TOPIC: University of Maryland University College: Master of Science in Digital Forensics and Cyber Investigation

COMMITTEE: Education Policy

DATE OF COMMITTEE MEETING: March 28, 2012

SUMMARY: In 2010, upon approval by MHEC and the Board of Regents of the University System of Maryland, UMUC launched a suite of degree and certificate programs in cybersecurity, which quickly attained combined enrollments of more than 3,000 part-time students. The existing programs are the centerpiece of a range of activities that UMUC has undertaken to foster awareness of cybersecurity issues and establish itself as a national leader in cybersecurity education. UMUC faculty actively participate in national and global conferences and seminars related to cybersecurity, and UMUC has hosted several face-to-face and virtual cybersecurity seminars.

Officials at the Department of Defense (DoD) Cyber Crime Center (DC3) have identified a pressing need on a national level for expert practitioners in digital forensics. The national authority in digital forensics, DC3 was founded to "enhance through research, science, engineering, analysis, and planning current and future capabilities to conduct electronic forensic analysis, threat analysis, cyber investigations, and operations." (http://www.dc3.mil/). To encourage institutions to develop high quality educational programs that will provide training in digital forensics, DC3 is sponsoring a new effort to establish National Centers of Digital Forensics Academic Excellence (CDFAE). Institutions can become CDFAEs after demonstrating a tangible commitment to providing high-quality digital forensics education. This program is similar to the Centers of Academic Excellence in Information Assurance (CAE), a program jointly sponsored by the National Security Agency and Department of Homeland Security. UMUC is already designated as a CAE, and it is a logical extension for UMUC to seek recognition as a CDFAE as a sign of UMUC's commitment to support the national need for expanded education in digital forensics. In the event that the proposed degree is approved, UMUC has been invited by DC3 to pre-load its programs for consideration of CDFAE certification.

Similar to UMUC's existing Cybersecurity and Cybersecurity Policy master's degrees, the proposed M.S. in Digital Forensics and Cyber Investigation will prepare students for careers in industry, government, and academia by combining academic education with real world practical techniques. The program will emphasize educating students to use and apply computer forensics methods and knowledge in a variety of real life scenarios. Computer forensic specialists work in both the public and private sectors, and the Maryland/Virginia/Washington, D.C. corridor is home to a large potential work force including Computer Forensic Examiners (CFEs). CFEs work for the FBI, DEA, USSS, as well as with the vast majority of Inspectors General and local police departments. Practically all of the major accounting and consulting firms employ computer forensic examiners on staff, and there is a growing cadre of independent consultants that work in this field.

On the national level, Forensics Focus, an online repository of forensics articles and resources, lists only eleven master's degree programs related to digital forensics in the United States (see http://www.forensicfocus.com/computer-forensics-education-north-america). These include one program each in California, Florida, Maryland, New York, Rhode Island, Texas, and Vermont and two programs each in Pennsylvania and Virginia. The Maryland program listed by Forensics Focus is the Master of Science in Security Informatics at Johns Hopkins University. Although there is no existing

program specifically in Digital Forensics in Maryland, Stevenson University has proposed a program in Cyber Forensics that is currently in the approval process, and several institutions offer programs in related fields. However, UMUC's program would be unique when compared with existing or the proposed Stevenson University program in terms of curriculum, admissions requirements, mode of delivery, and intended student audience.

ALTERNATIVE(S): The Regents may not approve the program or may request further information.

FISCAL IMPACT: No additional funding is necessary. The program will be supported through tuition and a one-time reallocation of funds.

CHANCELLOR'S RECOMMENDATION: That the Committee on Education Policy recommend that the Board of Regents approve the proposal from the University of Maryland University College to offer the Master of Science in Digital Forensics and Cyber Investigation.

COMMITTEE RECOMMENDATION: DATE:

BOARD ACTION: DATE:

SUBMITTED BY: Irwin Goldstein (301) 445-1992 irv@usmd.edu

University of Maryland University College
Office of the Provost

March 7, 2012

Danette G. Howard, Ph.D.
Interim Secretary of Higher Education
Maryland Higher Education Commission
6 North Liberty Street
Baltimore, MD 21201

Dear Dr. Howard:

University of Maryland University College (UMUC) proposes to create a new degree, the Master of Science (M.S.) in Digital Forensics and Cyber Investigation. The proposed M.S. is an outgrowth of UMUC's growing focus on cybersecurity and would complement UMUC's existing suite of successful programs: two master's degrees (Cybersecurity and Cybersecurity Policy), three cybersecurity post-baccalaureate certificates (Foundations of Cybersecurity, Cybersecurity Policy, and Cybersecurity Technology), and a Bachelor of Science in Cybersecurity.

The proposed 36-semester hour M.S. in Digital Forensics and Cyber Investigation will consist of four existing courses drawn from the curriculum of the M.S. in Cybersecurity (HEGIS 070212; CIP 111003), plus two new courses developed specifically for this new program.

Offering the Digital Forensics and Cyber Investigation degree will allow UMUC to leverage its institutional capabilities and experience in cybersecurity to address a workforce need in Maryland. It also will support the State of Maryland's emergent growth as an epicenter of the cybersecurity industry. UMUC has sufficient resources to implement the new program and it will not require new funds from the state.

