University of Victoria Engineering

Faculty of Engineering

COURSE OUTLINE

ELEC 570 – Digital Forensics Methodologies

Term – Spring 2018 (201801)

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: EOW 415

Course Objectives

The purpose of the course is to introduce the practice of digital forensics 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.

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

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 from memory capture

Chapter 4: Carving

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

Chapter 5: Forensics Analysis

- Forensics Analysis Tools
- Forensics Analysis Approaches
- Windows Forensics
- Linux Forensics

Chapter 6: Network Forensics

- Network Forensics Architecture
- Network Forensics Data
- Packets Analysis

Chapter 7: Intrusion Investigation

- Intrusion Investigation Process
- Intrusion Scenario Reconstruction

Chapter 8: E-mail Forensics

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

Chapter 9: Mobile Device Forensics

- Mobile Device Data
- Flash Memory
- Data Acquisition
- Mobile Forensics Analysis

Chapter 10: Forensics Documentation

- Internal Report
- Declaration
- Affidavit
- Expert Report

A-Section(s): A01 / CRN 30320 B01 N/A TA (email) N/A
A02/CRN 30321
Days: Monday, Thursday
Time: 8:30-9:50am
Location: CLE A308

Required Text

Title: Cybercrime and Digital forensics: and Introduction
Author: Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar
Publisher: Routledge
Year: Oct. 16, 2017

Optional Text

Title:
Author:
Publisher:
Year:

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 7, 2018
Project #2:	25%	July 12, 2018
Project #3:	25%	August 3, 2018
Mid-term:	35%	July 5, 2018
Final Exam (N/A):		Date: N/A

Attendance and Participation: 5%

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://web.uvic.ca/calendar2018-05/grad/academic-regulations/grading.html

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 Assistant to set up an appointment.

Accommodation of Religious Observance:
https://web.uvic.ca/calendar2018-05/grad/registration/Registration.1.16.html

Policy on Inclusivity and Diversity:
https://web.uvic.ca/calendar2018-05/general/policies.html

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

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://web.uvic.ca/calendar2018-05/grad/academic-regulations/academic-integrity.html

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 Resource Centre for Students with a Disability located in the Campus Services Building.
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.