# Integrated Science & Technology 449
## Data Recovery & Analysis

**Fall 2014**
**Tues/Thurs 11:00 – 12:15**
**Morrow Library 121**

**Instructor** – John Sammons
**Office** – Prichard Hall 208
**Office Phone** – 304 -696-7241
**eMail Address** – john.sammons@marshall.edu

**Office Hours:**
Monday 10:00am – 11:00am
Tuesday 10:00am – 11:00am
Wednesday 10:00am – 11:00am
Thursday 10:00am – 11:00am
Friday 10:00am – 11:00am

### Textbooks

*The Basics of Digital Forensics. The Primer for Getting Started in Digital Forensics*. John Sammons. Syngress; (March 9, 2012). 978-1597496612

AccessData Training Manual. Academic Edition.

### Course Description

In IST 449 introduces students to core digital forensic concepts, common Windows artifacts, and the fundamentals of the forensic examination of digital media using the AccessData suite of tools.

### Credit

The course is three (3) credit hours.

### Pre/co-requisites

IST 264 Technology Foundations

**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 and Mac forensic artifacts. | PowerPoint/Prezi development, peer & instructor review, journal assignments | Presentations, Quiz questions, concept map, high stakes writing assignment, "hot seat" quizzes |
| Students will correctly **apply** the phases of the EDRM in civil litigation. | Case studies and practical exercises, journal assignments | Presentations, Quiz questions, concept map, high stakes writing assignment, "hot seat" quizzes |
| Students will **demonstrate** their ability to communicate effectively both orally and in writing. | PowerPoint/Prezi development, peer & instructor review, journal assignments | Presentations, Quiz questions, concept map, high stakes writing assignment, "hot seat" quizzes |
| Students will correctly **apply** the phases of the EDRM in civil litigation | Case studies and practical exercises, journal assignments | Presentations, Quiz questions, concept map, high stakes writing assignment, "hot seat" quizzes |
| Students will correctly **interpret** common Windows artifacts as they relate to the facts and circumstances of a particular investigation. | Journal exercises, in-class team assignments | Quizzes, "hot seat" quizzes, high stakes writing assignment |
| 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 |

## 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. You will also be responsible for all assigned reading from the "Basics" book. You will be quizzed on that material. 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 |
|---|---|
| Learning Journals | 200 (Approx. Subject to change based on progress) |
| Quizzes | 200 (Approx. Subject to change based on progress) |
| Midterm & Final | 200 |
| **Total** | **600** (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.

*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 e 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. Bb email is the last method 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.

File Names: All electronic submissions must follow this file naming convention:

Ist447_Last Name_First Initial_Assignment Name.doc ("ist447_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 period will not be accepted.

## Attendance Statement

Attendance is very important in this course. Much of this course involves the use of forensic tools that are only available in the lab. If you miss class you will loose out on critical time with the software. This could have an extremely negative impact on your grade. The final exam is the AccessData Certified Examiner test. This test will require you to use the software to analyze computer evidence.

If you miss class, it is your responsibility to catch up on material missed, and it will not be the responsibility of the instructor to catch you up on material missed during office hours, or re-lecture to you. Throughout the semester, there will be in-class assignments that are done for a grade. Those assignments cannot be made up without a university excused absence. Exit slips in the learning journal are one example.

**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.

## University Holidays & Key Dates

**September 1, Monday**
Labor Day – University closed

**October 14, Tuesday - October 17, Friday**
Midterms

**November 24, Saturday – November 29, Friday**
Thanksgiving/Fall Break – Classes Dismissed

**November 27, Thursday – November 28, Friday**
Thanksgiving Holiday – University Closed

**December 1, Monday**
Classes Resume

**December 5, Friday**
Last Day to Drop

**December 1, Monday – December 6, Saturday**
Dead Week

**December 5, Friday**
Last Class Day

**December 6, Saturday – December 12, Friday**
Final Exams

**December 23, Tuesday – January 1, 2015**
Winter Break – University closed

## 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 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. It's 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. 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. Reading assignments are TBA. Please note these topics and schedules are tentative.

| Week | Dates | Topics | Reading |
|---|---|---|---|
| 1 | Aug 25 - 29 | FTK Imager<br>Introduction | Mod 2<br>Chap 1 |
| 2 | Sept 1 - 5 | Windows Registry/ Registry Viewer<br>Key Tech Concepts | Mod 3<br>Chap 2 |
| 3 | Sept 8 - 12 | Windows Registry/ Registry Viewer<br>Key Tech Concepts | Mod 3<br>Chap 2 |
| 4 | Sept 15 - 19 | Working with FTK Part 1<br>Labs & Tools | Mod 5<br>Chap 3 |
| 5 | Sept 22 - 26 | Working with FTK Part 1<br>Labs & Tools | Mod 5<br>Chap 3 |

| | | | |
|---|---|---|---|
| 6 | Sept 29 –<br>Oct 3 | Working with FTK Part 2<br>Collecting Evidence | Mod 6<br>Chap 4 |
| 7 | Oct 6 - 10 | Processing the Case<br>Narrowing Your Focus | Mod 7<br>Mod 8 |
| 8 | Oct 13 - 17 | Midterm/Flex | |
| 9 | Oct 20 - 24 | Filtering the Case | Mod 10 |
| 10 | Oct 27 - 31 | Recycle Bin | Mod 11 |
| 11 | Nov 3 - 7 | Common Windows Artifacts<br>Windows System Artifacts | Mod 12<br>Chap 5 |
| 12 | Nov 10 - 14 | Common Windows Artifacts<br>Windows System Artifacts | Mod 12<br>Chap 5 |
| 13 | Nov 17 - 21 | Working with PRTK<br>Anti-forensics | Mod 13<br>Chap 6 |
| 14 | Nov 24 - 28 | Fall Break | N/A |
| 15 | Dec 1 - 5 | Case Reporting<br>Legal | Mod 15<br>Chap 7 |
| 16 | Dec 8 - 12 | Finals | |

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. 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.

## Learning Journal

As part of this class, each student must maintain a learning journal. This journal will contain a variety of low/medium 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. The journals are graded ALL or NONE. If the journal is complete, you will receive full credit. Missing entries will result in a 0. You will be responsible for all the entries listed in Bb.

Do NOT procrastinate. You will need your journal during almost every class. It is your responsibility to ensure that it's available and 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

There will be an online quiz for each chap and module assigned in the syllabus. You will be expected to complete these outside of class. You will be permitted up to three attempts for each with only the highest score counting.

The number of quizzes may vary, depending on class progress, participation, and the how well students keep up with assignments, readings, etc. Students are expected to keep up with all reading assignments and come to class prepared to discuss the material.

The final exam will be 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 your not fumbling around during the test.

## 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 CORRESPONDENCE. Messages left on Blackboard will result in delayed responses. Please read and follow the guidelines outlined in the "How to Email Your Professor" article. There is a link to it posted on Bb. 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.

## 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.

## 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

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, 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.

## NOTES::