If you have questions or need additional information about UMUC's proposal to modify this degree program, please feel free to contact me or Dr. Marcia Watson, Assistant Provost for Academic Affairs.

Sincerely,

Greg von Lehmen, Ph.D.
Provost

Enclosure

cc: Dr. Irwin Goldstein
Mr. Robert Goodwin

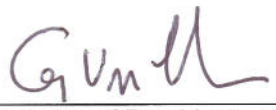
3501 University Boulevard East, Adelphi, MD 20783-8001 USA
301-985-7174 ■ Fax 301-985-6432 ■ www.umuc.edu

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

X	New Instructional Program
	Substantial Expansion/Major Modification
	Cooperative Degree Program
X	Within Existing Resources or
	Requiring New Resources

University of Maryland University College
Institution Submitting Proposal

Master of Science in Digital Forensics and Cyber Investigation
Title of Proposed Program

Master of Science	**Fall, 2012**
Degree to be Awarded	Projected Implementation Date
TBD	**430116**
Proposed HEGIS Code	Proposed CIP Code
The Graduate School	**Robert Goodwin, JD**
Department in which program will be located	Department Contact
(240) 684-2400	**graddean@umuc.edu**
Contact Phone Number	Contact E-Mail Address
	3/7/12
Signature of President or Designee	Date

University of Maryland University College
Master of Science in Digital Forensics and Cyber Investigation

University of Maryland University College (UMUC) proposes to create a new degree, the Master of Science (M.S.) in Digital Forensics and Cyber Investigation. The proposed M.S. is an outgrowth of UMUC's growing focus on cybersecurity. In just two years, UMUC has become an established leader in cybersecurity education, with over 3,000 students enrolled in a suite of highly successful programs: two master's degrees (Cybersecurity and Cybersecurity Policy), three cybersecurity post-baccalaureate certificates (Foundations of Cybersecurity, Cybersecurity Policy, and Cybersecurity Technology), and a Bachelor of Science in Cybersecurity.

The proposed 36-semester hour M.S. in Digital Forensics and Cyber Investigation will consist of four existing courses drawn from the curriculum of the M.S. in Cybersecurity, plus two new courses developed specifically for this new program.

Offering the Digital Forensics and Cyber Investigation degree will allow UMUC to leverage its institutional capabilities and experience in cybersecurity to address a workforce need in Maryland. It also will support the State of Maryland's emergent growth as an epicenter of the cybersecurity industry.

Mission

The mission of University of Maryland University College (UMUC) is "to offer top-quality educational opportunities to adult students in Maryland, the nation, and the world, setting the global standard of excellence in adult education. By offering academic programs that are respected, accessible, and affordable, UMUC broadens the range of career opportunities available to students, improves their lives, and maximizes their economic and intellectual contributions to Maryland and the nation." (http://www.umuc.edu/gen/mission.shtml).

The proposed M.S. in Digital Forensics and Cyber Investigation will support UMUC's mission by serving a large pool of prospective candidates in the Maryland, Virginia, Washington D.C. corridor and beyond, who are currently employed in or seeking a career in a cybersecurity-related field. The workplaces of the prospective candidates include private industry along with Federal, State, and local governmental agencies. Designated as a *National Center of Academic Excellence in Information Assurance Education* by the National Security Agency (NSA) and the Department of Homeland Security (DHS), UMUC is well positioned to serve this workforce need.

The proposed degree will be accessible to any academically qualified individual through UMUC's totally online virtual campus, and thus will support UMUC's mission of providing broad access to top-quality educational programs. The UMUC virtual campus allows students to perform hands-on work remotely using an Internet-based, state-of-the-art virtual laboratory, providing students with critical hands-on experience in a real-time environment. Moreover, UMUC's curriculum is designed specifically to meet the needs of adult students, who may require more flexibility in academic programs, support services and delivery methods (*2009*

Maryland State Plan for Postsecondary Education). UMUC provides flexibility in class schedules, locations and ways for students to interact with their peers and faculty.

UMUC has a long-standing commitment to military students, and 56% of UMUC's worldwide student population are active-duty service members or military affiliates. UMUC also serves students who are currently employed but who must acquire additional education to meet new requirements in their fields, or to enter a new field or to qualify for advancement. It is UMUC's mission to serve the educational needs of the workforce throughout the career span, providing re-education as necessary to keep up with shifts in individual career goals, the overall labor market and technology demands.

Rationale and Need for the Proposed Program

The decision to pursue this program is aligned with UMUC's internal goals as well as with key initiatives of the University System of Maryland and at the state and federal levels.

