

ECE570: Computer Forensics Methodologies

Course Dates

CRN(s):	Section A01 CRN: 30354 Section A02 CRN: 30355
Term:	Summer 2022
Course Start:	2022-05-04
Course End:	2022-08-17
Withdrawal with 100% reduction of tuition fees:	2022-05-16
Withdrawal with 50% reduction of tuition fees:	2022-06-05
Last day for withdrawal (no fees returned):	2022-06-29

Scheduled Meeting Times (M=Mon, T=Tue, W=Wed, R=Thu, F=Fri)

Section:	Location:	Classes Start:	Classes End:	Days of week:	Hours of day:	Instructor:
A01	ECS 108	2022-05-04	2022-07-29	MR	08:30-09:50	Issa Traore
A02	ECS 108	2022-05-04	2022-07-29	MR	08:30-09:50	Issa Traore

Instructor(s)

Name: **Issa Traore**
 Office: EOW 415
 Phone: (250) 721-8697
 Email: itraore at ece dot uvic dot ca

Office Hours: Comments
 Mon 12:00pm-01:00pm Zoom Links for Online lectures and Office hours are available on Brightspace.
 Thu 12:00pm-01:00pm

Course Objectives

The purpose of the course is to introduce the practice of digital forensics and cyber incident investigation by presenting key technical concepts, and the methodologies and tools used to conduct forensics examination. Details on forensics for computers, networks, and mobile devices will be covered. Methodologies for collecting evidence, documenting crime scene, and recovering deleted data will be introduced. Methodologies and tools for malware analysis and reverse engineering will be covered.

Learning Outcomes

By the end of this course, students should have a good grasp of:

1. What digital forensics is and how it is used in a variety of fields
2. Recognize anti forensic techniques used to hide or destroy data
3. Understand the common artifacts to look for during a forensic examination
4. Use sound methodologies to collect and analyze forensics evidence, and document the examination
5. Learn how to reconstruct cyberattack scenarios and analyze malware from security logs and artifacts
6. Learn how to analyze statically/dynamically and reverse engineer malicious code

Syllabus

Chapter 1: Introducing Digital Forensics

- Fundamental Concepts
- Forensic Evidence
- Evidence Source
- Opportunities and Challenges
- Other Uses of Forensics

Chapter 2: Forensics Data and Process

- Data Handling and Data Integrity
- Types of Data
- Data Acquisition Techniques
- Hard Drives and Disk Images
- RAM data
- Network Data
- Forensics Data Format
- Forensic Process

Chapter 3: Memory Forensics

- Memory Acquisition
- Memory Concepts
- Memory Analysis
- Malware analysis

Chapter 4: Basic Malware Analysis

- Static analysis
- Dynamic analysis

Chapter 5: File Carving

- File Systems
- Data Hiding Techniques
- File Signature
- File Carving and Recovery

Chapter 6: Forensics Analysis

- Forensics Analysis Tools
- Forensics Analysis Approaches
- Forensics Artifacts

Chapter 7: Mobile Device Forensics

- Mobile Device Data
- Data Acquisition
- Mobile Forensics Analysis

Chapter 8: Network Forensics

- Network Forensics Architecture
- Network Forensics Data
- Packets Analysis

Chapter 9: Intrusion Investigation

- Intrusion Investigation Process
- Intrusion Scenario Reconstruction

Chapter 10: Malware Reverse Engineering

- x86 Disassembly
- Recognizing C Constructs in Assembly
- Analyzing malicious Windows Programs

Chapter 11: E-mail Forensics

- E-mail as Evidence
- Investigating E-mail Headers
- Tracing E-mail
- Web-based E-mail

Chapter 12: Cyber Incident Response (IR)

- IR Phases and Roles
- IR Process
- Cyber Incident Attribution

Chapter 13: Forensics Documentation

- Internal Report
- Declaration
- Affidavit
- Expert Report

Textbook

Enter any textbooks required here. Usually done in a table. (Edit the sections labeled TBD to fill in your own information, leave the dashes and upright slashes alone - they will make it look like a table when you hit the preview button)

Required Text	Optional Text
Title:	Title: Introductory Computer Forensics - A hands on Practical Approach
Author:	Author: Xiaodong Lin
Publisher/Year:	Publisher/Year: Springer, 2018
Reference Materials	
Title:	Title:
Author:	Author:
Publisher/Year:	Publisher/Year:

Online Course Delivery

This course will be taught in person, making use primarily of Brightspace.

