Program Overview
Mason Engineering offers a Master of Science in Digital Forensics & Cyber Analysis through its Department of Electrical and Computer Engineering. The program prepares students for careers in industry, government, and academia by combining academic education with real-world practical techniques. Emphasis is placed on training students to use and apply computer forensics methods and knowledge in a variety of scenarios. Computer forensic examiners (CFEs) work in the public and private sectors. The Washington, D.C., area is home to a large workforce of CFEs, who work for the FBI, DEA, and Secret Service, as well as with the vast majority of inspectors general and local police departments. Practically all the major accounting and consulting firms have CFEs on staff, and there is a growing cadre of independent consultants who work in this field.

The distinctiveness of Mason’s program lies in the curriculum, which has been tailored to strengthen the employment opportunities of students in nonacademic jobs, as well as prepare students who may wish to pursue a doctorate. The program incorporates faculty research and teaching interests on a range of contemporary topical issues. It also provides students with advanced training in computer and network digital evidence, intrusion forensics, and legal and ethical issues.

Program Requirements
The MS in Digital Forensics & Cyber Analysis requires completion of a minimum of 30 credits of graduate course work with a core component of 21 credits (including a capstone course), and either a 9 credit concentration in penetration testing/reverse engineering or an elective component of 9 credits.

Core course options include:
- Introduction to Forensic Technology and Analysis
- Digital Forensics Analysis
- Network Forensics
- Digital Media Forensics
- Operations of Intrusion Detection for Forensics
- Legal and Ethical issues in IT
- Advanced Computer Forensics

Students may also take a range of courses offered by the MS in Digital Forensics & Cyber Analysis or other areas, such as Mobile Device Forensics, Penetration Testing in Computer Forensics, Malware Reverse Engineering and Memory Forensics.

Related Programs
- Electrical and Computer Engineering, PhD
- Information Security and Assurance, MS
- Information Technology, PhD
- Telecommunications, MS
Digital Forensics (M.S.)

Distance Education courses may be available for select programs. Graduate Certificate degree programs may also be offered. Please visit our website for details.

Admission Requirements
In addition to meeting general university admissions requirements, students should hold a BS or BA in engineering, math, science, computer science, business (with a quantitative background), economics, or other analytical disciplines from an accredited college or university, or students should hold a BS or BA from a college or university and have equivalent work experience indicating analytical aptitude. Typically, a minimum undergraduate GPA of 3.00 is required for acceptance.

Required application materials include:
- Online application and non-refundable fee
- Transcripts showing all post-secondary study
- Professional and Educational Goals Statement
- Two letters of recommendation from professors or senior officials at place of employment
- Self-Evaluation
- Resume

Additional application materials, including English proficiency examination scores (e.g., TOEFL, IELTS), are required if the applicant holds a degree from an international institution and/or requires an F-1 or J-1 visa. Visit http://admissions.gmu.edu/grad for details.

Special admission programs are available for Volgenau School students and alumni.

Visit our website for details: http://cftrs.gmu.edu
Apply online: http://admissions.gmu.edu/grad/applynow