CSCI 4391: SELECT TOPICS COMPUTER SCIENCE
NETWORK FORENSICS
Fall 2019

Time: **Thursday** 1:00 to 3:50 pm

Room: Delta Building, Room TBA

Instructor: Dr. Kewei Sha
Office: Delta 148 **Phone: 281-283-3874**
E-mail: sha@uhcl.edu **URL:** **http://sceweb.sce.uhcl.edu/sha/**
Office Hours: TBD Or by appointment

Teaching Assistant (TA): TBD

****

The information contained in this class syllabus is subject to change without notice. Students are expected to be aware of any additional course policies presented by the instructor during the course.

****

Textbook

Ric Messier. Network Forensics, 1st **Edition**.
Sherri Davidoff, Network Forensics: Tracking Hackers through Cyberspace, 1st **Edition**.
Joshi, R.C., Pilli, Emmanuel S., Fundamentals of Network Forensics: A Research Perspective, 1st **Edition**.

Course Pre-requisite

CSCI 4312 Networking Protocols and/or ITEC 2381

Grading and Evaluation

Participation and discussion	5%
Assignments and Quizzes	25%
Labs	30%
Midterm Exam	20%
Final exam	20%

Grading Scale

90+ = A; 87-89 = A-; 84-86 = B+; 81-83= B; 78-80 = B-; 75-77 = C+;
71-74 = C; 68-70= C-; 65-67 = D+; 61-64 = D; 58-60 = D-; < 58 = F

Course Description

Exploration and examination of techniques, tools, and their applications to investigate, search, collect, analyze, and report on network based breaches and events.

Course Goals

This course introduces and explains the fundamental concepts of network forensics, core of network forensics related to different network devices and network based applications, and tools used to collect, analyze and report forensics related data.

Student Learning Outcomes (SLO)

After completing this class, students will be able to:

- Understand the concept of digital evidence
- Understand the design of network sensors and deployment
- Understand mechanisms to investigate network devices
- Understand mechanisms to investigate network applications
- Be able to use data collection tools and data analysis tools
- Be able to write network forensics report
- Understand the privacy issues in network forensics

General Course Outline (subject to change)

1. Module 1: Foundations of Network Forensics (3-4 weeks)
    a. Unit ND_1: Review of Network Threats (Internal threats & external threats)
    b. Unit ND_2: Review of Computer Forensics
    c. Unit ND_3: Event Logs
    d. Unit ND_4: Evidences
    e. Unit ND_5: Location awareness
    f. Unit ND_6: Co-relating attacks
2. Module 2: Core of Network Forensics
    a. Submodule 1 – Investigating Network Devices/Components (3-4 weeks)
        i. Unit ND_7: Proxies and Forensics
        ii. Unit ND_8: Firewalls and Forensics
        iii. Unit ND_9: NIDS & NIPS and Forensics
        iv. Unit ND_10: VPN and Forensics
        v. Unit ND_11: Router and Forensics
    b. Submodule 2 – Investigating Network Attacks (2-3 weeks)
        i. Unit ND_12: BotNet Forensics
        ii. Unit ND_13: DDoS Forensics
        iii. Unit ND_14: Malware Forensics
    c. Submodule 3 – Focused Topics in Network Forensics (3-4 weeks)
        i. Unit ND_15: Media Forensics
        ii. Unit ND_16: Web Forensics
        iii. Unit ND_17: Email Forensics
        iv. Unit ND_18: Smartphone Forensics
        v. Unit ND_19: Cloud Forensics
        vi. Unit ND_20: IoT Forensics
3. Module 3: Forensics and Privacy (2 weeks)
    a. Unit ND_21: Privacy and Forensics
    b. Unit ND_22: Ethics and Forensics
    c. Unit ND_23: Reporting Investigation Results
4. Module 4: Network Forensics Tools and Hands-on activities (embedded into lectures)
    a. Unit ND_24: lab – Tcpdumping with the libpcap library
    b. Unit ND_25: lab – Sniffing wireless traffic with Wireshark
    c. Unit ND_26: lab – Packet sniffing and analysis with NetworkMiner

d. Unit ND_27: lab - Malware identifying with YARA
e. Unit ND_28: lab – Evidence acquisition with SNORT
f. Unit ND_29: lab - Collect and analyze log file with Splunk

