



Lawrence Technological University  
College Of Management



MIS 5213 – Cyber Crime: First Responders

<b>Course Title:</b>	MIS 5213 – CyberCrime: First Responders
<b>Semester:</b>	Fall 2007
<b>Dates:</b>	100% Online Course, September 5 <sup>th</sup> to December 15 <sup>th</sup>
<b>Important dates to remember</b>	Sept 17 - Last day to drop with tuition credit Sept 18 - Withdrawal period begins; late transaction fee for added courses Nov 14 - Last day to withdraw Nov 21 - Last day of classes before Thanksgiving break Nov 26 - Classes resume Dec 8 - Last day of classes before Final Exams Dec 15 - End of Fall 2007 term
<b>Instructor Contact Information:</b>	Kamal Kakish proffkakish@gmail.com 248-703-6882
<b>Technical Support:</b>	LTU Help: ph. 248-204-4000 After-hours Blackboard Technical Support: 1-888-383-6570. (Identify yourself as a LTU student using Blackboard.)
<b>REQUIRED TEXT</b> <b>(See Blackboard for additional resources)</b>	<u>Guide to Computer Forensics and Investigations. Second Edition.</u> Phillips, Nelson, Enfinger, Stuart. Course Technology Incorporated, 2006, ISBN 0-619-21706-5 <u>Pocket Guide to APA Style</u> , by Robert Perrin, Houghton Mifflin Publishers, ISBN 0-618-30820-2.

Purchase from LTU Bookstore at  
<http://lawrence-tech1.bkstore.com/bkstore/TextbookSelection.do?st=489>

*Supporting Texts (Optional)*

Cyber Crime Investigations, by Kevin O'Shea et. al., 2007, Syngress Publishing, 2002, ISBN: 1-59749-133-0

Scene of The Cybercrime: Computer Forensics Handbook, by Debra L. Shnider & Ed Tittel, Syngress Publishing, 2002, ISBN: 1-931836-65-5

*Additional Resources*

ISO/IEC 17799 – Information Technology – Code of practice for Information Security management

NSA/IS 17799-2 – Information Security Management Systems – Part 2: Specification with Guidance for Use

LTU Online student resources

<http://www.ltu.edu/ltuonline/currentonline.asp>

Course-specific information is provided in the "Course Information" area

Technical support for using Blackboard is provided by the LTU Help Desk, 248-204-2330 or [vitrc@ltu.edu](mailto:vitrc@ltu.edu), 248-204-3750

**ADDENDA**

**TECHNICAL SUPPORT**

**Description of Course:**

*Guide to Computer Forensics and Investigation* presents methods to properly conduct a computer forensics investigation, beginning with a discussion of ethics while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. Specific topics covered 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

**Course Prerequisites:** Intro to Computer Forensics Methodology

Students should have a working knowledge of hardware and operating systems (OSs) to maximize their success on projects and exercises throughout the text.

**Learning Objectives/Outcomes:**

The course will give you the information needed to recognize, respond, investigate and manage cyber crime incidents. The emphasis will be focus around the Terrorists, Hackers, High Tech Criminals and Computer Forensics methodology that relates to the cybercrime investigations of computer crimes and incidents.

**Instructional Methods and Course Organization**

A variety of instructional methodologies are used in this course, which may include but are not limited to:

*Blackboard learning environment* – Blackboard at [my.ltu.edu](http://my.ltu.edu) contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.

*Student/Instructor Conversations* – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.

*Required readings* – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.

### **Class Policies and Expectations**

I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:

Each student has a LTU e-mail account. If you wish to use a different e-mail address for this course, please change your e-mail address in Blackboard under “Student Tools” and send an e-mail to me so I can store your address in my e-mail directory.

Readings, discussion forum participation, and written assignments must be completed according to the class schedule. If business travel will take you away from regular participation, please clear these dates with me in advance.

It is essential that all students actively contribute to the course objectives through their experiences and working knowledge of business and IT.

All assignments must be submitted on schedule, via Blackboard, and using Microsoft Office-compatible software. If you need to submit an assignment via e-mail, contact the instructor in advance. **Since most assignments in this course will be graded as part of the electronic binder that you will submit the last week of the course, the honor code will be applied. A sample Electronic Binder is included at the end of this syllabus for your convenience.**

Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus and on the LTU Online web site.

Be prepared to log into Blackboard at least **once each day**. Please focus your online correspondence within the appropriate Blackboard discussion forums so that your colleagues can learn from you as well.

Please review and understand the **Online Participation Guidelines document** which is available in Thread #1 under the Discussion Forum in BB.

At the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I encourage you to participate in the evaluation process.

