

Professional Track Master of Science in Digital Forensics (MSDF) FAQ

What is the MSDF?

The MSDF is a 30 hour master's degree composed of technical and non technical courses from forensic science, computer science, engineering technology, and related departments.

Whom should I contact if I have specific questions not answered in this FAQ?

Graduate application process:	Dr. Sheau Lang, slang@mail.ucf.edu . 407.823.2474.
Professional Track:	Dr. Philip Craiger, pcraiger@mail.ucf.edu . 407.823.3527.
Science/Academic Track:	Dr. Sheau Lang, slang@mail.ucf.edu . 407.823.2474.

What is digital forensics?

Forensics, or forensic science, is the application of science to questions that are of interest to the legal system. Digital forensics is the analysis of computers and other types of digital media to determine if they have been used for illegal or unauthorized activities, or if they are the “victims” of illegal attacks. Business and industry use digital forensics to gather internal information regarding intellectual property theft, fraud, network and computer intrusions, and unauthorized use of computers and other digital media including fax machines, answering machines, personal data assistants, cell phones, etc., to assist in employee termination, and both civil and criminal litigation.

Law enforcement agencies use digital forensics to gather digital evidence for a variety of crimes including child pornography, fraud, terrorism, extortion, cyberstalking, money laundering, forgery, and identity theft. The military and government intelligence agencies use digital forensics to gather intelligence information from computers captured during military actions.

Who is the target audience for the degree?

There are two audiences and a **track** for each. The **professional** track is for working professionals or students interested in working in industry, who are interested in a good technical hands-on education in digital forensics. The **academic** track is for individuals who are more interested in theory and research, and the academic aspects of digital forensics.

When did the program start?

Spring 2008

What are the mission and objectives of the MSDF?

The mission of the MSDF degree program is to provide a quality graduate education in science and practices of digital forensics, to prepare the students for digital forensics jobs, and to prepare the students for a lifetime of learning. The objectives of the program include the following:

- To give MSDF graduates the knowledge and skills necessary to participate as an effective team member or team leader in digital evidence investigations
- To prepare MSDF graduates for professional careers in digital forensics examination, forensic tool development, tool verification and validation, security and forensics administration
- To prepare MSDF graduates with the knowledge and skills to pursue advanced studies and research in computer technology or computer crime related disciplines
- To equip MSDF graduates with the communication skills, both oral and written, to become an effective problem solver as well as an effective communicator as an expert forensic examiner and expert witness

How do I know if I'm a good candidate for the degree?

Digital forensics is a technical specialty that requires good knowledge of computers, networks, and technology. Ideal candidates should have a good background in these topics, either through education, formal training, on-the-job training, etc. If you do not have this background and are still interested in the degree, we can identify several prerequisite courses that you must pass in order to demonstrate competency in computer technology.

I don't have a good background in computers. What courses can I take that will provide me with the necessary background?

We can recommend the following courses:

- CET 4505 Applied Operating Systems I
- CET 4333 Computer Organization and Design
- CET 3529 Linux/Unix Applications

Note that these courses have the following requirements:

- CET 2364 Systems Applications in C => CET 4505
- CET 3323 Digital Technology => CET 4333
- CET 2364 Systems Applications in C => CET 3529

Since two of the courses require programming course as a pre-req, that will likely be pretty simple to fulfill. The Computer Org class requires a Digital Tech class. In the worst case scenario the

students will need 5 classes to articulate without a solid background - but most will likely only need 4. These classes are offered by UCF, however, you could take similar classes at other institutions in order to gain the requisite knowledge and skills.

I heard that the degree is entirely online. Is this true?

Yes and no. **The professional track is entirely online.** The academic track is partially online, and will require some onsite attendance. (Read more below about the distinction between tracks).

What are the application requirements?

Students admitted to the program will be selected on a competitive basis and must meet the following minimum requirements: a bachelor's degree in a related discipline from an accredited institution, 3.0 GPA on the last 60 hours of attempted undergraduate coursework or a competitive GRE score, a personal statement (essay), and three letters of recommendation. Every applicant must submit a valid GRE subject test score; the minimum GRE scores for UCF graduate admissions are approximately 1000. Students are admitted to either the Professional Track or the Science/Computing Track. The two tracks share common core courses that lay the foundation of the discipline, and provide restricted electives and a thesis option to distinguish the intended audience and expected program outcomes.

