Course Syllabus

CIS*6520 Advanced Digital Forensics and Incident Response W [0.50]
School of Computer Science, University of Guelph, Guelph
Winter Semester | 2023

1. INSTRUCTIONAL SUPPORT

Instructor Information

Instructor Name	Office	Phone	Email
Dr. Xiaodong Lin	Reynolds 2210	X53889	xlin08@uoguelph.ca
Office Hours: Wednesday, 1:30 pm - 3:00 pm or by appointment			

Teaching Assistant Information

Teaching Assistant Name	Email
Qi Li	qli15@uoguelph.ca
Office Hours: TBD	

Lectures

Day	Time	Location
Thursday	02:30PM - 05:20PM	150 Research Lane, Suite 120

Hardware and System requirements

System requirements: 8 GB RAM, 25 GB hard disk free space.
Also, you will need a webcam, microphone, and speaker. A USB flash drive (small size is preferred, e.g., 8GB or smaller) is required for practice.
Virtual Machine Software: Install VirtualBox and its matching Extension Pack if you haven't already.
Note that if you already have VMware (e.g., VMware Workstation) installed, you can continue to use it as your virtualization platform.
Kali Linux Virtual Machine Image: Please use the following link to download a pre-built Kali Linux virtual machine image. All the hands-on exercises use this image.
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

2. LEARNING RESOURCES

Textbook

- Xiaodong Lin, "Introductory Computer Forensics: A Hands-on Practical Approach," November 2018, Springer (**Freely available** from Springer via University of Guelph network at https://www.springer.com/gp/book/9783030005801)

In addition, some latest developments and results are only available in research papers as well as online posts or articles. These articles or the download URLs will be put on the course website on the **CourseLink** as supplementary reading materials.

Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6520 website which can be found on **CourseLink**. It is the student's responsibility to check these pages frequently for new information or updates.

Course Description

This course provides an in-depth understanding of theoretical concepts and practical issues in the field of digital forensics and incident response. It introduces the practice of digital forensics and incidence response by presenting key technical concepts, the methodologies and software tools and practical skills used to conduct 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, memory analysis, mobile device forensics, anti-forensics and counter anti-forensics, log analysis and correlation, and IoT forensics.
Please see The Academic Calendar for more details. The Academic Calendars are the source of information about the University of Guelph's procedures, policies and regulations which apply to undergraduate, graduate and diploma programs:
http://www.uoguelph.ca/registrar/calendars/index.cfm?index

3. COURSE 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, stealthy activities detection, fake content detection, anti-forensics and counter anti-forensics, and log analysis and correlation, and IoT forensics
7. Understand the importance of an incident response plan and identify the necessary steps taken after the cyber security incident
8. Develop their forensic investigation skills through exposure to practical lab examples.

4. COURSE TOPICS

Introduction to Digital Forensics
Building a Forensics Workstation
Data acquisition
Volume Analysis
File System Forensics
File Carving
Volatile Data Forensic Analysis
Operating System Forensics including Windows and Linux
Network Forensics
Stealthy Activities Detection
Mobile Forensics
Special Topics in Digital Forensics
Project Presentations

5. EVALUATION METHOD

Final grade calculation
In determining the overall grade of the course, the following weights will be used:

Coursework	Amount	% of Grade
hands-on exercises	3	28
Scholarly research critique	1	4
Discussion Participation		2
Course project	1	30 (Class presentation (5) + Project report (25))
Final exam	1	36 (Theoretical (21) and practical (15) components)

The final grade is the weighted sum of all assessments shown above, using the weights indicated in the table above.

Important: Students must successfully complete all of the hands-on exercises with a passing grade (the average of all the hands-on exercises) in order to pass the course.

- Lab Exercises: 28%

- There are 3 lab exercises, which are focused on specific tasks pertaining to digital forensics. Three laboratory exercises are worth 27% of the total course grade, and each lab weight is as follows:

  Lab Exercise 1 =7%
  Lab Exercise 2 =9%
  Lab Exercise 3 =12%

- You are allowed to talk with other students currently enrolled in the course about the lab content. We encourage you to use discussion boards on the CourseLink course website to help your peers. However, each student must conduct the lab exercises and answer the questions/write up their lab reports completely independently.
- **Important: Students must successfully complete all of the hands-on exercises with a passing grade (the average of all the hands-on exercises) in order to pass the course.**

- Scholarly research critique: 4%
  - Throughout the semester you will be given some extra materials to read in order to understand the state of the art in digital forensics research. Each student is assigned **ONE** article selected from the proceedings of important conferences in the field (e.g., DFRWS USA, DFRWS EU, IEEE Symposium on Security and Privacy, ACM CCS, ACM ASIACCS, Usenix Security, or Network and Distributed System Security Symposium (NDSS)) and leading journals (e.g., Digital Investigation (Elsevier), IEEE Transactions on Information Forensics and Security). You will need to read it critically so as to help you know more about some topic's background and as well develop your own idea. Afterwards, you will write two to three pages that reflect on what you learned and thought about the paper. The critique includes a short summary, but most of it will contain your original thoughts about the paper and what you learned.