Internal: It is part of UMUC's mission to offer workforce related programs. In 2010, upon approval by MHEC and the Board of Regents of the University System of Maryland, UMUC launched a suite of degree and certificate programs in cybersecurity, which quickly attained combined enrollments of more than 3,000 part-time students:

- BS in Cybersecurity (HEGIS 070210; CIP 111003)
- M.S. in Cybersecurity (HEGIS 070212; CIP 111003)
- M.S. in Cybersecurity Policy (HEGIS 070213; CIP 111003)
- Post-graduate certificates in:
    - Foundations of Cybersecurity (HEGIS 070202; CIP 111003)
    - Cybersecurity Technology (HEGIS 070208; CIP 111003)
    - Cybersecurity Policy (HEGIS 070201; CIP 111003)

The existing programs are the centerpiece of a range of activities that UMUC has undertaken to foster awareness of cybersecurity issues and establish itself as a national leader in cybersecurity education. UMUC faculty actively participate in national and global conferences and seminars related to cybersecurity, and UMUC has hosted several face-to-face and virtual cybersecurity seminars.

University System of Maryland (USM): The proposed M.S. in Digital Forensics and Cyber Investigation supports USM's strategic plan, *Powering Maryland Forward: USM's 2020 Plan for More Degrees, A Stronger Innovation Economy, A Higher Quality of Life.* The 2020 Plan's strategies to support Theme 2 (Maryland's Economic Development and the Health and Quality of Life of Its Citizens—Ensuring Maryland's Competitiveness in the New Economy) include "increasing the number of graduates produced in workforce areas that are key to the state's ability to thrive and compete (including STEM, education, nursing, health care, **cybersecurity**, and other disciplines) and "Strengthen and promote programs designed to alleviate key workforce shortages and boost training and research in such vital health-care fields as medicine,

nursing, pharmacy, allied health, public health, and the emerging area of **cybersecurity**" (emphasis added).

Cybersecurity is also mentioned under one of the strategies supporting the 2020 Plan's Theme 5 (Most Importantly, Achieving and Sustaining National Eminence through the Quality of Our People, Our Programs, and Our Facilities): "Coordinate capital planning and programming with systemwide goals and strategies for expanding access and degree attainment, particularly in critical economic and workforce areas (i.e., STEM, health care, education, **cybersecurity**). It is such coordination in programming which UMUC seeks to achieve with its proposed degree program.

State of Maryland: One of the primary objectives identified in the *2009 Maryland State Plan for Postsecondary Education*, expressed in Goal 1, is to "maintain and strengthen a system of postsecondary education institutions recognized nationally for academic excellence and effectiveness in fulfilling the educational needs of students and the economic and societal development needs of the state and the nation." A significant aspect of this plan is to expand the use of **distance education** and related technology to provide access to postsecondary education for adult or other non-traditional students and to students in underserved areas of the State.

Goal 2 of the *Maryland State Plan for Postsecondary Education* is to "achieve a system of postsecondary education that promotes accessibility and affordability for all Marylanders." The proposed degree program will enhance the options available via UMUC's virtual campus. Online programs are, by their nature, accessible to students anywhere, anytime, and are more affordable for students because there is no need to relocate to attend a specific campus or to expend funds on daily commutes to campus. Online students are also able to remain in their current jobs while pursuing advanced education, and thus continue to contribute to the economy while supporting their families.

Goal 4 of the *Maryland State Plan* speaks to the need to "Achieve a system of postsecondary education that promotes student-centered learning to meet the needs of all Marylanders." Under this goal, the plan specifically calls upon universities to ensure that academic programs address high-need employment areas, including **STEM fields** (science, technology, engineering and mathematics). Goal 5 of the *Maryland State Plan* also highlights the need to increase the supply of qualified graduates in identified high-demand fields and workforce shortage areas by adopting strategies tailored to specific occupations, especially the STEM fields. The UMUC proposal for creating an M.S. in Digital Forensics and Cyber Investigation is consistent with these expectations.

The proposed degree also supports the goals expressed in the *CyberMaryland* report issued in 2010 by the Maryland Department of Business and Economic Development, which envisions Maryland as the nation's "epicenter for cyber security." *CyberMaryland* highlights Maryland's pivotal role in supporting President Barack Obama's national cyber initiative and includes the first comprehensive inventory of any state's cybersecurity assets. The role of Maryland as a "cyber security nexus" builds upon its geographic proximity, alongside neighboring Virginia and the Washington D.C. area, to an expansive high technology corridor with strong ties to the federal government. This corridor is home to the cyber forensic programs of several federal

agencies, including the Department of Homeland Defense (DHS) and the United States Secret Service (USSS), along with other departments too numerous to mention. When considered as a group, these organizations have extensive computer forensics educational and training requirements for their workforces. Additionally, the corridor houses a substantial private industry sector with a cyber forensic presence, including Deloitte Touch, Northrop Grumman, and Booz Allen Hamilton.

National: Officials at the Department of Defense (DoD) Cyber Crime Center (DC3) have identified a pressing need on a national level for expert practitioners in digital forensics. The national authority in digital forensics, DC3 was founded to "to enhance through research, science, engineering, analysis, and planning current and future capabilities to conduct electronic forensic analysis, threat analysis, cyber investigations, and operations." (http://www.dc3.mil/).

To encourage institutions to develop high quality educational programs that will provide training in digital forensics, DC3 is sponsoring a new effort to establish National Centers of Digital Forensics Academic Excellence (CDFAE). Institutions can become CDFAEs after demonstrating a tangible commitment to providing high-quality digital forensics education. This program is similar to the Centers of Academic Excellence in Information Assurance (CAE), a program jointly sponsored by the National Security Agency and Department of Homeland Security. UMUC is already designated as a CAE, and it is a logical extension for UMUC to seek recognition as a CDFAE as a sign of UMUC's commitment to support the national need for expanded education in digital forensics. In the event that the proposed degree is approved, UMUC has been invited by DC3 to pre-load its programs for consideration of CDFAE certification.

