DIGITAL FORENSICS, MS

Contacts

Deepika Das, ddas06@syr.edu, 315-443-1036
Assistant Teaching Professor, Director of Curricular Programs for the Forensic and National Security Sciences Institute at Syracuse University

Website

https://thecollege.syr.edu/degree-programs/digital-forensics-ms/

Overview

The M.S. in Digital Forensics is a 36-credit program that combines the iSchool's expertise in information security, digital forensics, and data analytics with the forensic science expertise of the Forensic and National Security Sciences Institute in the College of Arts and Sciences. Digital forensics is the acquisition and analysis of evidentiary information that is stored or transferred in binary form. Digital evidence is found on computers, networks, mobile devices, drones, "smart devices," and in "the cloud." Single investigations often generate dozens of digital devices with terabytes of data. It is the fastest growing area in forensics science. Courses will provide training and experience in the collection, examination, analysis, reporting, and legal proceedings involving digital evidence, preparing graduates for careers in in digital forensics, information security, business intelligence, investigations, and traditional forensic science.

Student Learning Outcomes

1. **Scientific Knowledge and Principles**: Apply knowledge to gain skills required for the identification, collection, preservation, examination and analysis of various types of digital evidence.
2. **Research and Critical Thinking**:
   a. Identify needs for research in digital forensics and critique methods and approaches used in investigations involving digital devices and different data sources.
   b. Use a rationale-based approach to evaluate and analyze complex digital problems relating to networks, file systems, operating systems, hardware and various digital devices.
3. **Ethics and Quality**: Assess and apply ethical standards, integrity, professionalism, and quality assurance protocols and standards as they relate to issues regarding seizure, chain of custody, and issues in acquiring and processing digital evidence.
4. **Communication and Collaboration**: Effectively communicate scientific principles with objectivity and transparency to stakeholders, including scientists and non-scientists.
5. **Practical Implementation**: Investigate digital evidence using forensic techniques and tools. Participate fully in a research project, including communicating findings both orally and in written forms.

Requirements

Code	Title	Credits
Primary Core		
Students are required to take the following seven courses.		
FSC 606	Advanced Forensic Science	3
FSC 633	Quality Assurance and Ethics	3
FSC 656	Mobile Forensics and Social Networking	3
FSC 668	Crime Scene Investigation with lab	3
IST 602	Digital Forensics	3
IST 623	Introduction to Information Security	3
IST 687	Introduction to Data Science	3
Secondary Core		
Select one of the following:		3
IST 618	Information Policy	
IST 704	Applied Information Security	
IST 707	Applied Machine Learning	
Electives		
FSC 631	Statistics for Forensic Science	3
FSC 632	Research and Career Resources	3
FSC 655	Computational Forensics	3
IST 634	Security in Networked Environments	3
IST 636	Leading Issues in Information Security	3
IST 659	Data Administration Concepts and Database Management	3
IST 718	Big Data Analytics	3
IST 719	Information Visualization	3
LAW 759	Computer Crimes	3
LAW 832	Cyber Security Law and Policy	3
Research		

Each student is required to participate in original research, write a detailed report of publishable quality, and successfully defend the results in front of a committee of three faculty members in a public seminar. This research should be conducted as part of an on- or off-campus research project, internship, or independent study. Additional credits of independent study or internship may be used to satisfy elective credit by petition.

FSC 690	Independent Study	1-6
IST 690	Independent Study	1-6