    The following format is mandatory:

    - The document will be in 12-point font, single spaced.
    - Set the stage. Begin with no more than a quarter page that states the problem that the paper addressed, the solution, and the meaning.
    - State the strength(s) of the paper in one to three sentences.
    - State the weakness(es) or flaw(s) of the paper in one to three sentences.
    - The remainder of your critique will include three of the following:
      - How did it impact the field?
      - What questions remain open?
      - What experiments are missing?
      - How does it really relate to the previous research?
      - Some examples for which it will or will not work.
      - What impact did it have on the field?
      - Ideas or thoughts it provoked.

- Do the authors overstate their contributions in the topic for the investigated research?
- Future research directions.
- Other interesting commentary.

Note that the strengths, weaknesses, and additional discussion should not just summarize what the paper did. They should present your own thoughts after having digested the material. **It is very important to use evidence to support your own opinion. Also, it is not always necessary that you agree with everything the authors say in their published papers.**

- Discussion Participation: 2%
  - Particularly, discussion board participation. In the Discussion Board make meaningful posts or initiate discussion threads (at least **8** for the entire semester) to get full participation marks.

- Course Project – 30%: There will be a course project, which has specialized in one of the following three digital forensics research topics. You can work in a team of at most **TWO** people to complete the course project.

  The project has the following milestones:
  - **Proposal**
    The project proposal is required for approval. A team must submit a project proposal which provides a brief description of the project, including objectives. It also should list all project team members. You should only submit one proposal per team for the course project.
    There isn't a required format for your research proposal, but it must include the following parts:
    - Goals/Objectives: What are we going to do?
    - Approach and Methodology
    - Summary: What will you learn by doing this project?

    Proposal Due on January 30th, 2023 at 11:59PM.
  - **Presentation and Class demonstration** (5%)
    Each team will present their studies on digital forensics and lead a short discussion on their studies in a 15-minute conference-style presentation (Each presenter will have approximately 13 minutes to present his/her project, plus 2 minutes for questions.). Class demonstration & presentation (5%) with the following assessment criteria:
    - Grasp of the problem/issue and associated knowledge;
    - Successful demonstration of studied digital forensic scenario
    - Clarity of presentation;
    - Q&A

    Class demonstration & presentation is MANDATORY. Otherwise, you will receive no credit for the project. However, not all team members in one group must be present in their presentation.
  - **Final Report** (25%) with assessment criteria as follows:

- Literature review and extensiveness of the review;
- Grasp of knowledge pertaining to the application/solution to the problem;
- Length of paper (**10** pages minimum in standard IEEE proceedings two-column format), including the abstract, tables, and figures (excluding references);
- Articulation/accuracy of argument/findings regarding the problem;
- Novelty and originality;
- Breadth of references/bibliography; and
- Proportionate effort put into work.

Please note that a Word template for IEEE proceedings or all Transactions two-column format, TRANS-JOUR.doc, can be found in the following link
http://www.ieee.org/web/publications/authors/transjnl/index.html

- Research project topics for CIS*6520 for Winter 2023:
  - File System Forensic Analysis
  - Internet of Things (IoT) Forensics (e.g., Smart TV Forensics, Vehicle Forensics, Game console (e.g., Play Station) Forensics, Smart Home Forensics)
  - Malware Forensics (e.g., Forensic Analysis of Ransomware, Javascript Malware, Wasm Malware)
- **Report Due on April 10th, 2023 at 11:59PM**.

In the following the term "lab grade" means the cumulative grade for all the lab works (hands-on exercises) expressed as a percentage. The overall course grade will be computed in two distinct ways as follows, depending on whether or not your lab grade is 65% (or a final mark of 18.2%) or more:

(a) If your lab grade is 65% or more: your overall course grade is the weighted sum of all assessments shown above, using the weights indicated in the table above.
(b) If your lab grade is less than 65%: your overall course grade is the lab grade.

Important Dates:

	Due Date	**Grade percentage**
Hands-on Exercise 1	February 9th	7%
Hands-on Exercise 2	March 9th	9%
Hands-on Exercise 3	April 6th	12%
Scholarly research critique	February 2nd	4%
Course Project Proposal	January 30th	0% (But Mandatory)
Course Project Presentation	TBD	5%
Course Project Report	April 10th	25%
Final exam	TBD	36%

Please note that the above schedule is tentative and may be subject to change, depending on class progress. If so, an announcement will be made on the CourseLink accordingly.

