## **CYBR 375: Cybercrime (3 credits)**

This course offers an in-depth exploration of cybercrime, covering key aspects such as the technology used in cyber offenses, law enforcement challenges, privacy concerns, hacking, malware, digital piracy, online fraud, cyberbullying, cyberstalking, cyberterrorism, and cyberwarfare. It also delves into the criminological theories behind cybercrimes, the evolution of digital forensics, legal challenges in forensic investigations, and future trends in cybercrime and policy. This curriculum is designed to equip students with a comprehensive understanding of the complexities and evolving nature of cybercrime methods.  *(Prerequisite: CYBR 310)*

**Course Learning Outcomes:**

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

A1. Demonstrate advanced knowledge in diverse cybercrime areas.

A2. Adapt appropriate methods, practices, techniques, tools, or materials for collecting evidence in diverse cybercrime scenarios.

B1. Critically evaluate and synthesize information and concepts within cybercrime scenarios, including the critical evaluation of evidence.

B2. Effectively communicate findings in cybercrime investigations through comprehensive reports and presentations.

C1. Demonstrate advanced proficiency in collaborative environments, achieving both personal and collective outcomes in cybercrime-related tasks.

**Course Learning Materials:**

* T. J. Holt, A. M. Bossler, and K. C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction*, 3rd ed., 2022
* S. Holt, A. Bossler, and K. Strumsky, "Cybercrime and Digital Forensics: An Introduction," 2nd ed., Routledge, 2019.
* N. Kshetri, "Cybercrime and Cybersecurity in the Global South," Springer, 2020.
* P. Stephenson and J. Gilbert, "Investigating Cyber Crime: A Complete Reference Guide," CRC Press, 2013.

**Course Content:**

1. Technology and Cybercrime
2. Law Enforcement, Privacy, and Security in Dealing with Cybercrime
3. Computer Hackers and Hacking
4. Malware and Automated Computer Attacks
5. Digital Piracy and Intellectual Property Theft
6. Online Fraud
7. Cyberbullying, Online Harassment, and Cyberstalking
8. Online Harassment, Cyberterror and Cyberwarfare
9. Cybercrime and Criminological Theories
10. Evolution of Digital Forensics
11. Legal Challenges in Digital Forensic Investigations
12. The Future of Cybercrime, Terror, and Policy