DIGITAL FORENSICS, MS

Banner Code: VS-MS-DFOR

3100 Nguyen Engineering Building
MS 1G5

Phone: (703) 993-1569
Email: ece@gmu.edu

Digital forensics is a discipline addressing the collection, processing, and analysis of digital data for the purpose of verifying/validating the existence of an event of investigative, intelligence, cyber, or business interest. The data can be from physical media, a mobile device, real-time network traffic, the Internet of Things (IoT), unknown code, memory, and many other sources. Digital forensics is interdisciplinary by nature and our program includes computer engineering, computer science, information technology, law, and ethics. Digital forensics is a key component in criminal, corporate, civil, cyber defense, incident response, intelligence, and counter-terrorism matters. In the last several years, with a proliferation of digital storage, transmission, and processing of sensitive information, there has been an increase in the aberrant use of digital devices. This aberrant behavior includes but is not limited to: digital extortion, intrusions, economic espionage, child exploitation, cybercrime, fraud, terrorism, and identity theft. In response to this, digital forensics has become an important profession serving both public and private sectors. The MS in Digital Forensics will prepare graduates for a wide variety of careers to include law enforcement, various other branches of government, incident response, and all facets of cyber security by combining academic education with real world practical techniques and by offering advanced training in analyzing digital evidence, intrusion forensics, reverse engineering, network analysis, and legal and ethical matters.

Admissions & Policies

Admissions

Students who hold a bachelor's 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 have equivalent work experience indicating analytical aptitude, may apply. Depending on their background, some domestic applicants may be accepted provisionally and required to complete 3 to 12 credits of preliminary coursework before they are allowed to enroll in any of the core or specialty courses in the program. A minimum undergraduate GPA of 3.00 is required for acceptance.

Requirements

(formerly VS-MS-CFRS)
Degree Requirements

Total credits: 30

Students must complete a minimum of 30 graduate credits beyond the bachelor's degree with a GPA of 3.00 or higher, with no more than 6 credit hours of C grades. The plan of study includes a 21-credit required core component which includes a mandatory capstone course, and the choice of either a concentration or a 9-credit elective component as shown below:

Core Courses

Code	Title	Credits
CFRS 510	Digital Forensics Analysis	3
CFRS 660	Network Forensics	3
CFRS 661	Digital Media Forensics	3
CFRS 663	Operations of Intrusion Detection for Forensics	3
or CFRS 664	Incident Response Forensics	
CFRS 760	Legal and Ethical Issues in IT [1]	3
or CFRS 770	Fraud and Forensics in Accounting	
CFRS 762	Mobile Device Forensics	3
CFRS 790	Advanced Computer Forensics	3
Total Credits		21

[1] Both CFRS 760 Legal and Ethical Issues in IT and CFRS 770 Fraud and Forensics in Accounting may be taken, but only one may be used in the core component.

Concentration in Penetration Testing/Reverse Engineering (PTRE)

Focused on the practical aspects of penetration testing and reverse engineering. Students are expected to master tools, techniques, and methodologies of penetration testing and reverse engineering.

Code	Title	Credits
CFRS 761	Malware Reverse Engineering	3
CFRS 767	Penetration Testing in Computer Forensics	3
CFRS 772	Forensic Artifact Extraction	3
or CFRS 775	Kernel Forensics and Analysis	
Total Credits		9

Electives

Code	Title	Credits
Students who do not choose the above concentration should select 9 credits from the following:		9
CFRS 590	Special Topics in Computer Forensics	
CFRS 663	Operations of Intrusion Detection for Forensics	
CFRS 664	Incident Response Forensics	
CFRS 698	Independent Reading and Research	
CFRS 710	Memory Forensics	
CFRS 720	Digital Audio Video Forensics	
CFRS 725	Linux Forensics	
CFRS 730	Forensic Deep Packet Inspection	
CFRS 737	Cloud Forensics	
CFRS 760	Legal and Ethical Issues in IT [1]	
CFRS 761	Malware Reverse Engineering	
CFRS 762	Mobile Device Forensics	
CFRS 763	Registry Forensics - Windows	

CFRS 764	Mac Forensics
CFRS 767	Penetration Testing in Computer Forensics
CFRS 768	Digital Warfare
CFRS 769	Anti-Forensics
CFRS 770	Fraud and Forensics in Accounting [1]
CFRS 771	Digital Forensic Profiling
CFRS 772	Forensic Artifact Extraction
CFRS 773	Mobile Application Forensics and Analysis
CFRS 775	Kernel Forensics and Analysis
CFRS 780	Advanced Topics in Computer Forensics
ECE 511	Computer Architecture
ECE 611	Advanced Computer Architecture
ECE 612	Real-Time Embedded Systems
ECE 642	Design and Analysis of Computer Communication Networks
ECE 646	Applied Cryptography
ECE 746	Advanced Applied Cryptography
ISA 650	Security Policy
ISA 652	Security Audit and Compliance Testing
ISA 656	Network Security
ISA 674	Intrusion Detection
ISA 785	Research in Digital Forensics
TCOM 662	Advanced Secure Networking
FRSC 510	Basic Crime Analysis
Total Credits	9

[1] Both CFRS 760 Legal and Ethical Issues in IT and CFRS 770 Fraud and Forensics in Accounting may be taken, but only one may be used in the core component.

Other courses may be appropriate as electives in the degree program, but they must be approved prior to registration.