The topics listed in the syllabus are only an estimate of the material, which can be covered during the semester. Some topics might be deleted and some others might be added at the

discretion of the instructor. Teamwork and collegiality are encouraged but everyone must understand and be responsible for their work, actions and work products; observations of the Honor Code Policy are mandatory. [http://www.ltu.edu/currentstudents/honor\\_code.asp](http://www.ltu.edu/currentstudents/honor_code.asp) All other University policies regarding incomplete grades, etc. apply.

### **Academic Integrity:**

This course falls under the provisions of the policies on academic integrity of LTU. Any violations of this policy will result in failure. Students are encouraged to utilize the Safe Assign tool within Blackboard to insure their writings meet the provisions of this policy.

### **Online Participation:**

Students are expected to actively participate online using the Bb Discussion Board. The due date for each discussion thread is ONE week after the associated chapter(s) is scheduled according to the class calendar below.

Assignments:

All assignments should be delivered electronically via the Blackboard View/Submit Assignment function located under "Assignments". If technical difficulties are encountered, you can send the assignment via e-mail to [profkakash@gmail.com](mailto:profkakash@gmail.com), but only as a last resort. Assignments are due on or before the date assigned. Late assignments will cause a 10% per day deduction from the value of the assignment.

It is important for you as students to know what to expect from me as your instructor:

- I will be available to you via e-mail and phone, and will promptly reply to your messages within 24 hours or less.
- I will NOT be available to you for face-to-face appointments (I do not live in Michigan), but will use Wimba Live Classroom for synchronous discussions as requested.
- I will maintain the Blackboard web site with current materials, and will resolve any content-related problems promptly as they are reported to me.
- I will send out a weekly e-mail update to all class members to guide upcoming work and remind you of assignment due dates.
- I will return all assignments to you promptly, and will include individualized comments and suggestions with each assignment.
- I will hold our personal written or verbal communications in confidence. I will not post any of your assignments for viewing by the class without requesting your approval in advance.
- **I will treat all members of the class fairly, and will do my best to accommodate individual learning styles and special needs.**

If any of these points need clarification, or when special circumstances arise that require my assistance, please contact me so that we can discuss the matter personally.

### **Course Schedule**

This fully online course begins with a one-week online course orientation period to familiarize yourself with the online learning environment and to meet online or via phone with your instructor. Each week starts on a Monday and ends on a Sunday.

Dates	Modules	Topics / Readings	Assignments Due
-------	---------	-------------------	-----------------

Dates	Modules	Topics / Readings	Assignments Due
<b>Prior to Start of Semester and Week of Sept 6-9</b>	Module 0	Overview of textbook Online Learning Orientation	Bb Forums Student Data Sheets Assignment A0 – Post to D0
Week of Sept 10 – Sept 16	Module 1	Computer Forensics and Investigations as a Profession	Chapter 1 Bb Forums D1 Quiz: Q1 Project Notebook: Assignment A1 – put in your Electronic Notebook Due by 11:59pm on 9/23/07
Week of Sept 17 – Sept 23	Module 2	Understanding Computer Investigations	Chapter 2 Bb Forums D2 Quiz: Q2 Project Notebook: Assignment A2 – put in your Electronic Notebook Due by 11:59pm on 9/23/07
Week of Sept 24 – Sept 30	Module 3	The Investigator's Office and Laboratory	Chapter 3 Bb Forums D3 Quiz: Q3 Project Notebook: Assignment A3 – put in your Electronic Notebook Due by 11:59pm on 9/30/07
Week of Oct 1 – Oct 7	Module 4	Current Computer Forensics Tools	Chapter 4 Bb Forums D4 Quiz: Q4 Project Notebook: Assignment A4 – put in your Electronic Notebook Due by 11:59pm on 10/7/07
Week of Oct 8 – Oct 14	Module 5	Processing Crime and Incident Scenes	Chapter 5 Bb Forums D5 Quiz: Q5 Project Notebook: Assignment A5 – put in your Electronic Notebook Due by 11:59pm on 10/14/07
Week of Oct 15 – Oct 21	Module 6	Digital Evidence Controls	Chapter 6 Bb Forums D6 Quiz: Q6 Project Notebook: Assignment A6 – put in your Electronic Notebook Due by 11:59pm on 10/21/07
Week of Oct 22 – Oct 28	Module 7	Working with Windows and DOS Systems  <b>Mid Term Exam</b>	Chapter 7 Bb Forums D7 M1 Available from 6:00 a.m. to 11:00 p.m. on Monday 10/22/2007 Mid-Term Evaluation
Week of Oct 29	Module 8	Macintosh and Linux Boot Processes and	Chapter 8

