CIS*6520
Advanced Digital Forensics and Incident Response
Fall Semester

UNIVERSITY of GUELPH

---

1 INSTRUCTOR

Instructor: Ali Dehghantanha

Office: REY 3326

Phone extension: 52999

E-mail: adehghan@uoguelph.ca

2 AIMS & OBJECTIVES

2.1 Calendar Description

This course provides an in-depth understanding of both theoretical and practical issues in the field of digital forensics and incident response. Students will develop necessary skills, methodologies, and processes to detect cyber incidents and conduct in-depth computer and network investigation.

2.2 Course Description

This course provides an in-depth understanding of both the theoretical and practical issues in the field of digital forensics and incident response. It develops necessary skills, methodologies, and processes to detect cyber incidents and conduct in-depth computer and network investigation following ethical requirements and collaborative best practices in the field.

2.3 Learning Outcomes

Upon successful completion of this course, students will have demonstrated the ability to:

1. Solve and document compromised cases through incident handling and forensics investigation methodologies to develop investigation plans;
2. Identify, collect, analyze, and preserve evidences from a variety of traditional and modern computing platforms;

3. Critically analyse various cyber incidents and build intelligence based on remnants of threat actors in file system, memory, and network data;
4. Analyse and integrate ethics, regulations, and best practices in digital investigation and incident response activities; and
5. Work collaboratively in teams to conduct research and communicate rational and reasoned arguments using appropriate methods.

2.4 Instructor's Role and Responsibility to Students

The course is delivered in a flipped classroom format so most instructional content will be delivered online while classroom time is used to deepen students' understanding through discussions and problem-solving activities facilitated by the instructor. The instructor delivers hands-on guided labs and practical lectures to practice key concepts of incident handling and digital investigation along with in-depth analysis of real-world case studies.

3 TEACHING AND LEARNING ACTIVITIES

3.1 Timetable

Lectures: 3 hours per week

3.2 Course Topics and Schedule

Week	Topic
Week 1	Introduction to digital forensics and ethics, regulations, and best practices for digital investigation and incident response
Week 2	Enterprise incident detection and response
Week 3	Data collection and forensics imaging process
Weeks 4, 5	File system analysis
Weeks 6, 7	Memory forensics
Weeks 8, 9	Network forensics
Weeks 10, 11	Attack intelligence and analysis of adversaries' lateral movements
Week 12	Big-data, IoT, and emerging networks investigation

4 LEARNING RESOURCES

4.1 Required Resources

- Kim-Kwang Raymond Choo and Ali Dehghantanha (2016), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (available electronically via library)
- Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters (2014), The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
- Michael Hale Ligh and Andrew Case (2014), The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
- Sherri Davidoff and Jonathan Ham (2012), Network Forensics: Tracking Hackers Through Cyberspace
- Eoghan Casey (2009). Handbook of Digital Forensics and Investigation. Amsterdam: Academic Press

5 ASSESSMENT

5.1 Dates and Distribution

Assignment	Due Date	Weighting	Learning Outcome(s) Assessed
Research Assignment	TBD (before the 40th class day)	50%	LO3, LO4, LO5
Practical Exam	TBD	50%	LO1, LO2, LO3, LO4

5.2 Assessment Descriptions

Research Assignment: Students will develop tools, techniques, and procedures for threat hunting or conduct a forensics investigation of an emerging cyber platform. Student will be required to document their results and compile a professionally written, high-quality academic report. This is a group-based assignment (max 3 people in each group), which should be submitted electronically as advised by the instructor prior to the submission deadline.

Practical Exam: The practical exam will be conducted in the cybersecurity lab. The practical exam will evaluate students' capabilities to conduct in-depth incident detection, handling, and investigation of different cyber-attacks. The exam evaluates student capabilities to conduct in-depth forensics investigation and incident identification following ethical requirements and best practices in the field. Students will be expected to extract remnants of attackers' activities and report them in a suitable format.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

---

6 University Statements

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs:
https://www.uoguelph.ca/academics/calendars