Market Demand

The proposed M.S. in Digital Forensics and Cyber Investigation responds to current needs within the State of Maryland and beyond. This section provides a contextual background on both existing and emerging demands for graduates. It is generally accepted that the work place demands for skilled computer forensics will only expand in the future, leading to strong growth in, and – just as important – the sustainability of, the proposed program.

Evidence of employer demand comes primarily from three sources: 1) analysis of federal employment projections; 2) a sample of advertisements for positions requiring the skills provided by the proposed degree; and 3) anecdotal support for the demand of digital forensic professionals.

Employment projections on the national level were obtained from the *2009 Federal Occupational Outlook Handbook* (http://www.bls.gov) in the area of computer forensics, as shown in the table below.

Occupational title	Employment, 2011	Projected employment, 2016	Change, 2011-2016	
			Number	Percent
Computer forensics examiner	500,000	650,000	150,000	30%
NOTE: Data in this table are rounded. See the discussion of the employment projections table in the *Handbook* introductory chapter on *Occupational Information Included in the Handbook*				

Based on the table above, it is projected there will likely be a nationwide demand for more than 150,000 additional computer forensic specialists over the next five years, and the actual need may likely exceed this number. One of the challenges in estimating employment is that, apart from the title *Forensic Examiner*, there is no one title and job description that encompasses the field, and therefore potential job titles including *Computer Forensic Analyst*, *Computer Forensics Expert*, *Computer Auditor*, and even *Vulnerability Security Researcher* were used in this analysis.

A considerable number of positions are available in the local area at the present time. A sample of advertisements was obtained on February 15, 2012 by conducting an online job search using the *SimplyHired* utility (http://success.simplyhired.com/). The results included positions advertised by prominent firms in the greater D.C. area, including Booz Allen Hamilton, CACI, Cydecor, Harris Corporation, Inceptre, Kforce Technology, ManTech International, and Tasc; a sample of the open job titles include Computer Forensic Analyst, Senior Computer Forensics Analyst, Computer Forensic and Intrusion Analyst, Incident Responder/ Forensic Analyst, Cyber Forensics/Malware Analyst, and Senior Computer Forensic Engineer.

Anecdotal support for the demand for digital forensics specialists is available from many experts in the field. For example, according to Marcus Rogers, who heads the computer forensics program at Purdue University, "… graduate students in computer forensics are being recruited for law enforcement and private-industry jobs all over the country. They are getting multiple job offers, and the starting packages are growing each year. There is huge competition to hire anyone with expertise in this field." (http://www.newswise.com/p/articles/view/520054/)

The U.S. Department of Defense (DOD) reported on the need to protect networks from attackers and cyberspies. According to Regina Dugan, Director of the Defense Advanced Research Projects Agency (DARPA), "The potential capability for cyber mayhem makes cyber security 'one of the most intense challenges of our time.'...Malicious cyberattacks are not merely an existential threat to our bits and bytes. They are a real threat to an increasingly large number of systems that we interact with daily, from the power grid to our financial systems to our automobiles and our military systems."
(http://www.defense.gov/news/newsarticle.aspx?id=65988)

Army Gen. Keith Alexander, commander of U.S. Cyber Command and Director of the National Security Agency (NSA), added, "When you look at the vulnerabilities that we face in this area, it's extraordinary. What we see is a disturbing trend, from exploitation to disruption to destruction." The DOD wants to "create special 'hunter teams' to actively look for computer

viruses and malware" as part of "a 'dynamic' perimeter-defense network." (http://www.defense.gov/news/newsarticle.aspx?id=65988)

Moreover, as reported at the recent 2012 Department of Defense *DC3 Conference on Cyber Crime* the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), the Department of Defense (DoD), the Department of Homeland Security (DHS), the National Aeronautics and Space Administration (NASA), and the National Security Agency (NSA) are all in the market to recruit experts in digital forensics. (http://dc3.mil/dc3/dc3Conference.php)

The State of Maryland lays claim to of one of the highest technology workforce concentrations in the nation, with over 10 percent of jobs classified as technology-related, and led the nation in 2009 with the largest growth in computer systems design jobs (Maryland Department of Economic Development, *CyberMaryland*, January 2010). Maryland is also home to numerous federal facilities and major military installations, as well as many of the nation's top defense contractors. There is also a growing cluster of private sector organizations specializing in digital forensics. There already exists a pent up demand for trained digital forensic investigators.

Together these serve to substantiate strong, and increasing, demand for graduates of the proposed M.S. in Digital Forensics and Cyber Investigation as evidenced by the large number of federal, state, and local government agencies, situated in the greater Maryland and surrounding area, directly involved in the field of computer forensics, as well as private sector representation. The field of computer forensics is a thriving activity in the commercial sector, including Maryland state and local agencies, federal agencies and private sector organizations.