Accelerated Master's

Applied Science, BAS Cyber Security Concentration/Digital Forensics, Accelerated MS

Overview

Highly-qualified students in the Applied Science, BAS, Cyber Security Concentration (http://catalog.gmu.edu/colleges-schools/interdisciplinary-programs-courses/applied-science-bas/#cybs) have the option of obtaining an accelerated Digital Forensics, MS.

For more detailed information, see AP.6.7 Bachelor's/Accelerated Master's Degrees (http://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7). For policies governing all graduate degrees, see AP.6 Graduate Policies (http://catalog.gmu.edu/policies/academic/graduate-policies/).

Admission Requirements

Students in the Applied Science, BAS, Cyber Security Concentration (https://catalog.gmu.edu/colleges-schools/interdisciplinary-programs-courses/applied-science-bas/#cybs) program may apply for this option if they have earned 90 undergraduate credits with an overall GPA of at least 3.25. Criteria for admission are identical to criteria for admission to the Digital Forensics, MS program.

Accelerated Option Requirements

Students must complete all credits that satisfy requirements for the BAS and MS programs, with 6 credits overlapping with two of the following four courses:

Code	Title	Credits
CFRS 510	Digital Forensics Analysis	3
CFRS 660	Network Forensics	3
CFRS 661	Digital Media Forensics	3
CFRS 664	Incident Response Forensics	3

Degree Conferral

Students must apply the semester before they expect to complete the BAS requirements to have the BAS degree conferred. In addition, at the beginning of the student's final undergraduate semester, students must complete a Bachelor's/Accelerated Master's Transition form that is submitted to the Office of the University Registrar and the VSE Graduate Admissions Office. At the completion of MS requirements, a master's degree is conferred.

Cyber Security Engineering, BS/Digital Forensics, Accelerated MS

Overview

Highly-qualified students in the Cyber Security Engineering, BS (http://catalog.gmu.edu/colleges-schools/engineering/cyber-security-engineering/cyber-security-engineering-bs/) have the option of obtaining an accelerated Digital Forensics, MS.

For more detailed information, see AP.6.7 Bachelor's/Accelerated Master's Degrees (http://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7). For policies governing all graduate degrees, see AP.6 Graduate Policies (http://catalog.gmu.edu/policies/academic/graduate-policies/).

Admission Requirements

Students in the Cyber Security Engineering, BS (http://catalog.gmu.edu/colleges-schools/engineering/cyber-security-engineering/cyber-security-engineering-bs/) program may apply for this option if they have earned 90 undergraduate credits with an overall GPA of at least 3.25. Criteria for admission are identical to criteria for admission to the Digital Forensics, MS program.

Accelerated Option Requirements

Students must complete all credits that satisfy requirements for the BS and MS programs, with 6 credits overlapping.

Students register for two Digital Forensics core courses (6 credits) in place of two of the three required technical electives, as part of the undergraduate degree requirements. Specifically, students must take:

Code	Title	Credits
CFRS 500	Introduction to Forensic Technology and Analysis	3
and one of the following:		3

CFRS 510	Digital Forensics Analysis (satisfies the IT 357 requirement for the INFS concentration in the BS program)	
CFRS 660	Network Forensics (satisfies one NTEL concentration course in the BS program)	
Total Credits		6

Note: Students complete all Digital Forensics, MS core courses and apply the two courses from the above list toward the Digital Forensics, MS requirements.

Degree Conferral

Students must apply the semester before they expect to complete the BS requirements to have the BS degree conferred. In addition, at the beginning of the student's final undergraduate semester, students must complete a Bachelor's/Accelerated Master's Transition form that is submitted to the Office of the University Registrar and the VSE Graduate Admissions Office. At the completion of MS requirements, a master's degree is conferred.

Information Technology, BS/Digital Forensics, Accelerated MS

Overview

Highly-qualified students in the Information Technology, BS (http://catalog.gmu.edu/colleges-schools/engineering/information-sciences-technology/information-technology-bs/) have the option of obtaining an accelerated Digital Forensics, MS.

For more detailed information, see AP.6.7 Bachelor's/Accelerated Master's Degrees (http://catalog.gmu.edu/policies/academic/graduate-policies/#ap-6-7). For policies governing all graduate degrees, see AP.6 Graduate Policies (http://catalog.gmu.edu/policies/academic/graduate-policies/).

Admission Requirements

Students in the Information Technology, BS (http://catalog.gmu.edu/colleges-schools/engineering/information-sciences-technology/information-technology-bs/) program may apply for this option if they have earned 90 undergraduate credits with an overall GPA of at least 3.25. Criteria for admission are identical to criteria for admission to the Digital Forensics, MS program.

Accelerated Option Requirements

Students must complete all credits that satisfy requirements for the BS and MS programs, with 6 credits overlapping with two of the following three courses:

Code	Title	Credits
CFRS 500	Introduction to Forensic Technology and Analysis	3
CFRS 510	Digital Forensics Analysis (satisfies the IT 357 requirement for the INFS concentration in the BS program)	3
CFRS 660	Network Forensics (satisfies as one NTEL concentration course in the BS program)	3

Degree Conferral

Students must apply the semester before they expect to complete the BS requirements to have the BS degree conferred. In addition, at the beginning of the student's final undergraduate semester, students must complete a Bachelor's/Accelerated Master's Transition form that is submitted to the Office of the University Registrar and the VSE Graduate Admissions Office. At the completion of MS requirements, a master's degree is conferred.