INSE6610: Cybercrime Investigations
TENTATIVE COURSE OUTLINE
(Revision 1.1)

INSE6610 FALL 2015
Instructor: Serguei A. Mokhov mokhov@ciise.concordia.ca

Instructors

Lectures
• S. Mokhov (Sec. UU, Tuesdays, 17:45–20:15, H-1070)

Office hours
Office hours are by appointment. Contact me in class or by email mokhov@ciise.concordia.ca
to set one up.

Course Coordinator
Dr. Debbabi is the coordinator for this term. He can be contacted at debbabi@ciise.concordia.ca.

Course

Description Quoted from the Academic Calendar
Introduction to cybercrimes: unauthorized access, mischief to data, possession of hacking tools,
possession of child pornography; Legal aspects: Canadian judicial system, computer crime laws,
charter of rights, common law, mutual legal assistance treaty, search warrants, production and as-
sistance orders, international laws, upcoming legal changes; Investigation process: search planning,
acquisition methods, environment recognition, evidence identification; Reporting process: inves-
tigation and analysis reports, notes taking; authority of seizure; forensic interviews; Computer
crime trials: witness preparation, court sentencing, rebuttal witness, cross-examination, testimony,
credibility attacks; in-depth case studies. A project.
Note: Students who have received credit for INSE 691E (Cybercrime Investigations) may not take
this course for credit.

Objectives
The course introduces best practices of the industry along with case studies when confronted with
computer crimes. Through a practical assessment, we will analyze in great details the Canadian
judicial system and how to successfully be recognized as an expert witness and how to give such a testimony before the court. We will cover the different steps involved in the making of a search warrant and how to handle the evidence gathered following the search. We will address the prominent methods that are used to conduct computer crime investigations. We will see how to involve different partners in an ongoing investigation as well as using the legal methods in place to move your investigation to an international level. We will also study the techniques used in suspect interviews as well as extracting the maximum information from your witnesses. We will study the needed steps to achieve a full investigation report.

Learning Outcomes

This course aims to give students a good grasp of cybercrime investigations, Canadian computer crime laws, and best practices of the industry, presenting a full investigation report and also properly testifying as an expert witness. By the end of the course, the students will learn about:

- Case studies
- Search warrants
- Court testimony
- Investigation steps
- Interview techniques
- Canadian laws and upcoming changes
- Practical and formal aspects of digital forensic investigation and forensic computing

Textbook

The primary textbook used for the course is [1]. The book, as as a coursepack, was specifically compiled by Patrick Boismenu for this course and is available at Concordia Bookstore.

Suggestions for additional readings will be provided for each lecture topic. There are additional useful resources on the subject that we may refer to for one concept or another throughout the class. They are listed under the “References” section: [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22].

Drop Deadlines

- DNE: Monday, September 21, 2015
- DISC: Sunday, November 8, 2015
Tentative Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>What (lecture time)</th>
<th>Deliverable</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Week of</td>
<td>Course Introduction. Introduction to investigations and the Canadian Justice System.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Sep 11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Week of</td>
<td>Canadian computer crimes laws</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Sep 18</td>
<td>C.E.R.T.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Week of</td>
<td>Cybercrime case study</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Sep 25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Week of</td>
<td>Warrants; production and assistance orders.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Oct 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Week of</td>
<td>Technological crime search planning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Oct 9</td>
<td>Evidence identification.</td>
<td>Quiz 1</td>
<td>Fri, Oct 9, in class</td>
</tr>
<tr>
<td>6</td>
<td>Week of</td>
<td>Forensic analysis, lessons learned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Oct 16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Week of</td>
<td>Cybercrime case study</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Oct 23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Week of</td>
<td>Investigation Report, Analysis Report</td>
<td>Quiz 2</td>
<td>Fri, Oct 30, in class</td>
</tr>
<tr>
<td></td>
<td>Fri, Oct 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Week of</td>
<td>Computer crime interviews, cybercrime</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Nov 6</td>
<td>Community policing, court sentencing impacts.</td>
<td>DISC deadline</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Week of</td>
<td>Cybercrime case study</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Nov 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Week of</td>
<td>Computer crime trials, practical assessment review.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Nov 20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Week of</td>
<td>Cybercrime case study</td>
<td>Final Quiz 3</td>
<td>Fri, Nov 27, in class</td>
</tr>
<tr>
<td></td>
<td>Fri, Nov 27</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Week of</td>
<td>Formalism in cybercrime investigations, Formal modeling, and event reconstruction</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fri, Dec 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Week of</td>
<td>(Possibly makeup class)</td>
<td>Project due</td>
<td>Tue, Dec 8 via EAS</td>
</tr>
<tr>
<td></td>
<td>Tue, Dec 8</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administrative Policies

