## **CYBR 315: Network Security and Forensics Analysis (3 credits)**

This course on network forensics focuses on the nuances and challenges unique to network environments within digital forensic investigations. It includes advanced exploration of network-based evidence, emphasizing the practical application of network forensics. The course integrates hands-on examples and case studies to deepen the understanding of network forensics, highlighting its importance in the context of modern network-centric computing environments. The course is structured to provide a comprehensive overview of the basics of computer and network forensics.  *(Prerequisite: CMPE 215)*

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate advanced knowledge and understanding of concepts and theories related to network security and forensics.

A2. Apply appropriate practices and techniques to collect various types of digital evidence from computer networks.

B1. Critically evaluate digital evidence from computer networks, utilizing network forensics techniques to formulate evidence-based solutions.

B2. Effectively communicate in written the outcomes of collecting various types of digital evidence from computer networks.

**Course Learning Materials:**

* S. Davidoff and J. Ham, Network Forensics: Tracking Hackers Through Cyberspace. 2012.
* W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.

**Course Content:**

1. Network Forensics: An Overview
2. Introduction to Network Forensics and Technical Fundamentals
3. Traffic Analysis
4. Statistical Flow Analysis
5. Wireless Forensics
6. Network Intrusion Detection and Analysis
7. Event Logs and Web Proxies
8. Switches, Routers, and Firewalls, and Network Tunneling
9. Malware
10. Legal Issues in Network Forensics