Disclaimer
Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings, changes in classroom protocols, and academic schedules. Any such changes will be announced via CourseLink and/or class email.

This includes on-campus scheduling during the semester, mid-terms and final examination schedules. All University-wide decisions will be posted on the COVID-19 website and circulated by email.

Illness
Medical notes will not normally be required for singular instances of academic consideration, although students may be required to provide supporting documentation for multiple missed assessments or when involving a large part of a course (e.g., final exam or major assignment).

For information on current safety protocols, follow these links:
https://news.uoguelph.ca/return-to-campuses/how-u-of-g-is-preparing-for-your-safe-return/
https://news.uoguelph.ca/return-to-campuses/spaces/#ClassroomSpaces

Please note, these guidelines may be updated as required in response to evolving University, Public Health or government directives.

Course Grading Policies
Late assignments: We will allow **3 total late days** ("grace days") for coursework (assignments, Scholarly research critiques, and project) **which you can use to give yourself extra time without penalty**. Please email me with your late submission if you decide to use these days for a particular assignment. Late days may be spread over any number of assignments at your own discretion, but the total number may not exceed 3. Late days are rounded up so that an assignment that is 28 hours late accumulated 2 late days. No extensions will be considered beyond the late days.
All assignments are due at 11:59 PM on the due date. Late assignments (and project report) beyond the grace days will incur a penalty of 25% in the first 24 hours, 50% in the second 24 hours, 75% in the third 24 hours, and 100% thereafter, unless prior arrangements are made or a valid reason presented within five days from the missed deadline. In no case will an assignment be accepted more than three days past the deadline; if a valid reason exists for being unable to hand in an assignment within five days following the deadline, then the assignment will be assigned a weight of zero and the weight of the missing assignment will be moved to your course project.
If you are prevented from completing your project due to medical or personal reasons you are advised to contact the instructor earlier so the proper arrangements can be made and an INC grade may be assigned.

Submission policy: All your course work will be only be accepted via submission through CourseLink unless otherwise indicated on the assignment by the instructor. Failure to submit assignments correctly (e.g., wrong files, etc.) will result in a zero mark.

Regrades: Students may request a reassessment of their assignments in writing and specify the reasons for such requests. Their entire assignment will be reassessed, and the reassessment may result in raising or lowering of the original marks. Remark requests will only be accepted up to **5**

calendar days from the release of the assignment mark. Please carefully read through the comments made by the marker on CourseLink before sending a remark request.

Missed Assessments: If you are unable to meet an in-course requirement due to medical, psychological, or compassionate reasons, please contact your course instructor within five days following the deadline. Please see below for specific details and consult the graduate calendar for information on regulations and procedures for Academic Consideration: https://calendar.uoguelph.ca/graduate-calendar/

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the 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://calendar.uoguelph.ca/graduate-calendar/

Plagiarism Policy: All work submitted must be your own. Similarities between assignment submissions are monitored using Turnitin as well as by manual means.

Special Note:

• A reliable internet connection that is sufficient for online learning is necessary for this course. If you do not have a sufficiently fast and reliable internet connection then you may not be able to view or download lectures or other course material. It may also not be possible to attend online advising with teaching assistants or the instructor.
• This course is offered in the eastern standard time zone (EST). While taking this course then you may be required to attend online activities such as advising times or labs between 9:00 and 5:20 EST.
• Keep copies of assignments which you have submitted. You may be asked to resubmit assignments at a later time.
• All cases of academic misconduct are handled by the Dean, in conjunction with the School Director. Successive infractions of misconduct affirmed by this process could have consequences as serious as expulsion from the University. For details please see related pages in the University of Guelph Graduate Calendar.
• Requests for academic consideration because of illness or of a compassionate nature must be made in writing (via email).

6. STANDARD STATEMENTS

The following are standard statements for inclusion on all course outlines (adapted with permission from the College of Arts). Some departments or colleges may also elect to post this information on a common website and link to such sites in the course outline. However, it is strongly recommended that statements on academic misconduct and links to the academic misconduct section of the academic calendars are included on all course outlines.

E-mail Communication

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

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. See the graduate calendar for information on regulations and procedures for Academic Consideration.

Drop Date

Students will have until the last day of classes to drop courses without academic penalty. The regulations and procedures for course registration are available in their respective Academic Calendars.

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.

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 7 days in advance, and not later than the 40th Class Day. More information: www.uoguelph.ca/sas

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.

Recording of Materials

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

Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies and regulations which apply to undergraduate, graduate and diploma programs.