Student Audience and Potential Careers

The target audience for UMUC's proposed program consists of working adults and its fully online, asynchronous mode of delivery is designed to meet their needs. The program is anticipated to be especially attractive to many of UMUC's 50,000+ military students who may be pursuing their education under one of UMUC's contracts or Memoranda of Understanding with the Department of Defense, stateside or overseas. No previous technical education or work experience will be required for admission, making the program suitable for career-changers.

Similar to UMUC's existing Cybersecurity and Cybersecurity Policy master's degrees, the proposed M.S. in Digital Forensics and Cyber Investigation will prepare students for careers in industry, government, and academia by combining academic education with real world practical techniques. The program will emphasize educating students to use and apply computer forensics methods and knowledge in a variety of real life scenarios. Computer forensic specialists work in both the public and private sectors, and the Maryland/Virginia/Washington, D.C. corridor is home to a large potential work force including Computer Forensic Examiners (CFEs). CFEs work for the FBI, DEA, USSS, as well as with the vast majority of Inspectors General and local police departments. Practically all of the major accounting and consulting firms employ computer forensic examiners on staff, and there is a growing cadre of independent consultants that work in this field.

The American Society of Crime Lab Directors (ASCLAD), the governing association in the field of forensics sciences, requires that all computer forensic examiners possess a minimum of a bachelor's degree supplemented by hands-on forensics work. The FBI, for example, actively recruits computer forensics examiners, and then puts new recruits through an intensive, in-house training program. Each recruit is mentored through the training program consisting of at least five exams and five searches, and the average training program takes at least one year. Once through this program, the FBI assigns their recently trained CFEs to a senior partner so that additional, real-life, operational training can take place on actual cases. The reason the FBI, and other organizations, are willing to recruit at the bachelor level and then commit to expensive in-house training, is that there are currently very few academic programs that are designed to produce graduates in computer forensics candidates on which the FBI can draw upon for its recruits. The proposed degree program in Digital Forensics and Cyber Investigation will address this need by providing students with the necessary skills and knowledge to perform in a variety of computer forensic roles, including forensics examiner.

While technology is changing at such a rapid pace, the rules governing the application of digital forensics to the fields of auditing, homeland security, and law enforcement are evolving as well. Digital forensics can be defined as the process of extracting and analyzing information from computer systems that can be used to show the systems have been attacked or compromised. Evidence of unauthorized access, inappropriate use, data exfiltration can be proven and provided to law enforcement for prosecution. The challenge is finding this data, collecting it, preserving it, and presenting it in a manner admissible in a court of law. Electronic evidence is fragile and can easily be modified. Additionally, cyber thieves, criminals, and dishonest (and even honest) employees hide, wipe, disguise, cloak, encrypt and destroy evidence from storage media using a variety of sophisticated freeware, open source and commercially available utility programs.

The M.S. in Digital Forensics and Cyber Investigation will provide students with an opportunity to advance beyond the certification level to mastery of both theory and practice. Cyber security professionals who are looking to improve their understanding of theory and current practices in the areas of digital forensics and cyber security will be interested in this program. Employees at agencies that develop, host, secure and defend the government's information systems, such as the Defense Information Systems Agency (DISA), United States Cyber Command (USCYBERCOM), the Department of Defense (DoD) Cyber Crime Center, the National Security Agency (NSA), and the Defense Intelligence Agency, will benefit from these courses. UMUC's model of delivering the course content entirely online will provide the platform to ensure that educational needs are met.

Program Duplication

On the national level, Forensics Focus, an online repository of forensics articles and resources, lists only eleven master's degree programs related to digital forensics in the United States (see http://www.forensicfocus.com/computer-forensics-education-north-america). These include one program each in California, Florida, Maryland, New York, Rhode Island, Texas, and Vermont and two programs each in Pennsylvania and Virginia. The Maryland program listed by Forensics Focus is the Master of Science in Security Informatics at Johns Hopkins University.

Stevenson University has a proposed program in Cyber Forensics that is currently in the approval process. There are several institutions in Maryland offering master's programs that include only one course in digital forensics or even none but may be assigned a HEGIS or CIP code that includes the discipline of digital forensics, since this new field is not reflected specifically in the most recent code taxonomy. The analysis on the following pages compares UMUC's proposed program against those of Johns Hopkins, Stevenson and others across a range of factors including curriculum, admission requirements, mode of delivery, and intended student audience.

Institution	Degree Program	Curriculum	Mode of Delivery	Admission Requirements	Target Student Audience
UMUC	M.S. in Digital Forensics and Cyber Investigation (proposed)	18 semester hours of specialized courses in digital forensics combined with 12 sh of core courses in cybersecurity plus a 6 sh capstone course for a total of 36 sh	Entirely online, asynchronous learning environment	Bachelor's degree from a regionally accredited institution; any major; no minimum GPA; no prior work experience	Working adults, especially active-duty service members and affiliates under Department of Defense contracts and MOUs; no prior background or experience in technical fields necessary; suitable for career-changers.
Johns Hopkins University	M.S. in Security Informatics	Two computer forensics courses; JHU courses run in research seminar format and students will be given both basic and applied research projects in such areas as intrusion analysis, network forensics, memory forensics, mobile devices, and other emerging issues.	Traditional face-to-face	M.S. in Security Informatics is open to outstanding candidates who hold a Bachelors degree with sufficient technical exposure to information technology as preparation for the core technology courses.	Traditional full-time students with technical educational background and with research focus.
Johns Hopkins University	M.S. in Information Assurance	JHU courses run in research seminar format and students will be given both basic and applied research projects in such areas as intrusion analysis, network forensics, memory forensics, mobile devices, and other emerging issues.	Mix of online courses and traditional face-to-face	Requires a grade point average of at least 3.0 on a 4.0 (B or above) scale in the latter half of their studies or hold graduate degrees in relevant technical disciplines	Traditional full-time students with technical educational background and with research focus.

