VOLGENAU SCHOOL OF ENGINEERING

GEORGE MASON UNIVERSITY

MS in Digital Forensics & Cyber Analysis

Introduction:

Digital forensics is the science of detecting, processing, and analyzing digital information such that this information can be admitted as evidence into a court of law. Digital forensics supports all investigative endeavors. It is interdisciplinary in its nature, including topics and tools from computer engineering, computer science, information technology, network engineering, telecommunications, law, and ethics. In the last 30 years, digital forensics has evolved into its own industry. Once primarily focused on supporting criminal prosecutions, computer forensics also supports civil litigation, the intelligence community, and cyber critical incidents.

Admission Requirements:

Students who hold a B.S. or B.A. degree from an accredited college or university in engineering, math, science, computer science, business (with a quantitative background), economics, or other analytical disciplines, or students who hold a B.S. or B.A. degree from an accredited college or university and who have equivalent work experience indicating analytical aptitude, may apply to the M.S in Digital Forensics & Cyber Analysis. An undergraduate GPA of 3.00 is suggested for acceptance. Up to 12 credits of prerequisites may be required in operating systems, programming, and digital networks.

Degree Requirements:

The M.S. in Computer Forensics requires the completion of a minimum of 30 hours of graduate course work with a GPA of 3.000, or higher. The CFRS program is split into two elements: A ***Core*** component of 18 credit hours (15 credit hours plus a mandatory, 3-credit, capstone course that is taken towards the end of the degree) and an ***Elective*** component of 12 credit hours.

Core Component (18 cr.):

Either CFRS 500 Introduction to Forensic Technology and Analysis ***Or*** ISA 562 Information Security Theory and Practice (CFRS 500 is required for those with little to no experience in the computer forensics.)
CFRS 660 Network Forensics
CFRS 661 Digital Media Forensics
Either CFRS 663 Operation of Intrusion Detection for Forensics **Or** CFRS 664 Incident Response Forensics
Either CFRS 760 Legal and Ethics ***Or*** CFRS 770 Fraud and Forensics in Accounting
CFRS 790 Advanced Computer Forensics (capstone)

Elective Component (12 cr.): A range of courses may be taken. Below is a selection of courses:

CFRS 510 Digital Forensics Analysis	CFRS 771 Forensic Digital Profiling
CFRS 663 Operation of Intrusion Detection for Forensics	CFRS 772 Forensic Artifact Extraction
CFRS 664 Incident Response Forensics	CFRS 773 Mobile Application Forensics and Analysis
CFRS 698 Selective Readings and Research in CFRS	CFRS 775 Kernel Forensics & Analysis
CFRS 710 Memory Forensics	CFRS 780 Special Topics Course
CFRS 720 Digital Audio-Video Forensics	CFRS 798 Research Project
CFRS 725 Linux Forensics	ECE 511 Microprocessors
CFRS 737 Cloud Forensics	ECE 646 Cryptography and Computer- Network Security
CFRS 730 Forensic Deep Packet Inspection	
CFRS 760 Legal and Ethics	ECE 746 Secure Telecommunication Systems
CFRS 770 Fraud and Forensics in Accounting	FRSC 510 Crime Scene Analysis
CFRS 761 Malware Reverse Engineering	INFS 785 Data Mining for Homeland Security
CFRS 762 Mobile Device Forensics	ISA 650 Security Policy
CFRS 763 Registry Forensics	ISA 652 Security Audit/Compliance Testing
CFRS 764 MAC Forensics	ISA 656 Network Security
CFRS 767 Pen Testing & Ethical Hacking	ISA 674 Intrusion Detection
CFRS 768 Digital Warfare	ISA 785 Research in Digital Forensics
CFRS 769 Anti-forensics	TCOM 662 Advanced Secure Networking

For more information, please visit

http://cfrs.gmu.edu/

Bob Osgood

Director Digital Forensics & Cyber Analysis

rosgood@gmu.edu

(703) 993 – 5443