Office Hours:

Online office hours will use Zoom on Monday/Thursday 12:00-1:00 pm. You can also contact me through e-mail for appointments.

Assessment

Assessment	Weight	Date
Project #1	10%	June 6, 2022
Project #2	30%	July 4, 2022
Project #3	20%	July 29, 2022
Mid-term Exam	40%	July 14, 2022

Notes

The final grade obtained from the above marking scheme for the purpose of GPA calculation will be based on the percentage-to-grade point conversion table as listed in the current Graduate Calendar.

<https://www.uvic.ca/calendar/archives/202205/grad/index.php#/policy/B13jeiMdE?bc=true&bcCurrent=07%20-%20Grading&bcltemType=policies>

General Information

Note to Students:

Students who have issues with the conduct of the course should discuss them with the instructor first. If these discussions do not resolve the issue, then students should feel free to contact the Chair of the Department by email or the Chair's Secretary to set up an appointment.

Accommodation of Religious Observance:

<https://www.uvic.ca/calendar/archives/202205/grad/index.php#/policy/SkmigiMOV?bc=true&bcCurrent=17%20-%20Accommodation%20of%20Religious%20Observance&bcltemType=policies>

Policy on Inclusivity and Diversity:

Engineering: <https://www.uvic.ca/engineering/about/equity/index.php>

Academic Calendar: <https://www.uvic.ca/calendar/archives/202205/grad/index.php#/policy/HkQ0pzdAN?bc=true&bcCurrent=General%20University%20Policies&bcltemType=policies>

Standards of Professional Behaviour:

You are advised to read the Faculty of Engineering document Standards for Professional Behaviour, which contains important information regarding conduct in courses, labs, and in the general use of facilities.

<http://www.uvic.ca/engineering/assets/docs/professional-behaviour.pdf>

Academic Integrity:

Cheating, plagiarism and other forms of academic fraud are taken very seriously by both the University and the Department. You should consult the entry in the current Graduate Calendar for the UVic policy on academic integrity.

https://www.uvic.ca/calendar/archives/202205/grad/index.php#/policy/BJujesM_E?bc=true&bcCurrent=02%20-%20Policy%20on%20Academic%20integrity&bcltemType=policies

Equality:

This course aims to provide equal opportunities and access for all students to enjoy the benefits and privileges of the class and its curriculum and to meet the syllabus requirements. Reasonable and appropriate accommodation will be made available to students with documented disabilities (physical, mental, learning) in order to give them the opportunity to successfully meet the essential requirements of the course. The accommodation will not alter academic standards or learning outcomes, although the student may be allowed to demonstrate knowledge and skills in a different way. It is not necessary for you to reveal your disability and/or confidential medical information to the course instructor. If you believe that you may require accommodation, the course instructor can provide you with information about confidential resources on campus that can assist you in arranging for appropriate accommodation. Alternatively, you may want to contact the Centre for Accessible Learning located in the Campus Services Building:

<https://www.uvic.ca/services/cal/>. The University of Victoria is committed to promoting, providing, and protecting a positive, and supportive and safe learning and working environment for all its members.

Course Lecture Notes:

Unless otherwise noted, all course materials supplied to students in this course have been prepared by the instructor and are intended for use in this course only. These materials are NOT to be re-circulated digitally, whether by email or by uploading or copying to websites, or to others not enrolled in this course. Violation of this policy may in some cases constitute a breach of academic integrity as defined in the UVic Calendar.

Sexualized Violence Prevention and Response at UVic:

UVic takes sexualized violence seriously, and has raised the bar for what is considered acceptable behaviour. We encourage students to learn more about how the university defines sexualized violence and its overall approach by visiting www.uvic.ca/svp. If you or someone you know has been impacted by sexualized violence and needs information, advice, and/or support, please contact the sexualized violence resource office in Equity and Human Rights (EQHR). Whether or not you have been directly impacted, if you want to take part in the important prevention work taking place on campus, you can also reach out:

Where: Sexualized violence resource office in EQHR; Sedgewick C119

Phone: 250.721.8021

Email: svpcoordinator@uvic.ca

Web: www.uvic.ca/svp

Office of the Ombudsperson:

The Office of the Ombudsperson is an independent and impartial resource to assist with the fair resolution of student issues. A confidential consultation can help you understand your rights and responsibilities. The Ombudsperson can also clarify information, help navigate procedures, assist with problem-solving, facilitate communication, provide feedback on an appeal, investigate and make recommendations. Phone: 250-721-8357; Email: ombuddy@uvic.ca, Website:

<https://uvicombudsperson.ca/>