Dates	Modules	Topics / Readings	Assignments Due
– Nov 4		Disk Structures	Bb Forums D8 Quiz: Q8 Project Notebook: Assignment A8 – put in your Electronic Notebook Due by 11:59pm on 11/4/07
Week of Nov 5 – Nov 11	Module 9	Data Acquisition	Chapter 9 Bb Forums D9 Quiz: Q9 Project Notebook: Assignment A9 – put in your Electronic Notebook Due by 11:59pm on 11/11/07
Week of Nov 12 – Nov 18	Module 10	Computer Forensic Analysis	Chapter 10 Bb Forums D10 Quiz: Q10 Project Notebook: Assignment A10 – put in your Electronic Notebook Due by 11:59pm on 11/18/07
Week of Nov 19 – 25	Module 11	Happy Thanksgiving!	Nothing! Enjoy a Break and Give Thanks!!!
Week of Nov 26 – Dec 2	Module 12	Network Forensics	Chapter 12 Bb Forums D12 Quiz: Q12 Project Notebook: Assignment A12 – put in your Electronic Notebook Due by 11:59pm on 12/2/07
Week of Dec 3 – Dec 9	Module 13	E-Mail Investigations	Chapter 13 Bb Forums D13 Quiz: Q13 Project Notebook: Assignment A13 – put in your Electronic Notebook Due by 11:59pm on 12/9/07 Mid-Term Evaluation
Week of Dec 10 – Dec 15	Module 14	Becoming an Expert Witness and Reporting Results of Investigations Review <b>Final Exam</b>	Chapter 14 Bb Forums D14 F1 – Final Exam Available from 6:00 a.m. to 11:00 p.m. on Monday 12/10/2007 Last Chance to turn in any late work

### Student Evaluation

30% of the grade is based on a midterm and a final examination. Both examinations are cumulative and are given in a varied format.

15% of the grade is based on quizzes. Quizzes may vary from three to five questions that may be in any format.

30% of the grade is based on keeping a project notebook. Students are asked to obtain a small electronic notebook (such as MS OneNote 2003, MS Word, or similar SW) or to use a lab notebook and keep notes on the results of the hands-on activities within each chapter and the hands-on and case projects at the end of each chapter in the text. **Please note that you are NOT required to submit any of these assignments online. You should “keep” all of your assignments in the *electronic project notebook* which you will submit to me at the end of the semester. There is a sample electronic project notebook at the end of this document for your convenience.**

25% of the grades is allocated to online participation – The Discussion Board – D0 to D14. Please make sure you read the ONLINE PARTICIPATION GUIDELINES document, which is found in the discussion forum of BB.

Letter grades are awarded based on the total number of points achieved (right column). Points are deducted for late assignments.

Assignments, Quizzes, Exams	Points
A0 – Student Introduction	5
Midterm Exam Chapters 1-7	15
Final Exam Chapters 8-14	15
Q1 – Q14	15
Online Participation Online Forum Discussions on Bb	25
Project Notebook (Contains All Assignments)	30%
Total	100

Class Points	Letter Grade
96 and above	A
90 – 95	A-
87 – 89	B+
83 – 86	B
80 – 82	B-
77 – 79	C+
73 – 76	C
70 – 72	C-
61 – 70	D
60 and below	E

**Note: Grades lower than “B” fall below the LTU graduate standard**

### Practical Guidelines for Class Load Expectations

A three-credit graduate course generally requires at least nine hours per week of time commitment. Here are some practical guidelines to help schedule your time commitments for this online course:

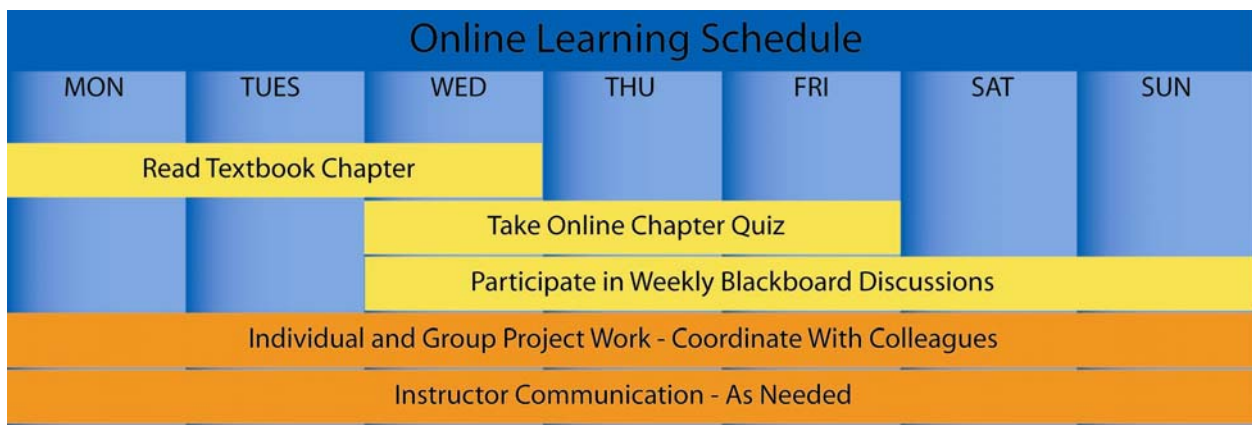
A 14-week semester (the Summer “E” semester is compressed into 11 weeks) would require at least 126 hours of time commitment to successfully complete all readings, activities, assignments, and texts as described in this syllabus.

