University of Victoria
Faculty of Engineering | Electrical and Computer Engineering
Engineering Office Wing Room 448 PO Box 1700 STN CSC Victoria BC V8W 2Y2 Canada
T 250-721-6036 | ecesec@uvic.ca |

COURSE OUTLINE

ECE 570 – Digital Forensics Methodologies

Term – Summer 2020 (202005)

Instructor

Dr. Issa Traore
Phone: 250 721 8697
E-mail: itraore@ece.uvic.ca

Office Hours

Days: Monday, Thursday
Time: 11:30am-12:30 pm
Location/Platform/link:
Blackboard Collaborate
https://ca.bbcollab.com/guest/aab01b0e8b66487b967ba07ef9a05872

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
- Windows Forensics
- Linux Forensics

Chapter 7: Network Forensics
- Network Forensics Architecture
- Network Forensics Data
- Packets Analysis

Chapter 8: Intrusion Investigation
- Intrusion Investigation Process
- Intrusion Scenario Reconstruction

Chapter 9: Malware Reverse Engineering
- x86 Disassembly
- Recognizing C Constructs in Assembly
- Analyzing malicious Windows Programs

Chapter 10: E-mail Forensics
- E-mail as Evidence
- Investigating E-mail Headers
- Tracing E-mail
- Web-based E-mail

Chapter 11: Mobile Device Forensics
- Mobile Device Data
- Flash Memory
- Data Acquisition

- Mobile Forensics Analysis

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

A-Section(s): A01 / CRN 30346 B01 N/A TA (email) N/A
A02/CRN 30347
Days: Monday, Thursday
Time: 8:30-9:50am
Location/Platform/link:
Blackboard Collaborate
https://ca.bbcollab.com/guest/aab01b0e8b66487b967ba07ef9a05872

Required Text

Title: Introductory Computer Forensics – A hands on Practical Approach
Author: Xiaodong Lin
Publisher: Springer
Year: 2018

Optional Text

Title:
Author:
Publisher:
Year:

Online Course Delivery:
As this course will be conducted online during this term, students will need to complete assignments/labs/exams online. The students will require access to a computer which has the following software installed: web browser.

References:

1. "Hacking Exposed-Computer Forensics: Secrets and Solutions". Aaron Philipp, David Cowen, Chris Davis. McGraw Hill Professionals, ISBN: 0072256753, 2005
2. Lectures Notes available on Course Space

Assessment:

Project #1:	10%	Due Dates: June 8, 2020
Project #2:	30%	July 8, 2020
Project #3:	20%	July 31, 2020
Mid-term:	35%	July 16, 2020
Final Exam (N/A):		Date: N/A

Attendance and Participation: 5%

Important: All deadlines and schedules for this course will reference Pacific Daylight Time.

Note:

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/calendar2020-05/grad/index.php#/policy/B13jeiMdE?bc=true&bcCurrent=07%20-%20Grading&bcItemType=policies

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.

Course Withdrawal Deadlines:

- May 16, 2020: Withdrawal with 100% reduction of tuition fees
- June 6, 2020: Withdrawal with 50% reduction of tuition fees
- July 1, 2020: Last day for withdrawal (no fees returned)

Accommodation of Religious Observance:
https://www.uvic.ca/calendar2020-05/grad/index.php#/policy/SkmigiMOV?bc=true&bcCurrent=17%20-%20Accommodation%20of%20Religious%20Observance&bcItemType=policies

Policy on Inclusivity and Diversity:
Engineering: https://www.uvic.ca/engineering/about/equity/index.php
Academic Calendar: https://www.uvic.ca/calendar2020-05/grad/index.php#/policy/HkQ0pzdAN

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/calendar2020-05/grad/index.php#/policy/BJujesM_E?bc=true&bcCurrent=02%20-%20Policy%20on%20Academic%20Integrity&bcItemType=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; Web: https://uvicombudsperson.ca/