Institution	Degree Program	Curriculum	Mode of Delivery	Admission Requirements	Target Student Audience
SANS Technology Institute	M.S. in Information Security Engineering	Three courses; unlike UMUC's courses which are not vendor- or operating system-specific, SANS courses emphasize techniques and tools for forensics investigations in Windows and Linux operating systems.	Face-to-face, short intensive formats as well as online	Academic success at the undergraduate level, professional experience in the security field, leadership ability, and the ability to write well. Must be employed or have current access to an organizational environment that allows application of the concepts and hands-on technical skills learned in the Master's Program. Must have at least 12 months of professional work in information technology, security or audit; and must have earned a baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.8.	Working adult students with previous work experience in the field. **Note:** SANS is a candidate for regional accreditation through Middle States.
Stevenson University	M.S. in Forensic Studies, track in Computer Forensics	36 credits	Both online and face-to-face.	B.A. or B.S. in information technology, or substantial experience working in the information technology field.	Working adults and traditional students with prior education in technical fields as indicated by admission requirements, or with prior work experience.
Stevenson University	M.S. in Cyber Forensics (proposed program)	36 credits of cyber forensics courses; Stevenson's program appears to be more technically-oriented than UMUC's. Specifically, only six of Stevenson's 36 credit program are non-technical, whereas twelve credits of UMUC's program are non-technical.	Mixture of online and face-to-face classes	Must have a bachelor's degree in a related technical field such as information assurance, computer science, or computer security, plus two years or relevant experience, or at least five years of work experience in information technology.	Working adults and traditional students with prior education in technical fields as indicated by admission requirements, or with prior work experience. Students must be able to fit synchronous course activities into their schedules.
Towson University	M.S. in Forensic Science	33 credits of graduate course work in computer forensics are available.	Traditional face-to-face.	B.S./B.A. in biological sciences, chemistry or forensic chemistry required for full admission. Students with B.S. in natural science with general chemistry, organic chemistry, general physics, general biology, analytical chemistry, statistics, biochemistry, molecular biology and genetics can be considered for admission. A GPA of 3.00 in previous science course work and an overall GPA of 3.00 required for full admission. Students with GPA of 2.75-2.99 may be given conditional admission.	Working adults and traditional students with prior education in technical fields as indicated by admission requirements. Students must be able to fit synchronous course activities into their schedules.

In summary, UMUC's proposed degree would be the only program in Maryland designed in terms of curriculum, mode of delivery, and admission requirements to fully meet the needs of a target audience consisting of working adults, in particular active-duty service members and military affiliates with no prior technical background or education. Military students and other working adults require extreme flexibility in course scheduling, and UMUC's fully online, asynchronous delivery method is designed to fulfill this need. Further, UMUC's proposed curriculum combines 18 semester hours of specialized coursework with 12 semester hours of non-technical credits, and does not require any previous education or work experience in the field. No other program in Maryland combines all of these features.

Characteristics of the Proposed Program

Catalog Description of the Program

Technology is changing a rapid pace, and the rules governing the application of digital forensics to the fields of auditing, homeland security, and law enforcement are evolving as well. Digital forensics is the process of extracting and analyzing information from computer systems that can be used to show the systems have been attacked or compromised. Evidence of unauthorized access, inappropriate use, and data exfiltration can be proven and provided to law enforcement for prosecution. The challenge is finding this data, collecting it, preserving it, and presenting it in a manner admissible in a court of law. Electronic evidence is fragile and can easily be modified. Additionally, cyber thieves, criminals, and dishonest (and even honest) employees hide, wipe, disguise, cloak, encrypt and destroy evidence from storage media using a variety of sophisticated freeware, open source and commercially available utility programs.

The M.S. in Digital Forensics and Cyber Investigation is designed for midcareer professionals who wish to help meet the challenges posed in uncovering digital evidence. Using a multidisciplinary approach, the program is designed to provide students with a broad analytical framework for becoming a cyber investigator.