Important dates:

Midterm:	Oct 10, 2019
Final:	Dec 12, 2019 Thursday, 1:00 pm - 3:50 pm

Other important dates: (You must confirm on the University Website)

August 26 ..... First Class Day for Regular Session
October 10 …….. Midterm
November 28 ……. University Holiday – Thanksgiving
December 5 ..... Last Day of Class
December 12 ..... Final Exams

Other course policies

- The Blackboard site will be the official site for this course.
- Must use UHCL-mail. Please note course (CSCI 4391) in Subject Line. Should check your mail at least once per day. Be respectful in email correspondence.
- Respect your TA. The TA is your first line of defense/offense.
- This is a face-to-face course conducted as lectures and presentations. The material will be posted on the course Blackboard before class time. Students are expected to read class material from the book before coming to class. Other notes and material are accessible from Blackboard during class.
- All submissions and deliverables of assignments are due according to Blackboard-posted times and dates.
- Class attendance is expected. It is the student's responsibility to get the material discussed, announcements, handouts, or anything conducted during a missed class meeting. Class attendance is part of the Participation Grade.
- Participation and discussion from students are highly encouraged.
- I **WILL NOT** accept assignments handed in after the deadline UNLESS (a) you have made prior arrangements with me OR (b) you have a reason such as illness or injury, which is substantiated by the dean of students.
- Makeup of exams and quiz will be very restricted, and is allowed only under a documented (appropriate documents) legitimate excuse that is to the discretion of the instructor.
- If you believe that you have a disability requiring an academic adjustment/auxiliary aid, please contact Disability Services by phone at 281-283-2648, or email disability@uhcl.edu, or go to the office in the Student Services Building (SSCB), Room 1.302. website: www.uhcl.edu/disability
- The University of Houston System complies with Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990, pertaining to the provision of reasonable academic adjustments/auxiliary aids for students with a disability. In

accordance with Section 504 and ADA guidelines, each University within the System strives to provide reasonable academic adjustments/auxiliary aids to students who request and require them.

- Regrading work policy: If you believe that the TA or myself have made a mistake in grading you have two class periods after I return the assignment/exam to submit a regrade request. On a separate sheet of paper attached to the front of the assignment/exam you must give a clearly written logical argument as to why you believe that you should have received a different score. I will then regrade the entire problem. On occasion this may result in a lower score. After the deadline has passed I will not regrade assignments.
- Incomplete course policy: The university's incomplete course policy is contained in both the undergraduate and graduate catalogues which are available on the university website (www.uhcl.edu).
- **6 Drop Rule:** Students who entered college for the first time in Fall 2007 or later should be aware of the course drop limitation imposed by the Texas Legislature. Dropping this or any other course between the first day of class and the census date for the semester/session does not affect your 6 drop rule count. Dropping a course between the census date and the last day to drop a class for the semester/session will count as one of your 6 permitted drops. You should take this into consideration before dropping this or any other course. Visit www.uhcl.edu/records for more information on the 6 drop rule and the census date information for the semester/session.
- Academic Honesty: HONESTY CODE of UHCL states: **I will be honest in all my academic activities and will not tolerate dishonesty.** Students and Faculty are bound to the honor code; therefore, academic dishonesty will not be tolerated in this class! See the UHCL catalog for more details. You are encouraged to become familiar with the policy of academic dishonesty found in the UHCL official student handbook. All submissions are considered completely 100% your own work. Copying the work of others and allowing others to copy your own work is not acceptable and is considered academic dishonesty. Also, sharing the course material after finishing this course is not allowed. Any violation of the dishonesty rules will result in filing *Academic Dishonesty Form* and subtracting 10% of total course grade for each incident and for all students involved in the incident.

  Academic Honesty Code: see section 2.1.4 in the Students Life Policies handbook for the UHCL Academic Honesty Code: http://prtl.uhcl.edu/portal/page/portal/PRV/FORMS_POLICY_PROCEDURES/STUDENT_POLICIES/Academic_Honesty_Policy .