For more information about the application process, contact Dr. Sheau Lang, slang@mail.ucf.edu.

I heard there are two tracks, what are they?

There is a **professional** and an **academic** track. The professional track is for working professionals or those who are interested in going into industry after graduating. The academic track is more research and theory-based. The professional track requires an internship to graduate. The academic track has a thesis and a no thesis option.

For more information about the professional track, contact Dr. Philip Craiger, pcraiger@mail.ucf.edu.

For more information about the academic track, contact Dr. Sheau Lang, slang@mail.ucf.edu.

Is the MSDF an accredited program?

At the present time, there is not an accreditation for any graduate digital forensics program. Professor Pollitt chaired the group which developed the proposed standards and was asked to participate in the further development of accreditation of digital evidence programs. Accreditation is a process that requires a degree program to produce several years worth of graduates and then complete a self-study documenting that the institution meets all of the requirements of accreditation. An on-site evaluation is then conducted, the results of which are presented to the accrediting body. If voted upon favorably, the

institution is then granted accreditation, which must then be periodically updated. It will likely be a couple of years before the first programs are accredited.

What is most important is that 1) the MSDF currently meets all of the proposed FEPAC accreditation guidelines and 2) we would seek accreditation as soon as we are eligible. UCF is recognized within the academic community as having a strong program that is standards-based. Accreditation will add to that in the future, but should not be an issue currently, as there is no existing accreditation in the field.

What courses comprise the MSDF professional track?

Here is a list of the core/required courses.

- CHS 5503 Topics in Forensic Science
- CGS 5131 Computer Forensics 1
- CGS 5132 Computer Forensics 2
- CHS 5518 Collection and Examination of Digital Evidence
- CIS 6395 Incident Response Technologies
- CIS 6986 OS & File System Forensics
- CET 6xxx Practice of Digital Forensics (capstone/project)
- CET 6946 Graduate Internship/Practicum (minimum three hours, maximum six hours)

An additional six hours of electives must be taken for a total of 30 hours. The student may propose any course that is related to digital forensics, the law, or criminal justice, or an additional three hours of internship. The courses must meet the graduate program committee's oversight.

What are potential electives?

For the Professional Track an additional six hours of electives must be taken for a total of 30 hours. The student may propose any course that is related to digital forensics, the law, or criminal justice, or an additional three hours of internship. The courses must meet the graduate program committee's oversight.

This is a list of **potential** electives

- CAP 6133, Advanced Topics in Computer Security and Computer Forensics
- CAP 6xxx, Wireless Security and Forensics
- COP 6xxx, Malware and Software Vulnerability Analysis
- COP 6xxx, Distributed Processing of Digital Evidence
- CCJ 6074, Investigative and Intelligence Analysis, Theory and Methods
- CCJ 6706, Quantitative Methods and Computer Utilization in Criminal Justice
- PLA 5587, Current Issues in Cyberlaw
- CHS 5596, The Forensic Expert in the Courtroom

- CHS 5518, Forensic Examination of Digital Evidence
- CJE 5688, Cybercrime and Criminal Justice

However, we strongly suggest that the student identify electives of interest to themselves. An elective is any course that is related to computer forensics, forensics, the law, technology, etc. Whether a course is suitable to serve as an elective will be made on a case by case basis.

What is the philosophy behind the professional track?

The philosophy of the Professional Track curriculum is to provide each student not only with technical expertise, but also with a well-rounded and practical education. In particular, we developed the Professional Track based on **industry-driven competencies**, derived from the Technical Working Group on Training and Education (described below), so that students graduate with the following:

- A solid technical computer foundation, including detailed knowledge of computers and networks;
- A solid digital forensics foundation, covering all aspects of digital forensics, including all procedures to be used in the identification, collection, and examination/analysis of digital evidence from a myriad of digital devices;
- A solid legal foundation so that the student understands the legal implications that may occur as a result of his/her actions;
- Numerous practical experiences to reduce the transition time from student to working professional.

