

ITS4236 : Cyber Forensics

Cyber forensics goes beyond just analyzing computer hard drives or detecting intrusions to infrastructures. The term “cyber forensics” is the term adopted by the US Department of Defense, which indicates that the practice of forensics covers digital forensics, network forensics, and application forensics. The course is designed to be aligned with the common body of knowledge of the Computer Hacking Forensic Investigator Certification from the EC-Council. The course covers established digital forensics disciplines and new domains, such as mobile forensics. The course examines digital forensics techniques and procedures, standards and best practices, as well as legal considerations and ethics. The student learns how to obtain digital evidence that is accurate, complete, and dependable. The course also examines the application of the cyber forensics' competencies to different information security areas, such as e-discovery, malware analysis, and incident response. The course includes a direct component, which consists of demonstrations and virtual-lab assignments.

Credits 4.0

Prerequisites

[ITS4235: Ethical Hacking II](#)

Corequisites

None