# Department of Electrical and Computer Engineering

## EEE 4XXX – Network Forensics Engineering

### Catalog Description

This course will cover the details of the of network forensics engineering that is used to collect and analyze evidence from the network environment containing devices such as firewalls, routers, IDS, etc. The course will enable to student to follow the footprint of a cyber-attacker with the goals of counteracting cybercrime, cyberterrorism, and cyberpredators, and making them accountable.

### Catalog Objectives

- To give the students an understanding of what Network Forensics entails
- To give the students a hands-on exposure to the latest tools and techniques to prepare an investigative plan.
- To extract information from network devices such as routers, switches, firewalls, proxies, and IDSs/IPSs.
- To analyze other network devices like DHCP and DNS servers to find useful information.
- To perform Covert Tunnel Analysis.
- To analyze IDS captures and web proxy cache.
- To provide exposure to well-known and novel forensic methods using command-line and graphical open-source computer forensics tools for examining a wide range of target systems and artifacts.

### Prerequisites

- Knowledge of windows operating system.
- Knowledge of TCP/IP
- EEE-4XXX (Introduction to Digital Forensics Engineering)

#### Textbooks

- Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham (Jun 23, 2012)

### Topics covered

- Ethical Issues
- Analysis of Routers and Switches
- Analysis of IDS/IPS and Web Proxies
- Analysis of DHCP and DNS servers

- Wireless Packet Capture and Analysis
- Covert Network Tunnels

**Class schedule**
Twice a week 75 minutes class with hands-on lab as part of the lectures

**Contribution of course to meeting the professional component**
Engineering science – 90% (math/science required for creative applications)
Engineering design – 10% (decision making process of devising a system, component or process to meet a desired need).

**Relationship of course to program outcomes:**
In the course EEE 4XXX – Introduction to Digital Forensics Engineering, the student will have to show

1. An ability to apply knowledge of mathematics, science, and engineering
2. An ability to design and conduct experiments, as well as to analyze and interpret data
3. An ability to identify, formulate, and solve engineering problems
4. An understanding of professional and ethical responsibility
5. Recognition of the need for, and an ability to engage in life-long learning
6. Knowledge of contemporary issues
7. An ability to use the techniques, skills and modern engineering tools necessary for engineering practice

**Person who prepared this description and date of preparation:**
Dr. Faisal Kaleem