The Professional Track includes no thesis option; instead, all students must complete a number of technical and practical assignments in each course in order to demonstrate the fundamental skills required to be a proficient digital forensics examiner, and additionally a (minimum) three-hour internship to demonstrate their competence.

These students will likely enroll part-time, while working in the field. They will likely continue in their current employment or seek a more challenging position after degree completion. UCF has a ready audience of these students who are enrolled in its graduate certificate program. All courses in the Professional Track will be fully online in order to provide these working students with flexibility in taking these courses.

Students in the Professional Track must complete 30 hours, 24 of which are for required courses. These students must complete an internship for graduation. Students must take an additional six hours to reach the 30-hour requirement. These final six hours may come from one of the elective sets below, or another course that is related to digital forensics, and must be acceptable to the graduate program committee.

From where did the Professional Track ‘core competencies’ come?

In 2003, the National Institute of Justice created a committee composed of academicians and industry practitioners from the various forensic sciences to develop a model curriculum. This curriculum was published as “Education and Training in Forensic Science: A Guide for Forensic Science Laboratories, Educational Institutions, and Students.” The curriculum was targeted at biological and physical sciences, as the core requirements are fairly homogenous. What was not included was digital forensics, for the primary reason that the subject matter and student outcomes are significantly different from those of the “traditional” forensic sciences.

As a consequence, in 2005 the National Institute of Justice created a similar committee – the Technical Working Group for Education and Training in Digital Forensics - to develop a model curriculum for associate, undergraduate, and graduate degrees in digital forensics. The model curriculum is expected to be completed in early 2007 and published as “Education and Training in Digital Forensics: A Guide for Forensic Science Laboratories, Educational Institutions, and Students.” Dr. Craiger was a core member of the Technical Working Group on Training and Education in Digital Forensics.

Below is a list of competencies allowing evidence to be entered into a court of law that our graduating students will exhibit, along with the courses that cover those competencies:

- 1. Identify and preserve a variety of digital devices:** Digital evidence can be found on many types of devices, including hard drives, cell phones, music players, embedded devices (e.g., black boxes in cars or aircraft), and game consoles. It is crucial that professionals understand not only where to look for evidence, but how to gather that evidence in a forensically sound manner.
- 2. Preserve and collect digital evidence in the field on a network:** Network intrusions may produce evidence located on disparate machines throughout the world, and in many different formats. Professionals should be able to understand where this evidence may reside, and how to gather it in a forensically sound manner.
- 3. Acquire, validate, and restore forensic images:** Professionals must be able to gather evidence, make copies of the evidence, and validate that the copies are exactly the same as the original evidence.
- 4. Develop and validate new forensic techniques and solve problems using the scientific method:** Professionals must be able to validate the tools they use to ensure that the results are as expected.
- 5. Identify, analyze, and solve both technical and investigative problems:** Professionals must understand the investigative process, and how non-digital sources of information may provide clues as to what types of evidence could be expected on the digital media.
- 6. Demonstrate an understanding of computer and network components and their interactions:** Professionals must understand the intricacies of the interplay between computers and networks, and how these interactions affect the types of evidence that may exist.

7. **Effectively communicate technical findings in both oral and written form:** Digital forensics is technical by nature, and a professional must be able to explain technical procedures and findings in a clear and accurate format.

8. **Demonstrate an understanding of expert testimony:** Professionals must be able to explain technical subject matter in a way that lay persons (jurors) can understand.

9. **Demonstrate understanding of current laws pertaining to computer crime:** Professionals must understand how and whether information found on a computer may be relevant to particular local, state and Federal laws.

10. **Demonstrate an understanding of forensic sciences:** Professionals must understand how the various forensic sciences affect each other. For instance, bloody fingerprints on a computer monitor should be gathered as evidence before any processing of the hard drive takes place.

11. **Demonstrate an understanding of ethics and professionalism:** Professionals should understand the importance of ethics and professionalism, as this has an effect not only on the individual's credibility, but also on the field as a whole.

