MASTER OF SCIENCE IN DIGITAL FORENSICS

The Master of Science in Digital Forensics is a thirty hour program that prepares students for service in a variety of public and commercial arenas such as digital forensics or as network security professionals. In particular, graduates from the Digital Forensics program will be able to effectively plan, establish, and administer security and information assurance systems in commercial settings and law enforcement. This program utilizes state-of-the-art facilities, like Sam Houston State University's Cyber Forensics Intelligence Center. The facility includes a Network Security Lab, accommodating training in data, network and cyber security intrusion detection, prevention and tracing, and a Data Recovery Lab that will provide training in the identification, recovery, and preservation of data for legal purposes.

Applicants seeking admission to the Master of Science in Digital Forensics must submit the following directly to the Office of Graduate Admissions (https://www.shsu.edu/dept/graduate-admissions/prospective-students.html):

1. Graduate Application (http://www.shsu.edu/admissions/apply-texas.html)
2. Application fee (http://www.shsu.edu/dept/graduate-studies/application-fee.html)
3. Official transcript(s) of all previous college work
4. Up-to-date Resume
5. Official GRE scores
6. Two letters of recommendation that address the applicant's qualification for graduate study

GRE Waiver Requests - In order to obtain the Waiver of the GRE Score Requirement, applicants must have either

1. An awarded M.S. degree from an accredited institution of higher education or,
2. 5+ years full time relevant work experience beyond B.S. degree.

This degree is accessible to students who have completed undergraduate Computer Science or Criminal Justice majors or minors and to those with baccalaureate degrees in technical fields with the equivalent of a Computer Science or Criminal Justice minor in formal coursework or professional experience. Applicants who do not possess the appropriate academic, technical, or experiential backgrounds may be required to take stem work courses. In addition, admission preference is given to applicants with a GPA of 3.0 or greater.

The degree requires a minimum of thirty hours of graduate credit. Students will be required to complete a written comprehensive examination in core subjects where they received a grade of B or lower, before graduation. Students may also be required to supplement their written responses in an oral examination. Students must be enrolled the semester in which they take comprehensive examinations.

The department chair assigns a committee advisor to each student at the time the student registers for DFSC 6347. The advisory committee consists of graduate faculty from the Department of Computer Science. Once enrolled in DFSC 6347, a student must be continually enrolled in each major semester until graduation.

Code	Title	Hours
Master of Science in Digital Forensics		
Specified Courses		
DFSC 5315	Network and Cyber Security	3
DFSC 5316	File System Forensics	3
DFSC 5317	Digital Security	3
DFSC 5318	Cyber Law	3
DFSC 5327	Digital Forensics Investigatn	3
DFSC 6347	Directed Mgt & Development Prj [1]	3
Electives		
Select four graduate courses in DFSC or any approved COSC graduate courses [2]		12
Total Hours		**30**

[1] Once enrolled in DFSC 6347, the student must enroll in this course until graduation.

[2] COSC 5301 and COSC 5302 do not count towards the degree plan.

The Texas Higher Education Coordinating Board (THECB) marketable skills initiative is part of the state's **60x30TX plan** and was designed to help students articulate their skills to employers. Marketable skills are those skills valued by employers and/or graduate programs that can be applied in a variety of work or education settings and may include interpersonal, cognitive, and applied skill areas.

The MS in Digital Forensics is designed to provide graduates with the following marketable skills:

- Establish & operate an investigator's lab and process digital evidence.
- Develop plans to safeguard digital files against unauthorized modification and destruction.
- Create plans and implement strategies for preventing attacks to a network.
- Acquire a strong academic foundation in Cyber Security needed to pursue Doctoral level programs.