Graduate Programs in

Cybersecurity and Digital Forensics

COLLEGE OF COMPUTING AT ILLINOIS TECH

Illinois Tech's Cybersecurity and Digital Forensics degrees are designed to help students and experienced information-technology professionals become cyber security and forensics practitioners, investigators, managers, and leaders. This program is appropriate for students with a strong academic background who are interested in cyber security, digital forensics, risk control, and information assurance.

The interdisciplinary courses will enhance your technology skills, prepare you for leadership and management, and provide you with a better understanding of policy issues related to information systems and networks. In addition to technology courses, Master of Science students will take courses from Illinois Tech's Chicago-Kent College of Law, which gives cybersecurity and forensics practitioners a thorough grounding in legal issues and compliance.

The programs provide an innovative experience where students work on cutting-edge, industry-sponsored projects. This teaching philosophy prepares students to become innovators, entrepreneurs, and leaders of the future.

Students utilize the resources of the Cyber Forensics and Security Lab and work with industry-standard tools such as EnCase, Forensic ToolKit, MPE+, other AccessData tools, WinHex, Tableau hardware write blockers, and much more.

Courses are held at Illinois Tech's campuses in both Chicago and Wheaton, and the Master of Cyber Forensics and Security is available completely online.

Degrees Offered

Master of Cyber Forensics and Security

Master of Science in Applied Cybersecurity and Digital Forensics

Degree Program Curricula

Master of Cyber Forensics and Security

The Master of Cyber Forensics and Security requires a minimum of 30 credit hours. The degree requires a minimum of 10 courses:

- Six required core courses
- Elective courses may be selected with advisor approval
- Project options

At the conclusion of their studies, graduates of the Master of Cyber Forensics and Security degree should be able to:

- Design and implement a comprehensive enterprise security program using both policy and technology to implement technical, operational, and managerial controls
- Comprehensively investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law
- Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions

Master of Science in Applied Cybersecurity and Digital Forensics

The Master of Science in Applied Cybersecurity and Digital Forensics requires a minimum of 32 credit hours. The degree requires a minimum of 10 courses:

- Five required core courses
- Two law courses, taken at Chicago-Kent College of Law
- Elective courses may be selected with advisor approval
- Thesis and non thesis/project options

In addition to gaining all of the skills taught in the M.A.S. degree program, graduates of the Master of Science in Applied Cybersecurity and Digital Forensics degree should be able to conduct and report on significant research in the areas of cybersecurity and/or digital forensics.

ILLINOIS TECH

Distinctive Programs

The National Security Agency and the United States Department of Homeland Security have designated Illinois Tech as a National Center of Academic Excellence in Cyber Defense Education. This designation results from meeting stringent Center of Academic Excellence criteria and mapping of information technology and management curricula to a core set of cyber defense knowledge units. Students attending such designated institutions are eligible to apply for scholarships and grants through the Department of Defense Cyber Scholarship Program and the Federal Cyber Corps Scholarship for Service Program.

The Center for Cyber Security and Forensics Education (C^2SAFE) is a multidisciplinary center that develops, promotes, and supports education and research in cyber security technologies and management, information assurance, and digital forensics across all academic disciplines at Illinois Tech. Among other activities, it engages with business and industry, government, professional associations, and community colleges to enhance knowledge, awareness, and education in cyber security and digital forensics and improve practices in information assurance. C^2SAFE plans, organizes, and conducts the annual ChiCyberCon cybersecurity and forensics conference, as well as additional activities and student competitions that advance the mission of the center.

Select Core Courses

Cyber Forensics (ITMS 538)

This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation of legal issues involved in network forensics. Technical issues in acquiring court-admissible chains of evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Technical topics covered include detailed analysis of hard disks, files systems (including FAT, NTFS and EXT), and removable storage media; mechanisms for hiding and detecting hidden information; and the hands-on use of powerful forensic analysis tools.

Vulnerability Analysis and Control (ITMS 543)

This course addresses hands-on ethical hacking, penetration testing, and detection of malicious probes and their prevention. It provides students with in-depth theoretical and practical knowledge of the vulnerabilities of networks of computers, operating systems and important applications. Integrated with the lectures are laboratories focusing on the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate and hack other networks.

Cyber Security Technologies (ITMS 548)

Students learn how to prepare for a role as a network security administrator and analyst. Topics include viruses, worms, other attack mechanisms, vulnerabilities and countermeasures, network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can be extended into a full operational security system in a follow-course.

Admission Requirements

Admission to Illinois Tech's Information Technology and Management graduate degree programs is based on a holistic approach that considers a variety of academic, extracurricular, social, and personal qualities. All students are held to a high standard of academic excellence, aptitude in mathematics and science, social service, and a desire to pursue a high-quality educational experience.

- Required for regular admission: four-year bachelor's degree conferred with a minimum cumulative undergraduate GPA of 3.0/4.0 (or its equivalent) from an accredited institution
- Citizens and permanent residents of the United States with a cumulative undergraduate GPA of at least 2.5/4.0 may be admitted as non-degree students
- GRE not required for domestic students who have graduated from a domestic university and who have earned a GPA higher than 3.0
- Admission requirements for international students: https://admissions.iit.edu/graduate/apply/degree-seeking-checklist

Contact

If you have questions regarding admission to Illinois Tech, contact Graduate Admissions at grad.admission@iit.edu.

Learn more about application fee waivers, and how to schedule a campus tour and meet with faculty, at https://admissions.iit.edu/graduate/visit.

For more information about the Cyber Forensics and Security program, including additional program and course requirements, visit https://www.iit.edu/academics/programs/cyber-forensics-and-security-mas.

ILLINOIS TECH