What kinds of jobs/tasks would be related to someone with a degree in digital forensics?

A typical position for someone with a degree in digital forensics would be a *digital forensics examiner*. Such positions are available in law enforcement, business/industry, government, the military, and the intelligence community. Examiners are responsible for the identification, collection, and examination of digital media, written reports of their findings and presentation of these findings in court. For instance, an examiner working in law enforcement may be responsible for identifying and recovering from a computer or other digital media such items as fake driver's license graphics, pornographic images of children, or documents used for credit card fraud or identity theft. An examiner in industry may be responsible for identifying and recovering stolen intellectual property (e.g., patents) from a company's computer. An examiner in the military or intelligence services may be responsible for identifying and recovering documents and emails that contain plans for poisoning a major water system from computers seized from a terrorist organization.

In each of the scenarios described above, the examiner would begin by identifying all digital media at the suspect's home or place of work that have the potential to store evidence, including computer hard drives, cell phones, USB/thumb drives, CDs, floppies, digital cameras, game consoles, etc. Once identified, the examiner performs a forensically sound collection of the media, making sure not to change any facet of the evidence (such as time and date stamps or the actual contents). Evidence collection may occur at the scene by forensically copying the digital data, or at the examiner's laboratory if the media is seized.

Back at the digital forensic laboratory, the examiner would use special digital forensics hardware and software to examine the evidence. Common tasks for examiners include recovering deleted files and slack space; using digital fingerprints to identify files; searching for specific text or images on hard drives; searching for specific file names; identifying times and dates associated with files; recovering and interpreting computer log files; identifying mislabeled files; and correlating information from multiple sources (such as servers, routers, and wireless access points) to determine the source of a network intrusion.

An examiner often must improvise to solve a problem because a commercial software tool may not be available for the task at hand. In this case the examiner may need to develop a software tool using a computer scripting language in order to solve the problem. Alternatively, the examiner may download from the Internet a freeware or open source tool, which may then be used to solve the problem. It is crucial that the tools downloaded from the Internet be scientifically validated. (Validation is a systematic procedure to determine whether software does what its makers claim it does, and does not do anything that may adversely affect the integrity of the evidence.) Thus it is important that the examiner understand the correct scientific procedures for the verification and validation of software tools, whether those tools are commercial, freeware or open source, or tools the examiner created of his or her own volition.

In this example, the examiner might first recover any deleted files in case the suspect attempted to hide the fruits or tools of the crime; search the media for specific keywords contained in the file to determine if the classified file exists on the media; identify and recover any encrypted files, which the suspect may have used to hide crime-related data; decrypt any encrypted files found using special software; and create a digital fingerprint of any recovered files that are of probative value to the case. Finally, the examiner would write a technical report based on his or her findings that describes the technical procedures used, as well as a description of any potential evidence located.

Examiners often testify in court regarding the results of an examination. It is common for prosecutors and attorneys to ask the court to admit the examiner as an expert witness to the case. An examiner's status as an expert witness is determined by whether the examiner's education, training, and experience are commensurate with those of an expert in the field, and this status is at the discretion of the judge in the case. Expert testimony allows the expert to offer their opinions and this requires very specific skills to be performed correctly. Specifically, the ability to communicate very technical details to a non-technical jury is considered a prized skill, as is being able to use visual aids to explain technical details to a lay jury. These are skills not taught in any typical university course; thus there is a need for courses that cover these practical skills so that students are prepared once they graduate.

What is a typical schedule for a student?

A 'Typical' Program of Study Outline for the Professional Track:

- Fall Year 1 – Nine hours:
 - CHS 5503 Topics in Forensic Science (three hours)
 - CGS 5131 Computer Forensics 1 (three hours)
 - Elective (three hours typical)

- Spring Year 1 – Nine hours:
 - CHS 5518 Collection and Examination of Digital Evidence (three hours)
 - CGS 5132 Computer Forensics 2 (three hours)
 - CIS 6386 OS & File System Forensics (three hours)

- Fall Year 2 – Six hours
 - CIS 6395 Incident Response Technologies (three hours)
 - Elective (three hours typical)

- Spring Year 2 – Six hours
 - CET 6887 Practice of Digital Forensics (capstone/project) (three hours)
 - CET 6946 Internship (three hours)

- TOTAL: 30 hours

Who are the faculty teaching the courses?

