

The University of Maryland Asian Division  
**IFSM 498Xg - Introduction to Digital Evidence and Computer Crime**

TERM 3  
July 12 & 13, 2008  
Saturday/Sunday 0900-1730

Syllabus

INSTRUCTOR: BJ Gleason  
Phone: 723-4300  
E-Mail: bjgleas@gmail.com  
Website: <http://thinairlabs.com>  
Office Hours: Before and After Class, by appointment.

TEXTBOOKS: Solomon, Barrett, & Broom (2004) Computer Forensics JumpStart, Sybex, ISBN: 078214375X  
**Due to the nature of the class, students should read the book before class begins.**

PREREQUISITE: IFSM 310 or CCJS 105, or permission of the instructor. This is a fairly technical class, so students should feel comfortable operating computers. This should *not* be your first computer class. If you have any questions, please contact the instructor.

COURSE DESCRIPTION: This course covers the relevant background and terminology, legal issues that arise in computer related investigations, and presents a systematic approach to investigating a crime based on the scientific method. Topics include file systems, data recovery, Internet traces, as well as procedures and tools for properly collecting and examining digital evidence. This course demonstrates how computers are extensions of traditional crime scenes and how digital evidence can be useful in a variety of investigations including computer intrusions and violent crimes.

EQUIPMENT: It is *highly* recommended that students have access to a computer running Windows 2000/XP, with a floppy drive and CD-ROM drive so they can complete the homework assignment. Students should bring a 256MB USB drive.

INTERNET ACCESS: Students will be expected to have e-mail and Internet access. Most of the assignments will require extensive use of these resources.

COURSE OBJECTIVES: On successful completion of this course, the student should be able to:

- Understand concepts of Storage Media and Data Hiding, File Systems and Location of Data
- Understand Computer Investigations techniques, including Authorization and Preparation, Documentation, Collection and Preservation, Examination and Analysis, and Reconstruction.
- Understand and apply knowledge using Digital Evidence Processing Tools
- Become familiar with basic Windows Data Recovery, Log Files, and Internet Traces

EVALUATION:

Attendance / Participation	10%
Quizzes	20%
Assignments	40%
Final Examination	30%

POLICIES, PROCEDURES AND GRADES: IAW with the University of Maryland, University Catalog, Asian Division, and the Student Handbook (current editions). These cover essential information such as attendance, grading, make-up work and plagiarism.

ATTENDANCE: Because much of the material in this class consists of in-class group problem solving activities, class

attendance is essential. Students are expected to attend all scheduled classes. However, if a student must miss a class due to military obligations or other unavoidable circumstances, every effort must be made by the student to obtain class notes and other material discussed. Communication with the instructor is vital and the student should notify the instructor of any anticipated absences. **There are NO makeups for missed assignments or examinations unless the instructor is informed ahead of time. Attendance is taken only at the beginning of class.**

**HOMEWORK: All assignments must be turned in at the beginning of class on the due date.** In the event of bonafide duty-related absence on the due date, arrangements must be made with the instructor in advance. **Homework is not accepted late.**

**PLAGIARISM POLICY:** Plagiarism is defined: to steal or use the ideas or writings of another as one's own. This may be avoided in most instances by giving credit/recognition to the original author. The University of Maryland, Asian Division's standard plagiarism policy is: intentionally plagiarized papers, reports, or exams will receive an F or 0 (zero), whether copied whole or in part. Subsequent cases of plagiarism can result in failure in the course. Unintentional plagiarism - cases arising from student inexperience rather than deliberate deception can result in a lower grade on papers than they might otherwise deserve.

**MISCELLANEOUS:** Students will be required to use a computer and associated software to complete course assignments. Software unique to the course will be introduced in during the class meetings. However, students will be expected to make a determined effort to learn to use course unique programs on their own.

**HAND PHONES, BEEPERS:** Are to be tuned off before class begins. Emergency personnel should set their devices to a setting that will not disturb the class.

**SCHEDULE:** *Schedule is subject to change, however all subjects will be covered. See website for current version.*

Week	DISCUSSION TOPICS
Day 1 Morning	Introduction History and Terminology of Computer Crime Investigation Computer Basics for Digital Evidence Examiners In Class: Evidence Collection Exercise
Day 1 Afternoon	Applying Forensic Science to Computers In Class: Evidence Analysis Exercise using WinHex Homework: Unknown File Analysis
Day 2 Morning	Forensic Examination of Windows Systems In Class: File Recovery
Day 2 Afternoon	Digital Evidence in the Courtroom In Class: System Examination Final Exam

**Prerequisite Quiz: Are you ready for this class?**

1. A sector on a floppy disk is typically \_\_\_\_\_ bytes.
2. Before the police can search a suspect's house, they typically require a \_\_\_\_\_.
3. How many bytes are in a 1K?
4. Self-incrimination is prohibited by the \_\_\_\_\_ amendment to the United States Constitution.
5. How many hard drives can connect on a single IDE channel?