You should reserve at least 6 hours per week to read the required textbook chapters and resources, participate in online discussions, review presentation materials, and work through online quizzes. This effort will total at least 84 hours over the course of the semester.

You should organize your remaining time to roughly correspond with the point value of each major assignment. This means that you should plan to spend at least:

8-9 hours preparing your case study review;  
 24-40 hours working with your group on the three parts of your semester-long project; and  
 8-9 hours working on the various components of your reflective consolidation (final exam).

These guidelines may not reflect the actual amount of outside time that you – as a unique individual with your own learning style – will need to complete the course requirements. The number of hours each week will vary based on assignment due dates, so please plan ahead to insure that you schedule your academic, work, and personal time effectively. The following graphic can be used to guide you in planning your weekly course work to remain on schedule:



### Assignment Details

Course assignments and evaluation criteria are detailed below. Please review these requirements carefully. See the section Academic Resources / Assessment Guidelines for information about assessment of written and oral presentations.

Details for all assignments are shown below. Please note that you should **not** submit any assignments to the Blackboard "Digital Drop Box." All assignments should be compiled inside the **electronic project notebook** and submitted during the LAST WEEK using the Blackboard "Assignments" function. Some assignments are also posted to the Blackboard Discussion Forum for student comments.

Please see the Assignments Section in BB for the details.

#### A1: Introduction Activity

Individual Assignment

Applying the assignment guidelines, students will post a photo and a brief personal introduction between 50 to 100 words

#### A2: Completing and Critiquing A Case

Here you need to complete and critique a cyber-crime case:



## Completing the case

- Take note of these guidelines on how to write an investigation final report:
  - State what you did and what you found
  - Show conclusive evidence for proving a suspect guilty or innocent
  - You can even include logs from forensic tools to support your points and show every single step you took when investigating the case
- Make a clear point that, if by repeating the process describe on a report you cannot achieve the same results, that work has no value as evidence.
- Also remember that the final report should be prepared accordingly to the expected readers.

## Critiquing the Case

- You can make a self-evaluation of your work by answering the following questions:
  - How could you improve your participation in the case?
  - Did you expect the results you found?
  - Did the case develop in ways you did not expect?
  - Was the documentation as thorough as it could have been?
  - What feedback has been received from the requesting source?
  - Did you discover any new problems? What are they?
  - Did you use new techniques during the case or during research?

### **A3: Small Project**

For this assignment, you may do ONE of the two projects:

Make an evaluation of the ergonomic situation of the computer lab you are working in right now.

OR

Investigate several low emanation workstation brands and find their advantages and disadvantages.

### **A4: Small Project**

For this Assignment, you may do ONE of these 2 projects:

Analyze the content of a Microsoft Outlook PST file. Can they read its contents?

OR

Investigate the major characteristics of USB 2.0 and FireWire ports.

### **A5: Small Project**

For this assignment you should do only ONE of these 2 projects:

Develop a policy that stipulates a corporate right to conduct investigations on its computer assets.

OR

Investigate appropriate warrant wording for a computer investigation from the local policy department.

### **A6: Small Project**

You may do ONE of these 2 projects:

Read about security problems on MD5. Why was MD5 successfully broken? What does it mean for MD5 not being collision resistant?

OR

Investigate "Bag and Tag" recommendations from at least two different sources.

### **Online Participation (25 points)**

Each student is expected to actively participate in online activities. Class participation is evaluated to a maximum of 25 points based on actively participating in Blackboard discussion forums, responding to questions posted by the instructor, and interacting positively with other students.

## Sample Electronic Binder

With exception to assignment A0: introduce yourself to the class, the electronic binder should contain all other assignments: A1 – A14. Assignments can be found in the Assignments Section of BB and in the Practice Folder of each Module.

Assignment #: A2

Assignment due date: get this date from the schedule

Actual completion date: write down the date when you finished the assignment.

Assignment Requirements: Completing and Critiquing A Case

Assignment Deliverables: This is where you answer the assignment and put the contents.

What I learned from doing this assignment: jot down your thoughts and what you learned in a brief and concise manner.

Assignment #: A3

Assignment due date: 11:59pm on 9/30/07.

Actual completion date: write down the date when you finished the assignment.

Assignment Requirements: A small project. Write down which of the 2 projects you selected to work on.

Assignment Deliverables: This is where you answer the assignment and put the contents.

What I learned from doing this assignment: jot down your thoughts and what you learned in a brief and concise manner.

.....