

BS in Cybersecurity: Digital Forensics Concentration



Digital Forensics Concentration

Add specialized expertise to your skill set and customize your BS in Cybersecurity degree by incorporating a Digital Forensics concentration. In law enforcement, digital evidence found on computers, phones, laptops, Fitbits, Alexa, smart refrigerators and other devices can be used to prosecute crimes. In the corporate world, digital forensics is used to investigate data breaches, intellectual property theft, corporate espionage and malicious employees. In the intelligence community, digital forensics is used to obtain actionable intelligence in the pursuit of terrorist organizations and espionage activities by hostile nation states.

Cybersecurity BS Program Requirements

- General Education (39 credits)
- Support Core (9 credits)
- Security Core (39 credits)
- Free Electives (15 credits)

Digital Forensics Concentration (18 Credits)

Students working toward a Cybersecurity: Digital Forensics concentration will complete the Cybersecurity program's Gen Ed core, Support Core, Security Core and Free Elective requirements as well as six (6) of the following eight Security Elective courses.

- LES 331 Electronic Discovery
- SEC 240 Foundations in Cyber Investigations
- SEC 350 Introduction Computer Forensics
- SEC 355 Mobile Device Security and Forensics
- SEC 360 Advanced Mobile and IoT Forensics
- SEC 370 Computer Incident Response Course
- SEC 375 Malware Analysis Techniques
- SEC 440 Network Forensics

For full program details, see the BS in Cybersecurity program sheet. The Cybersecurity program has set a minimum passing grade of "C-" for Security Core and Security Elective courses. Students receiving a grade lower than "C-" in any of these courses must retake that course.

Note: Students interested in declaring a Digital Forensics concentration who do not have enough available elective credits may request a waiver on the SEC480/490 requirement.

Students declaring a Digital Forensics concentration may also earn two certificates, Digital Evidence Discovery and Digital Forensics Investigation, by taking three additional courses: LES 330 – Cyber Law, SEC 360 – Advanced Mobile Device and IoT Forensics, and SEC 375 – Malware Analysis Techniques.



You can apply selected courses (and their credits) in this degree program to a variety of WilmU certificate programs, allowing you to earn a resume-boosting certificate and your bachelor's degree simultaneously. Learn more at wilmu.edu/DualCredit.

Have questions? We're here to help!

Academic Recruiters



Get Started Today!
wilmu.edu/Apply



TECHNOLOGY

WilmU and Dual-Credit ADVANTAGE are registered trademarks of Wilmington University. All rights reserved. © Wilmington University 2024

TEC-140 R43 6/24