Carrie Whitcomb, M.S.F.S, is the Director of the National Center for Forensic Science, a Fellow in the Academy of Forensic Sciences, and a leader in the field of digital forensics. Ms. Whitcomb is the former Director of the U.S. Postal Inspection Service Forensics Laboratory, in Washington, DC. Ms. Whitcomb served as founding Vice-Chair of the Scientific Working Group on Digital Evidence (SWGDE). She also served as a member of the International Organization on Computer Evidence (IOCE). Ms. Whitcomb is a Fellow in the American Academy of Forensic Sciences.

Dr. Philip Craiger has a dual appointment at UCF: He is the Assistant Director for Digital Evidence at the National Center for Forensic Science, and an Assistant Professor in the Department of Engineering Technology. He is also an Associate Member of the Academy of Forensic Sciences. Dr. Craiger is a member of the planning panel of the Technical Working Group for Education and Training in Digital Evidence (TWGDE), whose charge is to develop a nationally recognized curriculum at the associate's, bachelor's, and master's levels. He is also a member of the International Federation for Information Processing Working Group 11.9 Digital Forensics, a member of the Digital Forensics Working Group, and an Associate Member of the American Academy of Forensic Sciences.

Dr. Sheau-Dong Lang has been serving as the program coordinator for UCF's Graduate Certificate in Computer Forensics since its inception in the fall of 2001. Dr. Lang regularly teaches two UCF graduate courses in computer forensics, and does volunteer work with the computer crime squad at the Orange County Sheriff's Office.

FBI Special Agent (Retired) Mark Pollitt, M.S., is the former Director of the FBI's Computer Analysis and Response Team, former Director of the FBI's Regional Computer Forensic Laboratories (RCFL), and a Member of the Academy of Forensic Sciences. Mr. Pollitt has a dual appointment with NCFS and the Department of Engineering Technology as a Visiting Professor. Mr. Pollitt served as the Chairman of both the International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence (SWGDE). He currently serves as the Co-Chair of the Digital Forensic Educator's Working Group and is Vice-Chair of IFIP WG 11.9. Mr. Pollitt is a member of the American Academy of Forensic Sciences, and received the General Section Lifetime Achievement Award in 2006.

Required or Elective Courses for the Professional Track:

- CHS 5503 – Topics in Forensic Science. (3 credits) Topics in Forensic Science will include the history of forensic science, basic forensic science principles as applied in various forensic specialties, current issues in digital evidence, and professionalism.
- CGS 5131 – Computer Forensics 1. (3 credits) This course covers legal issues regarding seizure and chain of custody, technical issues in acquiring computer evidence, popular computer file systems, and reporting issues in the legal system.
- CGS 5132 – Computer Forensics 2. (3 credits) The purpose of this course is to teach the concepts of computer system security models, fundamentals of computer networking and the layered protocol architectures, detection and prevention of intrusion and attack, digital evidence collection and evaluation, and the legal issues involved in computer forensic analysis.
- CET 6386 – Operating System and File Systems Forensics (new course). (3 credits) The course will provide students with a practical understanding of the fundamental procedures required to correctly conduct digital forensics on Windows, Linux, and Macintosh operating systems, file systems, and associated applications.
- CET 6887 – Practice of Digital Forensics. (3 credits) This is a capstone course that allows students to demonstrate the ability to combine all they have learned. Students will work on several case studies that require them to apply the knowledge and skills they have acquired to practical assignments.
- CET 6946 Graduate Internship or Practicum. (minimum 3 credit hours) Inclusion of an internship underscores the importance of students' applying the knowledge and skills learned during their studies in the real world. Three credit hours are required.
- PLA 5587 Current Issues in Cyberlaw. (3 credits) Advanced examination and discussion of free speech, copyright, trademark, patent and privacy issues in the online environment through interactive class discussions, online discussions, postings, case study reviews, and legal research projects.
- CJE 5688 Cybercrime and Criminal Justice. (3 credits) Deals with the problem of cybercrime and the criminal use of the Internet. Includes investigation, enforcement and legal issues.
- CHS 5518: Collection/Examination DE. (3 credits) This course will cover the nature of digital evidence collection and examination under the constraints of law and courtroom procedures.

