

Computer Forensics II
IA328 – Winter 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 8:00pm, 01/09/2008 to 04/23/2008

Prerequisites: Successful completion of Computer Forensics I, IA 327

Course Description:

Computer Forensics II is the continuation of IA327, Computer Forensics I. This class will continue to build upon computer forensics fundamentals, and introduces the NTFS file system. Additionally, this class will expand the “investigators” understanding in investigating Microsoft Windows Operating Systems. This could potentially involve system artifacts such as internet history, user preferences, the registry, link files, etc. We will also address additional computer forensic software suites such as Access Data’s Ultimate Tool Kit and ProDiscover Basic.

Students must comply with special admission requirements prior to taking this course.

Specific topics covered may include:

- Hardware Validation
- Software Validation
- Current Computer Forensics Tools
- NTFS File Systems
- Microsoft OS System Artifacts
- Microsoft OS User Artifacts
- Macintosh and Linux Boot Processes and Disk Structures
- Microsoft Vista

Textbook: Kruse, Warren *Computer Forensics: Incident Response Essentials*. Addison-Wesley Professional, 2001, ISBN 0-201-70719-5

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.

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

Electronic Crime Scene Investigation: A Guide for First Responders, NCJ 187736. NIJ, July 2001.

**Copies of Supplemental Material will be distributed in class. It is suggested that you utilize a “thumb drive” for other digital material distributed during class.

Grading and Evaluation Criteria

Seventy five 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.

20 percent of your grade will be based on (4) assignments geared toward current discussion topics.

Assignments**

Assignment #1- Write Protection Validation

Using our procedures from the testing and validation of an IDE write protection device, create your own “white paper” testing and validating the USB software write protection method.

Assignment #2- TBD

Assignment #3-TBD

Assignment #4-TBD

***Assignments are subject to change based on semester progress. Students will be informed of any changes as they occur.*

The remaining five 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. Student averages will be made available periodically during the course indexed by student ID#.

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	Chapter Readings	Exams & Assignments
1	9-Jan	Course Introduction, System Preparation, Hardware Validation		
2	16-Jan	Hardware Validation, Software Validation		
3	23-Jan	Review FAT, Introduction NTFS		Assignment #1 Due
4	30-Jan	NTFS		
5	6-Feb	Windows OS Artifacts		
6	13-Feb	Windows OS Artifacts Cont...		
7	20-Feb	Windows OS Artifacts Cont...		
-	27-Feb	NO CLASSES (Campus Open)		
8	5-Mar	Midterm Review		
9	12-Mar	Midterm, Forensic Tool Comparison		Midterm
10	19-Mar			
11	26-Mar			
12	2-Apr	VISTA Artifacts**		
13	9-Apr	Macintosh and Linux File Structures **		
14	16-Apr	Final Exam Review		
15	23-Apr	Final Exam		Final Exam

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