

Faculty of Business and Information Technology

[INFR 4690U]: [IT Forensics]

Course outline for **Winter 2018**

**1. Course Details & Important Dates\***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Term | Course Type | CRN | Day | Time | Room |
| Winter | Lecture | 71722 | T and R | 2:10pm—3:30pm | J125 |
| Laboratory | 71723 | M | 2:10pm—5pm | UA2130 |
|  | Laboratory | 72910 | M | 8:10am— 11am | UA2240 |

|  |  |  |  |
| --- | --- | --- | --- |
| Classes Start | Classes End | Last day to drop course without academic consequence | Final Exam Period |
| January 8, 2018 | April 9, 2018 | February 2, 2018 | April 11 to 22, 2018 |

\* for other important dates go to: [www.uoit.ca](http://www.uoit.ca) >Current Students >Important Dates and Deadlines

**2. Instructor Contact Information**

|  |  |  |  |
| --- | --- | --- | --- |
| Instructor Name | Office | Phone | Email |
| Amirali Salehi-Abari | ERC 2086 | |  | | --- | | 905-721-8668 x5544 | | abari@uoit.ca |
| Office Hours: Tuesday 1pm—2pm, Thursday 3:30—4:30pm, or by appointment | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Laboratory/Teaching Assistant Name | Office | Phone | Email |
| Yong Deng |  |  | yong.deng@uoit.net |
| Yanwen Zhou |  |  | yanwen.zhou@uoit.net |
| Office Hours: Wednesday 5pm—6pm, ERC 2010. | | | |

**3. Course Description**

This course introduces the basic concepts of computer forensics, principles, techniques, special software tools and practical skills necessary to perform digital investigation of incidents in which computers or other digital devices play a significant or interesting role. Students will learn skills for the most important parts of digital crime scene investigation process, which has several phases, from initial system preservation through evidence searching to event reconstruction. Students will learn how to create an incident response plan and implement a computer forensics incident response strategy. Furthermore, through practical lab exercises, students will also learn how to conduct “Live” investigation including acquisition, examination, analysis, and evidence preservation, and documentation of computer evidence stored as data or computer encoded information. This course also covers state-of-the-art techniques for digital investigation analysis, including file carving, multimedia forensics, memory analysis, mobile device forensics, anti-forensics and counter anti-forensics, and log analysis and correlation.

**4. Learning Outcomes**

On the successful completion of the course, students will be able to:

1. Understand the importance of digital evidence (or electronic evidence) in both civil and criminal investigations, as well as corporate internal investigations

2. Understand digital crime scene investigation procedure

3. Understand the objectives and functions of file systems and become familiar with tools & techniques for file system forensics analysis

4. Have knowledge and understanding of tools & techniques for forensic investigations & examinations both in a Linux environment and Windows

5. Demonstrate an understanding of networking fundamentals and network forensics

6. Understand state-of-the-art techniques for digital investigation analysis, including file carving, memory analysis, mobile device forensics, anti-forensics and counter anti-forensics, and log analysis and correlation

7. Develop their forensic investigation skills through exposure to practical lab examples.

**5. Course Design**

The course focuses on both the principles and practice, including 3 hours of lecture and 3 hours of practical lab exercises and investigation per week. Each student is expected to bring their laptop to every class. You will install all necessary tools and build your own forensic workstation. Then, you will perform laboratory exercises for the hands-on portions of the laboratory sessions. The practical exercises reinforce the material you have learned in the course and teach "hands-on" skills.

The primary teaching method will be class lectures and hands-on laboratory sessions. The lectures will discuss topics presented in the textbook/references and cover additional material, while hands-on laboratory sessions acquaint students with practical skills and techniques relevant to the disciplines which are discussed in the lectures. Class attendance is expected in every class.