Grading

Grades will be based on the following components:

1. Quizzes [60%]: 3 quizzes (1-hr each, closed book), 20% each
2. Project [40%]: one nearly course-long group project
3. Failing grade: lack of regular effort will result in the failing grade. Specifically, in order to pass the course you must receive at least 50% of the overall possible marks.

NOTE: Should you fail to write a quiz and you have a valid justification (e.g., doctor’s note) then the weight of the quiz in question will be added to another quiz on the case-by-case basis.

NOTE: There is no a priori rule for translation of a numerical grade to a letter grade. Electronic submission is expected via EAS [https://fis.encs.concordia.ca/eas](https://fis.encs.concordia.ca/eas). Additional details will be given in the class or via the mailing list. Students should be aware of the University’s Code of Conduct (academic) as specified at the Academic Integrity web site, especially the parts concerning cheating, plagiarism, and the possible consequences of violating this code.

NOTE: This course outline is tentative, i.e., subject to changes and adjustments as we go along.
Contribution
In usual circumstances, it is expected that all members of a group end up with the same project mark. However, this must not be considered as a rule. For reasons of fairness, different evaluations will be considered to award those who provided outstanding input to the project, and to penalize those who provided minimal (below expectations) input to the project in case of disputes within the team. The team members would be expected to provide individual logs and timesheets of their contributions in the case of disputes.

Course Web Page and Mailing List
These are two more resources to be used frequently. The additional materials, grades, etc. will be published on the web page at:

http://www.encs.concordia.ca/~inse6610_2/

A mailing list has been created for discussion of the course topics among students and the instructors; to ask and answer questions related to the course, etc. All the announcements will be directed to that list as well. All the students and instructors must be subscribed to the mailing list. URL (to change your subscription settings):

https://mail.encs.concordia.ca:444/mailman/listinfo/inse6610-f15

E-mail (to post a message to the entire class for discussion or announcement):

inse6610-f15@encs.concordia.ca

Additional Materials
Additional materials, such as lecture notes and slides, examples, etc. will be provided by the instructor. The instructor will try his best to make the notes concise and complete as much as possible. Some materials may be borrowed from previous instructors for this or related courses, primarily Patrick Boismenu, Mourad Debbabi, and others.

The Project
The project represents the main component of the course. The project will be developed as a cooperative (group) project. Each group will be composed of about 5–7 students.

More details to follow.

Legal Statement
The final project is your property but it is also the property of everyone who shared a part of the realization of this project. You must notice that Concordia University has the full right to make whatsoever use of this project and without any restrictions. Your project may be made available to help other students in the future.
Disclaimer

In the event of extraordinary circumstances beyond the University’s control, the content and/or evaluation scheme in this course is subject to change.

Student Services

Need help? There are a variety student services available to you should you struggle through your studies and if the instructor for some reason is unable to help you. They are:

- One-stop information site on many questions:
  [http://www.concordia.ca/help4u/](http://www.concordia.ca/help4u/)

- Concordia Counseling and Development offers career services, psychological services, student learning services, etc.
  [http://cdev.concordia.ca](http://cdev.concordia.ca)

- The Concordia Library Citation and Cycle Guides:
  [http://library.concordia.ca/help/howto/citations.html](http://library.concordia.ca/help/howto/citations.html)

- Advocacy and Support Services:
  [http://supportservices.concordia.ca](http://supportservices.concordia.ca)

- Student Transition Centre:
  [http://stc.concordia.ca](http://stc.concordia.ca)

- New Student Program:
  [http://newstudent.concordia.ca](http://newstudent.concordia.ca)

- Office for Students with Disabilities:
  [http://www.concordia.ca/offices/acsd](http://www.concordia.ca/offices/acsd)

- The Academic Integrity Website:
  [http://www.concordia.ca/students/academic-integrity.html](http://www.concordia.ca/students/academic-integrity.html)

- Financial Aid & Awards:
  [http://www.concordia.ca/offices/faao.html](http://www.concordia.ca/offices/faao.html)

- Health Services:

References


