REQUIREMENTS FOR THE DIGITAL FORENSICS AND CYBERSECURITY MINOR

Those students who prefer to specialize in Digital Forensics and Cybersecurity have an opportunity to minor in the program. Methodist University also offers a 21 semester hour minor that will complement any undergraduate degree including (but not limited to) justice studies, computer science, business administration, accounting, mathematics, and education.

Required courses for the minor include: JUS 2430, JUS 2450, JUS 2500, JUS 2510, JUS 2550, JUS 3400, and JUS 3600.

HOW WILL THIS HELP ME FIND A CAREER?

The journey for a Methodist University Digital Forensics and Cybersecurity graduate can lead to success. Graduates can move forward and be accepted to prestigious graduate programs or they can find rewarding careers such as:

- Cyber Forensics Investigator
- Security Awareness and Training Analyst
- Information Security (INFOSEC) Specialist
- Special Agents with Federal Agencies
- Vulnerability and Threat Intelligence Analyst
- Cybersecurity Analyst
- Computer Network Defense Specialist
- Digital Forensics Technician
- Network Security Specialists
- Penetration Tester

WHERE DO I START?

The most common route for those interested in the Digital Forensics and Cybersecurity Program is to sign up for the JUS 2430 Introduction to Cybercrime course. This class provides a basic understanding of the area of cybercrime and serves as an introduction to courses within the program.

CAREER OUTLOOK

Demand for information security professionals is expected to be very high. Cyber attacks have grown in frequency and sophistication over the last few years, and many organizations are behind in their ability to detect these attacks. Analysts will be needed to come up with innovative solutions to prevent attackers from stealing critical information or creating havoc on computer networks.

In 2018, (ISC)^2 conducted a research study that assessed the Cybersecurity Workforce. They estimated the current shortage of information security professionals is almost three million globally; According to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), the United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019. The number of unfilled cybersecurity jobs has grown by more than 50 percent since 2015. By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions. The Bureau of Labor Statistics also projects that the employment outlook for information security related occupations is expected to grow 28% percent from 2016 to 2026.

METHODIST UNIVERSITY

CONTACT INFO

SABRINA KONCABA
Program Director, Digital Forensics and Cybersecurity
skoncaba@methodist.edu
910.630.7516

Design 1.0

DIGITAL FORENSICS
AND CYBERSECURITY PROGRAM

METHODIST UNIVERSITY

[Engage. Enrich. *Empower.*]

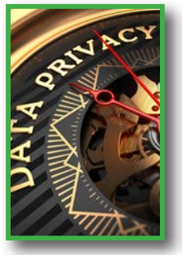
WHAT IS DIGITAL FORENSICS AND CYBERSECURITY?

Digital Forensics and Cybersecurity are two specializations within the Information Technology field that focus on the protection, identification, and prevention of various types of attacks against mobile and computer networks as well as using digital evidence that has been collected, analyzed, and presented to law enforcement personnel to prosecute criminals or help attorneys in civil litigation.

In response to the need for trained information security professionals and the growing number and sophistication of cyber attacks against our nation's businesses, defense industrial base, government and critical infrastructure, Methodist University developed the Digital Forensics and Cybersecurity program.

WHAT ARE THE THREATS THAT WE ARE FACING?

As technology changes, the threat landscape is also evolving. Although malware still exists, attacks are becoming more sophisticated and the attackers are using techniques such as social engineering, bots, zombies, and the like to compromise systems. In addition, the rise of mobile devices (i.e., smartphones and tablets) have added a new level of attack and compromise. Because mobile applications are rapidly developed, application level security is usually not considered. This makes them a prime target for cybercriminals. Students who complete the Methodist University's Digital Forensics and Cybersecurity program will be able to identify threats and help businesses protect against various types of cyber attacks.



WHY DO WE NEED CYBERSECURITY AND DIGITAL FORENSICS PROFESSIONALS?

Organizations are reaching out for trained and skilled information security professionals to help fill key positions. People with the right skill sets are becoming increasingly scarce and companies need individuals who can protect their programs and data from unintended or unauthorized access, change, or destruction. With the growing number of different technology platforms, there is a huge increase in the number of vulnerabilities to be exploited. Cyber criminals only need one way in, but trained professionals must be knowledgeable in all areas of information security. In addition, the skills gap is ever widening and businesses need professionals who can make recommendations based on business strategic initiatives as well as implement security measures that are cost effective and sustainable for long term management. Information Security Professionals who can act in both realms are rare. Many sectors including the government, utilities, and education need those individuals who are motivated and willing to step up to help defend our nation. Methodist University's program trains those individuals by offering applied learning and also helps them achieve industry standard certifications so they can prove their competency to prospective employers.

THE PROGRAM

Methodist University's Digital Forensics and Cybersecurity major is a 36 hour program that will prepare students for a career in the ever-growing Information Technology Security field. It is designed to provide graduates with a holistic view of information security from securing desktop systems to investigating digital intrusions and reporting findings to the proper authorities. The prevalence of companies and electronic devices in society has highlighted a need for those trained in digital evidence collection as well as those who can identify mitigate, protect and respond to the wide variety of cyber attacks. This program is designed to give students a leg up from the average undergraduate candidate, providing hands-on experience with network security and electronic evidence collection. Students who complete Methodist University's program requirements for a major in Digital Forensics and Cybersecurity will be qualified to enter private and public sector occupations focused on preventing, detecting and mitigating cyber attacks as well as gathering digital evidence and electronic crime investigations. Students receive information security content and skills in the following areas:

- Operating Systems
- Networking Concepts
- Cyber Intelligence
- Penetration Testing
- Vulnerability Scanning
- Network Forensics and Incident Response
- IT Governance
- Digital Forensics
- Virtualization
- Social Media Security and Investigations

THE COURSEWORK

Required Non-Digital Forensics and Cybersecurity Courses

- CSC 1000 | Introduction to Computers
- JUS 2200 | Applied Statistics
- JUS 2410 | Introduction to Criminal Justice
- JUS 3090 | Criminology
- JUS 3320 | Research Methods
- JUS 3890 | Criminal Evidence and Procedure
- JUS 4500 | Seminar in Criminal Justice

Note: Students must also complete university core requirements as outlined in the catalogue for the year they entered Methodist University or the catalogue they have chosen.

Required Digital Forensics and Cybersecurity Courses

- JUS 2430 | Introduction to Cybercrime
- JUS 2450 | Cybercrime Law and Ethics
- JUS 2470 | Operating Systems and Programming
- JUS 2500 | Digital Crime Investigation
- JUS 2510 | Networking Concepts
- JUS 2550 | Hardening The Enterprise Network
- JUS 2650 | Cyber Threats and Counterintelligence
- JUS 3400 | Penetration Testing and Vulnerability Scanning
- JUS 3600 | Basic Data Recovery
- JUS 4050 | Incident Response and Network Forensics
- JUS 4450 | Social Media and Cloud Security
- JUS 4650 | Mobile Device Forensics