

**Computer Forensics I**  
**IA327 – Fall 2008**  
**Mike Yauk**

**Course Information**

**Instructor: Mike Yauk**

**Office: 14 Roosevelt Hall**

**Office Hours: By appointment only**

**Campus Phone: 734-487-1590**

**E-mail: myauk@emich.edu**

**Course Web site: my.emich.edu groups website**

**Classroom: 6 Roosevelt Hall**

**Class Times: Wednesday 5:30pm to 8:10pm, 09/03/2008 to 12/10/2008**

**Final Exam: Wednesday 5:30pm to 8:10pm, 12/17/2008**

**Prerequisites:**

**Course Description:**

*Computer Forensics I* addresses the comprehension and application of Computer Forensic Investigations. Students will evaluate and synthesize technical and legal issues in relation to digital evidence. Students will apply various skills and techniques, combined with numerous investigative software tools to analyze seized electronic media. Students must comply with special admission requirements prior to taking this course. Specific topics covered may include:

- Computer Forensics and Investigations as a Profession
- Understanding Computer Investigations
- The Investigator's Office and Laboratory
- Current Computer Forensics Tools
- Processing Crime and Incident Scenes
- Digital Evidence Controls
- Working with Windows and DOS Systems
- Macintosh and Linux Boot Processes and Disk Structures
- Data Acquisition
- Computer Forensic Analysis
- Recovering Image Files
- Network Forensics
- E-Mail Investigations
- Becoming an Expert Witness and Reporting Results of Investigations

**Textbooks:**

*Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, NCJ 199408. NIJ, April 2004.

*Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, NCJ 219941. NIJ, April 2008.

**Supplemental Material\*\*:**

*Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*, NCJ 211314. NIJ, January 2007.

*Investigations Involving the Internet and Computer Networks*, NCJ 210798. NIJ, January 2007.

\*\*Additional Supplemental Material will be made available throughout the course. You must utilize a “thumb drive” for digital material distributed during class. It is suggested that this “thumb drive” be used only for CF1.

### **Grading and Evaluation Criteria**

Sixty percent of your grade will be based on a midterm and a final examination. Both examinations are cumulative and are given in a varied format. An in-class review will be held before each examination.

Thirty percent of your grade will be based on a presentation given by you on a topic within digital forensics. Several topics will be presented in upcoming courses for you to choose from. These projects must be approved in advance. The presentation must be at least 10 minutes and must utilize some form of visual aid.

### **Suggested topics for Presentation**

Forensic Certifications	PDA Forensics
Cell Phone Forensics	Evidence Elimination Tools
Bit-locker and Computer Forensics (Vista)	Steganography
Handheld imaging devices	Onsite Forensic Preview
Other Forensic Tools	Other Forensic Training
Metadata	Policy and Procedure

The remaining ten percent will be based on participation and on in class activities. Students are encouraged to utilize a small 3 ring binder to use as a lab notebook during in class hands-on activities. Similar activities may be used later on the midterm or final examination.

### **Grading:**

Grades will follow the percentage scale given below.

A	100-93%	C+	78-79%	D-	60-62%
A-	90-92%	C	73-77%	E	<60%
B+	88-89%	C-	70-72%		
B	83-87%	D+	68-69%		
B-	80-82%	D	63-67%		

### **Absence and Make-Up Policy:**

Class materials will be available but additional tutoring will be at the discretion of the Professor. Tests or assignments missed without prior arrangement may be taken late at a mutually agreed upon time and discounted by 30%, e.g. a score of 88% would be lowered to 58%.

### **Incompletes:**

An incomplete (I) grade will be given only in the case of serious health problems or particularly unusual circumstances.

### **Acceptable Use Technology Policy:**

We will follow the Acceptable Use Policy of Eastern Michigan University posted on the university web page.

<http://ict.emich.edu/policy>

### **Web site**

Supplementary information for the course is available at our **my.emich.edu group**. The web site will contain class notes, PowerPoint slides, class announcements, course syllabus, test dates, and other information for the course.

## Course Schedule\*\*

Week	Date	Topics	Readings	Exams
1	3-Sep	Class Introduction; What is Computer Crime?; Introduction to Computer Forensics and Search and Seizure	ECSI	
2	10-Sep	Setting up your Forensic workstation; Introduction to FTK Imager and Diskedit	FTK Imager Manual,	
3	17-Sep	Binary, ASCII, Decimal;	Class Handout / Activity	
4	24-Sep	Physical characteristics of digital storage media & Partitioning Concepts	FEDE	
5	1-Oct	Boot Process & Drive letter assignments	Class Handout	
6	8-Oct	FAT File System, Review		
7	15-Oct	Disk Write Protection & Disk Acquisition		Mid-Term
8	22-Oct	Working with FTK Imager & Introduction to FTK		
9	29-Oct	Working with FTK Imager & Introduction to FTK		
10	5-Nov	Working With FTK	FTK Manual	
11	12-Nov	Windows Investigations and Analysis		
12	19-Nov	Windows Investigations and Analysis		
-	26-Nov	NO CLASSES CAMPUS OPEN		
13	3-Dec	Presentations		
14	10-Dec	Case Reporting, Review		
15	17-Dec	Final Exam		Final Exam

Electronic Crime Scene Investigation = ECSI

Forensic Examination of Digital Evidence = FEDE

Investigations Involving the Internet and Computer Networks = I3CN

Digital Evidence in the Courtroom = DEC

\*\*Schedule is subject to change based on semester progress. Students will be informed of any changes as they occur.