> -30 <sup>th</sup>
<b>Week 2</b> Module 2: Working With FTK Imager	September 2 <sup>nd</sup> (Mon) Labor Day Holiday – University Closed	Sept. 2 <sup>nd</sup> -6 <sup>th</sup>
<b>Week 3</b> Module 3: Working With Registry Viewer		Sept. 9 <sup>th</sup> -13 <sup>th</sup>
<b>Week 4</b> Module 4: Working w/ FTK-Part 1		Sept. 16 <sup>th</sup> -20 <sup>th</sup>
<b>Week 5</b> Module 5: Working w/ FTK-Part 2		Sept. 23 <sup>rd</sup> -27 <sup>th</sup>
<b>Week 6</b> Module 6: Processing The Case		Sept. 30 <sup>th</sup> -Oct. 4 <sup>th</sup>
<b>Week 7</b> Module 7: Regular Expressions Module 8: Narrowing Your Focus		Oct. 7 <sup>th</sup> -11 <sup>th</sup>
<b>Week 8</b> Midterm Exam (10/14) Module 9: Filtering The Case	Midterm Practical Distributed (10/14)	Oct. 14 <sup>th</sup> -18 <sup>th</sup>



<b>Week 9</b> Module 10: Practical 1 Module 11: Common Windows XP Artifacts	Midterm Practical Due (10/21)	Oct. 21 <sup>st</sup> -25 <sup>th</sup>
<b>Week 10</b> Module 11: Common Windows XP Artifacts (Cont.)	Nov. 1 <sup>st</sup> - Last day to drop a full semester individual course	Oct. 28 <sup>th</sup> -Nov. 1 <sup>st</sup>
<b>Week 11</b> Module 12: Working With PRTK		Nov. 4 <sup>th</sup> -8 <sup>th</sup>
<b>Week 12</b> Module 13: Encrypting Filesystem Module 14- Practical 2		Nov. 11 <sup>th</sup> -15 <sup>th</sup>
<b>Week 13</b> Module 15: Case Reporting		Nov. 18 <sup>th</sup> -22 <sup>nd</sup>
<b>Week 14</b> No Class	Thanksgiving/Fall Break - Classes Dismissed	Nov. 25 <sup>th</sup> -29 <sup>th</sup>
<b>Week 15</b> Final Exam/ACE Certification Review/Practical Exercise	Dec. 2 <sup>nd</sup> - 6 <sup>th</sup> - Dead Week	Dec. 2 <sup>nd</sup> -6 <sup>th</sup>
<b>Week 16</b> Final Exam/ACE Certification Test (Tuesday 12/10 10:15-12:15pm)	December 13 <sup>th</sup> (Fri)- Makeup Day	Dec. 9 <sup>th</sup> -13 <sup>th</sup>



*\*Syllabus meets requirements set forth by MUBOG Policy AA-14*