MASTER'S DEGREE IN CYBERSECURITY

Digital Forensics Concentration Course Guide

CORE COURSES (12 CREDIT HOURS)

Information Security & Risk Management
(3 Credit Hours)

Recent years have seen an unfortunate and disruptive growth in the number of cyber-attacks. To help curb this major societal issue, there has been an increase in calls for well-trained cybersecurity professionals. However, individuals often lack key skills such as planning/implementing/upgrading/monitoring emerging technologies, incident response, security controls and basic systems administration. Moreover, candidates often lack the non-technical skills of researching and reading new technologies, regulatory compliance, internal security policies, standards and procedures. This hands-on, introductory course is backward engineered with DHS/NSA key knowledge unit requirements for maintaining the Center for Academic Excellence for Cyber Defense (CAE-CD) and aims to alleviate these concerns and help students become excellent candidates in the field. Course topics include the importance of information security and related business concerns; key definitions and terminology for information security; major categories of information security threats; common information security controls; implementing the basic information security controls; legal provisions regarding information security and the methodological implications for INFOSEC arising from these legal provisions; standard methodologies for complying with legal requirements for IT general controls; and IT risk management in organizations. Students will develop valuable skills, such as critical thinking, currently in demand for cybersecurity professionals. Upon completion of this course, students will have a strong foundation for advanced studies, including cybersecurity certifications such as Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Security+, Certified Information Systems Security Professional (CISSP) and SANS GIAC Security Essentials (GSEC).

Special Topics: Applied Cryptography
(3 Credit Hours)

Cryptography is the art and science of securing information in a broad sense. It includes not only the design and analysis of methods for data encryption to ensure confidentiality but also the solutions for authentication, secure distributed computation and more. This course provides an overview of applied cryptography. It introduces the necessary mathematical tools of applied cryptography and shows how they are applied to design algorithms and protocols to secure information. The course starts with a review of mathematical foundations of cryptography, focusing on number theory, probability and statistics. Then, an overarching applied framework of principles for secure system design will be provided. This course also will introduce the applied context of cybersecurity and describe the nature of attacks against networks and systems, along with the history and modern concepts of cryptography. In the discussion of symmetric encryption, you will learn about the difference between stream and block ciphers. You will also see examples of asymmetric encryption schemes, hash functions, digital signature schemes and key establishment protocols. The course concludes by considering how these concepts are applied in practice, such as in public-key infrastructures and in IPSec. The course concludes with a brief introduction to the use of firewalls and intrusion detection systems. Software used includes VirtualBox, Hex Editor and OpenSSL.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA

MASTERS DEGREE IN CYBERSECURITY

Digital Forensics Concentration Course Guide

Data Network, Systems and Security
(3 Credit Hours)

The goal of this course is to provide a technical introduction to data networks. The course is comprised of a series of modules and will include projects, quizzes, and a final exam. The course will start with an overview of database management and operating system technologies, which are critical to network operation and security. Key concepts and technologies in data networks will then be introduced, including layered architectures and topologies. The main elements in information technology networks will then be detailed, including routers, switches, gateways, servers, workstations and storage devices. Monitoring tools and protocols also will be covered, including data transport and addressing. The course will then look at network management and performance optimization, as well as troubleshooting and congestion control. Finally, network security topics will be covered, including encryption, authentication, firewalls and intrusion detection, security management tools and threat scenarios. This material will provide a basis for learning how to install, configure, maintain, upgrade and troubleshoot networks.

Decision Processes for Business Continuity and Disaster Recovery
(3 Credit Hours)

This course introduces students to decision making and risk assessment skills to plan for and respond effectively to disasters affecting our information systems and critical infrastructures with the goal of maintaining business continuity. Course objectives will be accomplished by helping students develop quantitative skills and frameworks to make decisions and assess risks and apply these skills in the service of protecting critical infrastructure. Students will use @Risk by Palisade, an advanced risk analysis software using Monte Carlo simulation, Microsoft Excel and Microsoft Project.

CONCENTRATION COURSES (15 CREDIT HOURS)

Cybercrime and Criminal Justice
(3 Credit Hours)

This course introduces the topic of criminality in online environments. Topics include hacking, online identity theft, fraud, trade in illicit substances/items, sexual crimes online and the criminal justice system's response to cybercriminality.

Digital Evidence Recognition and Collection
(3 Credit Hours)

This course is designed to instruct participants in the basics of recognizing potential sources of electronic evidence, responding to an electronic crime scene, and safely and methodically preserving and collecting items of evidentiary value to be used in court proceedings. Discussion also covers identification, collection, acquisition, authentication, preservation, examination, analysis and presentation of evidence for prosecution purposes. Attention will be given to digital evidence obtained from computer hard drives and removable media. Students will examine legal and evidentiary considerations in the field and the courtroom, the foundations of digital forensics, applying forensic science to digital technologies, digital crime scenes and digital investigations. The course also will include a review of the use of onsite previews and live acquisitions.

Introduction to Digital Evidence
(3 Credit Hours)

This course is designed to introduce students to basic concepts, techniques and procedures involved in the analysis of digital artifacts as they relate to forensic investigations. Basic operating system concepts will be examined, including different types of operating systems and variations among them. The disk, file and directory structures of major operating systems will be explored. Skills covered include logical and physical imaging of digital evidence, the application of cryptographic hash functions, protecting digital evidence, preparing and organizing evidence for analysis and analytical techniques.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA

MASTERS DEGREE IN CYBERSECURITY

Digital Forensics Concentration Course Guide

Network Forensic Criminal Investigations
(3 Credit Hours)

As applied to criminal investigations, this course focuses on forensic security issues involving access to data stored on networked computer systems and the transmission of data between systems. Topics include detecting and monitoring intrusions of networks and systems, authentication protocols, malware and intrusion response strategies.

Digital Forensic Criminal Investigations
(3 Credit Hours)

This course will introduce students to digital forensics as practiced by local, state and federal law enforcement. Students will gain hands-on experience with several digital forensic tools in this laboratory-based course. Students will work through several exercises in which they will conduct a forensic examination of digital images, search for evidence and bookmark files and items of evidential value to the investigation. Students taking this course will become familiar with the emerging responsibilities of cybercrime investigators and develop a hands-on working knowledge of the various software commonly used by many law enforcement agencies.

PRACTICUM (3 CREDIT HOURS)

Practicum for Digital Forensics
(3 Credit Hours)

The MS in Cybersecurity curriculum requires 3 credit hours of "experiential learning" or a practicum that allows students to apply knowledge from their program and to critically consider and address issues relevant to the cybersecurity field. Students will produce and submit a tangible outcome or artifact to document their experience. This can be in the form of an internship report, an essay, an assessment report, an app or any other concrete outcome.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA