

DIGITAL FORENSICS AND INCIDENT RESPONSE MAJOR

Cybersecurity, B.S.

Digital Forensics and Incident Response majors will become proficient with the same tools and technology that would typically require years of field experience to obtain. A total of eight lab-based courses will hone their skills in the most current topics in digital forensics investigations. Students will apply progressive learning strategies to master methods required to identify, investigate and perform post-mortem analysis of digital crimes, and will learn current approaches to detect/deter cybercrime and to investigate incidences related to digital crime, including an adept level of understanding of digital forensic tools and techniques needed to investigate emerging cybercrimes. High-performing students will have the opportunity to enter a 4 + 1 program during their senior year.

Additional student learning outcomes for the major in Digital Forensics and Incident Response are:

- Demonstrate an understanding of current approaches to detect and or deter cybercrime, and to investigate incidences related to digital crime activity.
- Demonstrate an understanding of the digital forensic tools and techniques.
- Express an understanding of current issues relating to digital forensics and determine the best practices for attending to them based upon available resources and tools, and the overall needs of the organization.

Degree requirements for the Digital Forensics and Incident response major are as follows:

| Code | Title | Hours |
|-------------------------------------|---|-------|
| <i>University Core</i> | | |
| Behavioral/Social Science Electives | | 9 |
| BUS 204 | Financial Wellness | 1 |
| ENG 114 | Critical Reading and Response | 3 |
| ENG 134 | Literary Genres | 3 |
| Humanities Electives | | 9 |
| MAT 120 | Statistics | 3 |
| Science Electives (lab required) | | 7 |
| WEL 100 | Empowered as Learners and Leaders | 3 |
| or WEL 220 | Empowered as Learners and Leaders | |
| WEL 350 | Strategies for Career and Personal Growth | 2 |
| <i>Major Requirements</i> | | |
| CBY 101 | Introduction to Cybersecurity | 3 |
| CBY 200 | Introduction to Digital Forensics | 3 |
| CBY 202 | Cyber Governance: Privacy, Ethics, and Digital Rights | 3 |
| CBY 220 | Cyber Investigations I | 3 |
| CBY 225 | Intrusion, Incident Response, and Crisis Management | 3 |
| CBY 301 | Fundamentals of Information Assurance | 3 |
| CBY 310 | Cyber Investigations II | 3 |
| CBY 330 | Mobile Technology Analysis I | 3 |

| | | |
|-------------------------------|---|-----|
| CBY 430 | Mobile Technology Analysis II | 3 |
| CBY 455 | Cybersecurity Capstone | 3 |
| COM 111 | Fundamentals of Computing Technology | 3 |
| CSC 101 | Applied Computing | 3 |
| CSC 210 | Computer Networks and Network Security | 3 |
| CSC 297 | Programming Languages | 3 |
| ENG 124 | Research and Writing in the Disciplines | 3 |
| <i>General Electives</i> | | |
| General Electives | | 35 |
| <i>Total Credits Required</i> | | 120 |