Expected student learning outcomes
Upon successful completion of the M.S. in Digital Forensics and Cyber Investigation, the graduate will be able to:

- Apply the basic procedures and technologies for conducting successful forensic examinations of digital media storage devices and computer networks;
- Design procedures at a suspected crime scene to ensure the digital evidence obtained is not corrupted;
- Conduct hands-on forensic searches to identify how digital media and/or digital networks were compromised, and the method(s) of intrusion employed;
- Employ the rigorous procedures necessary to have their forensic results stand up to scrutiny in a court of law;
- Understand the operation of the digital components they are handling (storage media, networks, etc.) so that all necessary forensic evidence can be extracted and validated;
- Successfully seize, image, deconstruct, and analyze digital media, analyze logs, decipher network traffic, and report this information in a suitable format;

- Present digital forensics results in a court of law as an expert witness ;
- Apply a strong ethical foundation to approach the application of the knowledge they have gained so that their results are above reproach;
- Learn advanced techniques and procedures that necessarily evolve in their field so that they remain current through life-long learning.

General requirements for degree

The M.S. in Digital Forensics and Cyber Investigation will consist of 36-semester of course work, consisting of six, 6-semester hour courses taken sequentially. Four of the courses are already offered as part of UMUC's existing degree programs in Cybersecurity; the remaining two courses will be new courses developed specifically for the proposed Digital Forensics degree.

Consistent with UMUC's focus on mid-career professionals, the program will be offered totally online and will be available to part-time students. The only admissions requirement is that the student must hold a bachelor's degree from a regionally-accredited university or college.

There is no thesis option for the degree. Students complete their program by taking the capstone course CSEC 670.

Degree Requirements: 36 semester hours

Core Courses		**12 sh**
CSEC 610	Cyberspace and Cybersecurity	6
CSEC 620	Human Aspects in Cybersecurity: Ethics, Legal Issues and Psychology	6
Digital Forensics Courses		**18 sh**
CSEC 650	Cyber Crime Investigation and Digital Forensics	6
CSEC 661	Digital Forensics Investigations*	6
CSEC 662	Cyber Incident Analysis and Response*	6
Capstone Course		**6 sh**
CSEC 670	Cybersecurity Capstone	6

* *New courses to be developed for this program.*

The program is designed to be completed in two years, with students taking one six-semester hour course each term (fall, spring, summer).

Course descriptions

Four of the six courses for the proposed M.S. in Digital Forensics and Cyber Investigation will be existing courses drawn from the current M.S. in Cybersecurity program. Two new courses will be developed (CSEC 661 and CSEC 662) specifically for this program.

CSEC 610 - Cyberspace and Cybersecurity (6 semester hours)

A study of the fundamentals of cyberspace and cybersecurity. Topics include cyber architecture, cyber services, protocols, algorithms, hardware components, software

components, programming languages, various cybersecurity mechanisms, business continuity planning, security management practices, security architecture, operations security, physical security, cyber terrorism, and national security.

CSEC 620 - Human Aspects in Cybersecurity: Ethics, Legal Issues and Psychology (6 semester hours)

Ethics, Legal Issues and Psychology: An examination of the human aspects in cybersecurity. Topics include ethics, relevant laws, regulations, policies, standards, psychology, and hacker culture. Emphasis is on the human element and the motivations for cyber crimes. Analysis covers techniques to prevent intrusions and attacks that threaten organizational data.

CSEC 650 - Cyber Crime Investigation and Digital Forensics (6 semester hours)

An in-depth study of the theory and practice of digital forensics. Topics include computer forensics, network forensics, cell phone forensics, and other types of digital forensics. Discussion also covers identification, collection, acquisition, authentication, preservation, examination, analysis, and presentation of evidence for prosecution purposes

CSEC 661 –Digital Forensics Investigations (6 semester hours)

A study of the processes and technologies used in the collection, preservation, and analysis of digital evidence in local, networked, and cloud environments. Discussion covers validating data, reporting evidence, and preparing depositions, as well as recovering information from encrypted, obscured, or deleted sources. Topics also include emerging forensic issues in computer, peripheral, and mobile environments and their global implications. (New course developed for this program).

CSEC 662 - Cyber Incident Analysis and Response (6 semester hours)

An examination of policies and procedures related to security incidents, exposures, and risks and technologies used to respond to such threats. Topics include dynamic vulnerability analysis, intrusion detection, attack response, evidence protection, and business continuity. Discussion also covers types and modes of computer-facilitated attacks, readiness, and evidence scope, as well as the role of computer emergency response teams. (New course developed for this program).

CSEC 670 - Cybersecurity Capstone (6 semester hours)

A study of and an exercise in developing, leading, and implementing effective enterprise- and national-level cybersecurity programs. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries (such as health, banking, finance, and manufacturing) are discussed. Topics include enterprise architecture, risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning. A project reflecting integration and application of learning of cybersecurity is included.

Expected Enrollment

Assuming the M.S. in Digital Forensics degree is approved for a fall 2012 start date, the following table shows projected student headcounts for the first five years of the program.

Academic Year	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
Estimated Student Headcount	15	33	48	73	118

The student population is expected to consist entirely of part-time students, each taking one six-credit course each term. Since degree completion will require two years of study, the first graduates will complete the program in 2014.

Impact on student's technology fluency

Technology fluency is a core learning area for UMUC students and is assessed at the institutional level as well as being incorporated into all degree programs. All UMUC graduate students are required to complete, within their first six credits of graduate study, the fully online course **UCSP 611 – Introduction to Graduate Library Research Skills**, which covers the appropriate use of online library and information resources. Students in the proposed Master of Science in Digital Forensics are required to complete the 6-semester hour course **CSEC 610 Cyberspace and Cyber Security**, which has a strong focus on the technologies used in cyberspace, including information and telecommunication technologies and their use and impact in the modern workplace. In addition, the online portions of the degree program will help students to acquire and maintain a very high level of technological proficiency.