**6. Outline of Topics in the Course**

| **Week #** | **Date** | **Topics** |
| --- | --- | --- |
| **1** | **Jan 9**  **Jan 11** | Introduction to Digital Forensics  Digital Investigation Fundamentals |
| **2** | **Jan 16**  **Jan 18** | Foundations of Computer Systems |
| **3** | **Jan 23**  **Jan 25** | Volume Analysis |
| **4** | **Jan 30**  **Feb 1** | File System Analysis I |
| **5** | **Feb 6**  **Feb 8** | File System Analysis II |
| **6** | **Feb 13**  **Feb 15** | File System Analysis III |
| **7** | **Feb 20**  **Feb 22** | Midterm Break—No Classes |
| **8** | **Feb 27**  **March 1** | File System Analysis IV and V |
| **9** | **March 6**  **March 8** | Midterm  File Carving and Volatile Memory Forensic Analysis |
| **10** | **March 13**  **March 15** | Operating System Forensics: Windows and Linux Forensics |
| **11** | **March 20**  **March 22** | Network Forensics |
| **12** | **March 27**  **March 29** | Mobile Forensics |
| **13** | **April 3**  **April 5** | Advanced Forensics Analysis Techniques |

\*Lecture/Lab schedule may be subject to change throughout the term.

**7. Required Texts/Readings**

**Textbook:**

B. Carrier. “File System Forensics Analysis”. Addison-Wesley, Upper Saddle River, NJ, USA, 2005. ISBN-10: 0321268172.

In addition, many materials including research papers from conferences and journals and white papers from security companies and computer forensics oriented websites (and forums) will be used as important references. All assigned readings and cases will be introduced in the class.

**Reading Reference:**

1. Dan Farmer, Wietse Venema. “Forensic Discovery”. Addison-Wesley Professional; January 9, 2005. ISBN-10: 020163497X

P.S.: You can download the first edition for free from the following link

http://www.porcupine.org/forensics/forensic-discovery/

2. D. Brezinski, T. Killalea. IETF RFC 3227: Guidelines for Evidence Collection and Archiving. February 2002. [Online] Available: http://www.rfc-archive.org/getrfc.php?rfc=3227

3. Hard Disk Drives. [Online] Available: http://www.storagereview.com/guide2000/ref/hdd/index.html

4. Understanding FAT32 Filesystems. http://www.pjrc.com/tech/8051/ide/fat32.html

5. The SANS (**S**ysAdmin, **A**udit, **N**etwork, **S**ecurity) Institute's Information Security Reading Room - Forensics. [Online] Available: http://www.sans.org/reading\_room/whitepapers/forensics/

6. The SANS (**S**ysAdmin, **A**udit, **N**etwork, **S**ecurity) Institute's Information Security Reading Room - Incident Handling. [Online] Available: http://www.sans.org/reading\_room/whitepapers/incident/

7. Forensic Focus. [Online] Available: http://www.forensicfocus.com/

8. Yahoo! Groups Groups Discussing computer forensics analysis. [Online] Available: http://groups.yahoo.com/phrase/computer-forensics-analysis

9. The Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University. [Online] Available: http://www.cerias.purdue.edu/

10. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, National Institute of Justice, USA, April 9, 2008. [Online] Available: http://www.ojp.usdoj.gov/nij/publications/ecrime-guide-219941/welcome.htm

11. E. Eugene Schultz and Russell Shumway. Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Sams, Nov 8 2001.

12. Mohd Taufik Abdullah, et al. Advances in Computer Forensics. International Journal of Computer Science and Network Security, VOL.8 No.2, pp. 215-219, February 2008

13. Position Paper for International Professional Certification of Digital Evidence V 3.2. [Online] Available: http://www.ncfs.org/New\_NCFS\_Example\_1/Certification\_Position\_Paper\_V3.2\_7-3-03.pdf

14. Forensic Examination of Digital Evidence: A guide for Law Enforcement. [Online] Available: http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm

15. Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System. [Online] Available: http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/swgit1.htm

16. Digital Evidence: Standards and Principles. [Online] Available: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

17. Recovering and Examining Computer Forensic Evidence. [Online] Available: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

18. Computer System and Network Security Information. [Online] Available: http://www.cromwell-intl.com/security/

*Additional readings may be assigned or recommended during the course.*

**8. Required Hardware and Software Tools**

**Hardware**

Laptop Computer

P.S.: You are expected to bring your laptop to every class.

The use of laptops often enhances the learning experience. However, there are circumstances when it can be obstructive. Instructors have the right and the responsibility to determine appropriate classroom protocols for student use of laptops.