- CHS 5596 The Forensic Expert in the Courtroom. (3 credits) A study of the uses of technically- and scientifically-trained expert witnesses at trial.
- CET 6395 Incident Response Technologies (new course). (3 credits) An advanced course covering topics related to computer incidents and intrusion response.
- CAP 6133 Advanced Topics in Computer Security and Computer Forensics. (3 credits) Advanced topics in computer security and forensics such as cryptography, automatic intrusion detection, pattern matching and statistical techniques, firewalls, and vulnerability scanning.

Can I get financial aid?

Financial aid is handled by the UCF financial aid office. <http://finaid.ucf.edu/>

How much do graduate courses cost?

The most up-to-date costs can be found here:

http://www.iroffice.ucf.edu/character/current_tuition.html

Can I take the capstone course prior to my last year?

NO. The capstone course draws upon what you have learned in all core courses. Consequently you must complete all required courses prior to taking the capstone course.

When can I take the internship?

Typically not before you have completed the 15 hours of your first year courses (see 'Typical Program of Study' above).

What do I need to do to sign up for an internship?

Your first need to create a statement of work that describes your proposed internship, what you intend to do, how it relates to digital forensics, and your sponsor. This document should be approximately 1 page in length (give or take). Send that to Dr. Craiger for approval. Note that this document serves as a CONTRACT between you and the College. You will receive either a Satisfactory or Unsatisfactory for your internship based upon the completion of your duties as specified in your statement of work.

If your statement of work is approved, you'll need to download and complete the graduate internship form here.

<http://www.cecs.ucf.edu/acadaffairs/forms.htm>

From this link download the file: Graduate Special Registration Access Agreement. Complete the form as directed, using the class number: CET 6946. Once completed you can either mail or fax the completed document to Dr. Craiger (Fax: 407-823-3162). He will sign the form and send to the CECS Office of Academic Affairs. They will put your information into their system, and after a few days you will be able to enroll in your internship.

Are there any special circumstances for graduates of the GCCF program? (answer from Dr. Lang)

Yes. It is a UCF Graduate Studies Office rule that requires at least half of the course work be at 6000 level. Thus, you will need to file a petition (appeal) to the Graduate Studies office for exemption of this rule if you only take 12 hours at 6000 level out of a total of 30 hours.

Can I start take classes BEFORE I'm accepted to the program?

A student can take up to 9 hours prior to any graduate program and still be assured that the hours will transfer. To do this they have to gain admission to a certificate program (to be able to enroll) or be an existing admitted undergraduate student (but can only take 5000 level courses). So if the student meets any of those requirements they are free to take the courses.

Students should realize that taking the courses does not guarantee them admission into the program.

Do I have to take the GRE?

Starting Spring of 2009, students that have 3.0 GPAs will not need the GRE in order for regular admission. If a student does not have a 3.0, then they will need to take the exam and score at least a 1000 on the math and verbal sections.

I don't have a Bachelor's Degree. Can I still get into the MSDF program?

A Bachelor's degree from an accredited university is a requirement for admission. This is a university requirement.

I've completed the Graduate Certificate program. Will my hours transfer to the MSDF?

Last updated: Thursday, February 12, 2009 by Dr. Philip Craiger

Yes, they will transfer. You are 1/2 to completion of the MSDF.

I've completed the Graduate Certificate program. Am I guaranteed acceptance into the MSDF program?

Not necessarily. You must still complete the application for the degree and meet all requirements.

Can I use my current job as my internship?

That depends. The internship must be largely digital forensics-related. This will be handled on a case-by-case basis, and will be reviewed by the Professional Track faculty committee.

Can I get help finding an internship?

Yes. We are constantly on the lookout for internship opportunities. Check with Dr. Craiger for more information.