

Digital Forensics Certificate

Program Number: 90-504-1

Certificate

Protective Services Program Cluster

Center for Human and Protective Services

Program offered at West Campus

For information call: (608) 245-5882 or
(800) 322-6282 Ext. 5882

About the Program

The Digital Forensics Certificate is a certificate program for individuals interested in pursuing careers in digital forensics for law enforcement agencies or a private company. The certificate is designed for working law enforcement professionals and IT security personnel. This certificate will give the student a solid foundation in the area of digital forensics.

Digital Forensics is the application of forensic science techniques to the acquisition and analysis of evidence that exists in digital form (e.g. evidence found in files on hard drives, in emails, in network activity, etc).

In an age when computers hold the key to everything from terrorist plots to accounting scandals, nearly every crime can potentially leave digital evidence. They also serve as record-keepers of conversations, files and transactions. Computer forensic analysts work for a variety of organizations in pursuit of that digital evidence.

As a Computer & Digital Forensics student, you'll learn about the law, the digital investigative process, and computer and network technology. Develop the specialized skills to recover, preserve, and evaluate forensic evidence to support civil, criminal, and internal investigations. Focus on how to discover and document violations of computer usage in corporate and public agency settings. Learn the laws and procedures to successfully capture criminal use of the internet, email, and electronic files.

Unique Requirements for Completion

The certificate will be awarded upon completion of the requirements with a minimum of a 2.0 grade average and no course grade lower than a C. Students are responsible for contacting the Department upon completion of the required classes. Certificate will be awarded after completion of all requirements is verified.

Required Knowledge

Must have a good working knowledge of computers. This can be self taught or through training and education.

Curriculum

| Courses | Credits | Hrs/week | |
|---|-----------|----------|-----|
| | | Lec | Lab |
| 10-504-185 Introduction to Computer Forensics | 3 | 3 | 0 |
| 10-504-186 Introduction to Internet & Network Concepts..... | 3 | 3 | 0 |
| 10-504-189 Introduction to Video Evidence..... | 3 | 3 | 0 |
| 10-504-196 Ethics | 1 | 3 | 0 |
| 10-504-187 Legal Issues and Computer Forensics..... | 3 | 3 | 0 |
| 10-504-195 Small Devices..... | 3 | 3 | 0 |
| 10-504-188 Advanced Computer Forensics/Practicum..... | 3 | 3 | 0 |
| Total | 19 | | |

Application Requirements

- Cannot have any abuse of technology in their background
- Criminal history cannot have any convictions for computer crimes
- Must have a 2.0 GPA
- Must complete an application for certificate
- Final entrance into certificate is by department consent

How to Apply

- Call Garilyn Truttschel 608-245-5882 (Program Director) for application packet or email at gtruttschel@matcmadison.edu



Program Courses

10-504-185 Introduction to Computer Forensics 3 credits

Introductory computer forensics concepts, terminology and management of digital evidence. This course will cover the identification and collection and preservation of computer related and digital evidence, the acquisition of digital evidence, basic forensic analysis concepts and presentation of digital evidence to the investigator, the DA's office, to Judges and to Juries. The course will also cover the incorporation of digital evidence into the investigation and prosecution of criminal investigations. Overview of Forensic Toolkit & Ultimate ToolKit, Overview of EnCase, Overview of Paraben's Device Seizure, Overview of various cell phone applications, Overview of other available tools for forensically sound preview and acquisition (Helix, Knoppix, etc...) Overview of live acquisition tools. Overview of forensic hardware solutions – forensic computers, hardware writes blocking tools.

10-504-186 Introduction to Internet & Networking Concepts 3 credits

Internet related investigations, terminology and management of evidence gathered from online sources. Internet service provider overview. Hacking investigations, chat room, email, website, phishing online auction sites, Instant messaging, newsgroups and Bulletin boards, internet related fraud methods, BotNets, viruses, worms, etc... This course would include an overview of how various computer networks work, how to read log files, IP addressing schemes, IP telephony, overview of various file sharing networks commonly found in forensic investigations. Basic overview of network intrusion detection and response and reporting. Overview of Netanalysis, Kazaalyzer, and other standard forensic tools.

10-504-189 Introduction to Video Evidence 3 credits

Video is one of the most powerful tools to help law enforcement investigate and solve crimes. Video is one of the most prevalent forms of evidence collected in modern criminal investigations. This course is designed to introduce the student to various aspects of video evidence within the criminal justice system. Students will gain an overview of the various types of video evidence and their respective roles in criminal investigations. Basic, practical knowledge and experience will be gained in video evidence collection, image comparison, report writing and court testimony. Competency will be tested through quizzes, written tests and hands-on performance and moot court.

10-504-196 Ethics 1 credit

Examines the ethical issues related to person involved in the career choice of digital forensics.

10-504-187 Legal Issues and Digital Evidence 3 credits

4th Amendment, ECPA, HIPPA, FERPA, Search warrants (computer, online), Subpoenas, Preservation Letters & 2703, Patriot Act as it affects digital evidence, Dealing with ISPs, Wisconsin Statutes covering computer related crimes (Child Pornography, Use of Computer to facilitate child sex crime, child enticement, stalking, computer crimes statute) Federal Computer Crimes statutes. Corporate law and e-Discovery issues. Digital evidence in the courtroom – presentation of data retrieved from computers or online sources. Expert Testimony in the courtroom.

10-504-195 Small Devices 3 credits

Includes cell phones, smart phones, PDAs, and related storage devices, are a growing source of digital evidence in the forensics profession, and present unique challenges for forensic examiners. This course will introduce fundamental concepts in mobile communications, including an overview of cell phone technology and networks, sources of potential evidence, evidence handling considerations, and small device forensic processes, and documentation techniques. Students will have the opportunity to work hands on with small device forensic tools and technology.

10-504-188 Advanced Computer Forensics Concepts//Practicum 3 credits

Overview of advanced computer forensics topics such as encryption, password cracking tools, data hiding techniques, steganography, anti-forensic tools and their effect on investigations, forensic problem solving (reconstruction of web pages from web cache, reverse engineering of P2P networks, images, etc.) INFO2 (Recycle Bin) Files, In depth discussion of file carving & Windows artifacts, hidden partitions, thumbs.db files, advanced MAC (modified, accessed, created) time discussion, metadata. Microsoft Vista & Bitlocker, X Box Forensics, Digital Deception. This course will also cover an overview of how Cell Phone networks, Cell Phones, Personal Data Assistants, and other portable devices work. This course would be a culmination of skills from previous courses. Students would be expected to take a case study from beginning to end of investigation and court process. The students would receive a case study problem, and would have to write incident reports, collect evidence, acquire digital evidence, perform forensic examination of several types of digital evidence, write reports regarding the forensic exams, participate in trial prep, and courtroom testimony.

Career Potential:

- Digital Forensics Unit in a Law Enforcement Agency
- Enhance skills for a IT security professional

More detailed and updated information on this program may be available at: madisoncollege.org. The college reserves the right to make changes in the regulations and courses announced in this publication without notice.

Madison Area Technical College provides equal opportunity in education and employment.

Rev: 07/10