About the MS in Digital Forensics

Digital forensics is the interdisciplinary science of detecting, collecting, processing, and analyzing digital information for the purpose of verifying/validating the existence of an event. Digital forensics supports all investigative endeavors. Digital forensics includes computer engineering, computer science, information technology, network engineering, telecommunications law, analytics, and ethics. In the last 35 years, digital forensics has evolved into its own industry.
Once primarily focused on supporting criminal prosecutions, digital forensics includes civil litigation, intelligence analysis, internal organizationa matters, and cyber critical incidents.

Scan Here for More Information

George Mason University
4400 University Drive
Fairfax, VA 22030

https://dfor.gmu.edu dfor@gmu.edu +1 (703) 993-3810

GEORGE MASON UNIVERSITY

Where Innovation Is Tradition

Prof. Bob Osgood
Director
Digital Forensics

rosgood@gmu.edu
(703) 993 - 5443

It's Not What You Know,
Its What You Can Prove!

Master of Science in Digital Forensics

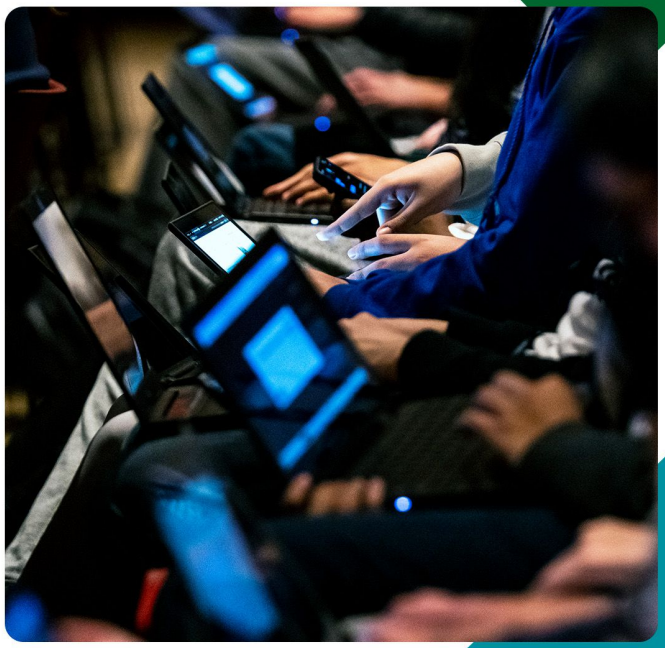
Admission Requirements

Students who hold a B.S. or B.A. degree from an accredited college or university with a technical background may apply. Technical competency for the DFOR program includes programming (Python preferred), Operating systems (Windows/Linux), TCP/IP, and Switching/Routing. Certifications can be used to meet entry level technical competency: A+, Net+, CCNA/CCNP Linux +, etc. Students lacking the required technical requirements will be required to complete certain foundation courses.

An undergraduate GPA of 3.00 is suggested for acceptance.

Degree Requirements

The M.S. in Digital Forensics requires the completion of a minimum of 30 hours of graduate course work with a GPA of 3.0 or higher. The DFOR program is split into two elements: A Core component of 21 credit hours (18 credit hours plus a mandatory, 3-credit, capstone course that is taken towards the end of the degree) and an Elective component of 9 credit hours.



Foundation Components If Required

(Does not count towards degree)

DFOR 500 Introduction to Forensic Technology and Analysis
TCOM 535 TCP/IP
TOCM 514 Switching or TCOM 515 Routing

Core Components (21cr.)

DFOR 510 Digital Forensics Analysis
DFOR 660 Network Forensics
DFOR 661 Digital Media Forensics
DFOR 672 Mobile Device Forensics
Either DFOR 663 Operation of Intrusion Detection for Forensics Or DFOR 664 Incident Response Forensics
Either DFOR 671 Legal and Ethics Or
DFOR 670 Fraud Analytics
DFOR 790 Advanced Computer Forensics (capstone)

Elective Components (9 cr.) A range of courses may be taken.

Below is a selection pf courses.

DFOR 698 Selective Readings and Research in DFOR
DFOR 710 Memory Forensics
DFOR 720 Digital Audio-Video Forensics
DFOR 675 Linux Forensics
DFOR 637 Cloud Forensics
DFOR 730 Forensic Deep Packet Inspection
DFOR 761 Malware Reverse Engineering
DFOR 698 Selective Readings and Research in DFOR

DFOR 710 Memory Forensics
DFOR 720 Digital Audio-Video Forensics
DFOR 675 Linux Forensics
DFOR 637 Cloud Forensics
DFOR 730 Forensic Deep Packet Inspection
DFOR 761 Malware Reverse Engineering
DFOR 773 Mobile Application Forensics and Analysis
DFOR 775 Kernel Forensics & Analysis
DFOR 780 Special Topics Course
DFOR 798 Research Project
ECE 511 Microprocessors
ECE 646 Cryptography & Network Security
ECE 746 Secure Telecommunication Systems
FRSC 510 Crime Scene Analysis
DFOR 673 Registry Forensics
DFOR 674 MAC Forensics
DFOR 767 Pen Testing & Ethical Hacking
DFOR 768 Digital Warfare
DFOR 769 Anti-forensics
DFOR 771 Forensic Digital Profiling
DFOR 772 Forensic Artifact Extraction
ISA 650 Security Policy
ISA 652 Security Audit/Compliance Testing
ISA 656 Network Security
ISA 674 Intrusion Detection
ISA 785 Research in Digital Forensics
TCOM 662 Advanced Secure Networking