**Software Tools**

VMWare Player (or VMware Workstation)

Telnet/ssh client: putty

SFTP client and FTP client for Windows: WinSCP

Sniffers: TCPDump, Ethereal

The Sleuth Kit (TSK)

dcfldd

**9. Evaluation Method**

The course final grade comes from 2 assignments, 2 in-class quizzes, 1 midterm, Lab activities and participation, final project, and the final exam.

* Quizzes (2): 10%
* Midterm (1): 15%
* Assignments (2): 15%
* Lab Activities (10): 15 %
* Final Project (1): 10%
* Final Exam (1): 35%

*Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found in Section 5 of the UOIT Academic Calendar.*

**9. Assignments and Tests**

|  |  |  |  |
| --- | --- | --- | --- |
| Course Evaluation Components | Posting Date | Due Date | Grading Weights |
| Quiz 1 | NA | Jan 30 | 5% |
| Assignment 1 | Feb 2 | Feb 19 | 7.5% |
| Midterm | NA | March 6 | 15% |
| Quiz 2 | NA | March 27 | 5% |
| Assignment 2 | March 14 | April 1 | 7.5% |
| Final Project | Feb 15 (proposal due date) | April 8 | 10% |
| Final Exam | NA | TBA | 35% |

**Missed Course Work**

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work. Medical absences must be accompanied by a UOIT Medical Statement form completed by the student and physician within 24 hours of the missed course work. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc. If missed coursework totals more than 20% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the other components. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

*Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact* [*studentlife@uoit.ca*](mailto:studentlife@uoit.ca) *for support.*

**10. Accessibility**

Students with disabilities may request to be considered for formal academic accommodation in accordance with the Ontario Human Rights Code. Students seeking accommodation must make their requests through Student Accessibility Services. Requests must be made in a timely manner, and students must provide relevant and recent documentation to verify the effect of their disability and to allow the university to determine appropriate accommodations.

Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining academic integrity.

**11. Academic Integrity**

Students and faculty at UOIT share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by UOIT’s regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one’s own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with UOIT’s regulations on academic conduct does not constitute a defense against its application.

Further information about academic misconduct can be found in the Academic Integrity link on your laptop. Extra support services are available to all UOIT students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found in the Academic Calendar.

**12. Turnitin (if applicable)**

UOIT and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents for five academic years. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to UOIT's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: <http://www.uoit.ca/assets/Academic~Integrity~Site/Forms/Assignment%20Cover%20sheet.pdf>

**13. Final Examinations (if applicable)**

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. Student ID cards can be obtained at the Campus ID Services, in C128 in the Gordon Wiley Building.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three week prior to the first day of the final examination period.

Further information on final examinations can be found in the Academic Calendar.

**14. Freedom of Information and Protection of Privacy Act**

The following is an important notice regarding the process for submitting course assignments, quizzes and other evaluative material in your courses in the Faculty of Business and Information Technology

As you may know, UOIT is governed by the *Freedom of Information and Protection of Privacy Act* (“FIPPA”).  In addition to providing a mechanism for requesting records held by the university, this legislation also requires that UOIT not disclose the personal information of its students without their consent.

FIPPA’s definition of “personal information” includes, among other things, documents that contain both your name and your Banner ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and Information Technology encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that UOIT will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact the UOIT Chief Privacy Officer at [accessandprivacy@uoit.ca](mailto:accessandprivacy@uoit.ca)

**15. Student Course Feedback Survey**

Student course feedback survey of teaching is a highly valued and helpful mechanism for monitoring the quality of UOIT’s programs and instructional effectiveness. To that end, Student course feedback survey are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about survey will be sent via e-mail, and posted on Blackboard, Weekly News and signage around the campus.

**16.Sexual Violence Policy**

UOIT is committed to the prevention of sexual violence in all is forms. For *any* UOIT student who has experienced Sexual Violence, **UOIT can help**. UOIT will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

* Reach out to a Support Worker, who are specially trained individuals authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolutions options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email [supportworker@uoit.ca](mailto:supportworker@uoit.ca)
* Learn more about your options at: [www.uoit.ca/sexualviolence](http://www.uoit.ca/sexualviolence)