Faculty Resources

The department that will administer the M.S. in Digital Forensics and Cyber Investigation includes several full-time faculty who will be available and are qualified to teach in the new program, including:

- Dr. Alan Carswell, Chair, Department of Cybersecurity and Information Assurance. Dr. Carswell holds a Ph.D. specializing in Information Systems from the Robert H. Smith School of Business, University of Maryland College Park.
- Dr. Patrick Fitzgibbons – Collegiate Professor, Cybersecurity. Dr. Fitzgibbons hold a Ph.D. with a specialization in information technology from SUNY Buffalo.
- Dr. Joon Son, Collegiate Assistant Professor, Cybersecurity. Dr. Son holds a Ph.D. in Computer Science from the University of Idaho.
- Dr. Ping Wang, Collegiate Professor and Program Director, Cybersecurity. Dr. Wang holds a Ph.D. in Information Systems from Nova Southeastern University.

In addition, UMUC currently employs over 100 adjunct faculty in the M.S. in Cybersecurity and M.S. in Information Technology (Information Assurance) programs, and many of these faculty are qualified to teach the digital forensics courses.

Library requirements
UMUC has an extensive online library with access to several full-text scholarly and professional databases. UMUC's own holding are enhanced by UMUC's participation in the University System of Maryland and Affiliated Institutions (USMAI) Consortium of Libraries. No new investment is required to support the M.S. in Digital Forensics and Cyber Investigation.

Facilities and equipment
UMUC already has a Virtual Cybersecurity Lab that supports its existing graduate cybersecurity program. It is expected that the lab will require an upgrade in terms of operating system software, hardware and infrastructure to accommodate additional students in the M.S. in Digital Forensics. It is also expected that UMUC will have to acquire specialized software to be used in digital forensics investigations to provide students with hands-on experience. UMUC has sufficient internal resources to support these needs, and these expenses are reflected in the financial tables included below.

Finance

UMUC will require no new general funds from the state to develop and launch the proposed program. Current staff and faculty resources are adequate for initial development of the program, and as demonstrated on the following pages, the program's enrollment growth is expected to support addition resources as they are needed.

TABLE 1: RESOURCES					
Resources Categories	**(Year 1)**	**(Year 2)**	**(Year 3)**	**(Year 4)**	**(Year 5)**
1. Reallocated Funds'	$255,595[1]	0	0	0	0
2. Tuition/Fee Revenue (c+g below)	124,920	285,912	432,000	683,280	1,149,792
a. #F.T. Students	0	0	0	0	0
b. Annual Tuition/Fee Rate	N/A	N/A	N/A	N/A	N/A
c. Annual Full Time Revenue (a x b)	N/A	N/A	N/A	N/A	N/A
d. # Part Time Students	15	33	48	73	118
e. Credit Hour Rate	$694	$722	$750	$780	$812
f. Annual Credit Hours per student per year	12	12	12	12	12
g. Total Part Time Revenue (d x e x f)	124,920	285,912	432,000	683,280	1,149,792
3. Grants, Contracts, & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 - 4)	**$380,515**	**$285,912**	**$432,000**	**$683,280**	**$1,149,792**

[1] Reallocated funds will be requested as a one-time allocation from the university's investment fund, which is designed to support the start-up of new programs. No other programs will be impacted by this reallocation. The reallocation is consistent with the institution's strategic plan in that the Cybersecurity degree programs have been identified as a high priority within UMUC's mission area.

TABLE 2: EXPENDITURES					
Expenditure Categories	**(Year 1)**	**(Year 2)**	**(Year 3)**	**(Year 4)**	**(Year 5)**
1. Total Faculty Expenses (b + c below)	3,888	7,776	7,776	11,664	19,440
a. # FTE	.2	.4	.4	.6	1.0
b. Total Salary (Adjunct faculty)	3,888	7,776	7,776	11,664	19,440
c. Total Benefits	N/A	N/A	N/A	N/A	N/A
2. Total Administrative Staff Expenses (b + c below)	63,250	64,831	132,903	136,227	139,632
a. # FTE	.50	.50	1.0	1.0	1.0
b. Total Salary	50,000	51,250	105,062	107,689	110,381
c. Total Benefits (26.5%)	13,250	13,581	27,841	28,538	29,251
3. Total Support Staff Expenses (b + c below)	18,975	19,423	39,871	61,302	62,835
a. # FTE	.25	.25	.50	.75	.75
b. Total Salary	15,000	15,375	31,519	48,460	49,672
c. Total Benefits (26.5%)	3,975	4,048	8,352	12,842	13,163
4. Equipment	250,000	0	0	0	0
5. Library (see Overhead)	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses (Course development, marketing, overhead)	44,402	45,497	93,298	106,666	109,332
TOTAL (Add 1 - 7)	**$380,515**	**$139,527**	**$273,848**	**$315,859**	**$331,239**