DEPARTMENT OF COMPUTER SCIENCE

About

Chair
Peter A. Cooper (cooper@shsu.edu)

Website: Department of Computer Science (http://cs.shsu.edu)

Mission

The Department of Computer Science is a community of faculty, staff, and students centered in the computer science disciplines. The Department of Computer Science is dedicated to providing the highest quality education possible to its graduate and undergraduate students through excellence in teaching and excellence in research. The department is committed to furthering the pursuit of knowledge and meeting the needs of a diverse society.

The Department of Computer Science seeks to provide an environment that encourages innovative thinking, academic rigor, and the pursuit of scholarship in an atmosphere that promotes high ethical and moral values and mutual respect, embracing diversity and working towards a goal of instilling a life-long love of learning.

Contact Information
(936) 294-3846

Websites
Computer Science (http://cs.shsu.edu)
Digital Forensics (http://df.shsu.edu)

Highlights

Sam Houston State University provides a comprehensive computing environment for students. The Computer Services Department operates a large number of computing laboratories containing desktop computers and workstations. A variety of operating systems, network protocols, programming languages and application packages are available. Students have full access to the Internet and E-mail facilities when on campus and through dial-up facilities from off-campus. In addition to the institutional facilities, the Department of Computer Science operates a range of lab facilities to support its mission and programs, including network robotics and Unix labs, a data recovery lab, and a network security lab. The department operates a 40-node symmetric multiprocessing system for use in parallel processing, digital forensics, cryptanalysis, and steganographic research. The department also has access to state of the art visualization facilities. As part of its operations, the Department of Computer Science houses the Sam Houston State University Center of Excellence in Digital Forensics, a center dedicated to the development of digital forensics training for law enforcement personnel and research opportunities into forensics and security issues.

Career Opportunities

Computing professionals support many scientific, governmental, and commercial enterprises though network and communication systems management, application (computer program) development and maintenance, and hardware design. The management of computing resources within organizations is typically a mission critical activity and computing professionals occupy key organizational roles as network and database administrators, software engineers, systems analysts and programmers. Of key concern in today's modern environment is the protection, assurance, and recovery of computing resources, providing opportunities for those wanting to work in the information assurance and digital forensics fields.

- Ph.D. in Digital and Cyber Forensic Science (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/digital-and-cyber-forensic-science-phd/#curriculumtext)
- Master of Science in Computing and Information Science (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/computing-information-science-ms)
- Master of Science in Digital Forensics (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/digital-forensics-ms)
- Master of Science in Information Assurance and Security (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/information-assurance-security-ms)
- Graduate Certificate in Cyber Security (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/cyber-security-certificate)
- Graduate Certificate in Data Assurance (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/data-assurance-certificate)
- Graduate Certificate in Digital Investigation (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/digital-investigation-certificate)
- Graduate Certificate in Educational Technology (catalog.shsu.edu/archives/2017-2018/graduate/college-departments/science-and-engineering-technology/computer-science/educational-technology-certificate)

Student Organizations and Activities

Sam Houston Association of Computer Scientists - The club sponsors field trips, campus visits by guest speakers, and occasional student/faculty outings.

Internships

The Computer Science department does not operate internships as part of its degree programs.

Scholarships

The Department of Computer Science offers the following scholarship:

- The Kailas and Becky Rao Scholarship in honor of Mr. Albert Kidd: awarded to full time graduate or undergraduate students in good standing and majoring in Computer Science.

This scholarship requires a minimum GPA of 3.0 and registration in courses leading to a degree in Computer Science. Other criteria are also pertinent to individual scholarships. More information can be obtained through the department.

Computer Science

COSC 5301. Quantitative Foundations of CS. 3 Hours.
This course provides the fundamental quantitative methods needed in the area of computer science (CS). Topics include numbering systems, propositional logic, digital logic, combinatorics, probability and statistics, and automata theory, focusing on their application to computing and information science. This course serves graduate students without an undergraduate degree in a quantitative field by providing necessary stem work. This coure may not be counted toward the requirements for a graduate degree in Computer Information Science, Digital Forensics, or Information Assurance and Security.
Prerequisite: Approval by the graduate advisor.

COSC 5302. Computer Science Core Topics. 3 Hours.
This course provides a solid foundation of Computer Science core concepts, fundamental principles, generalizations, and theories essential to pursuing the CS graduate program. Topics include computer programming, database systems, and computer networks. This course provides stem work for those graduate students whose undergraduate degrees are not in CS and thus have little exposure to core CS topics. This course may not be counted toward the requirements for a graduate degree in Computer Information Science, Digital Forensics, or Information Assurance and Security.
Prerequisite: Approval by the graduate advisor.

COSC 5310. Cryptography & Steganography. 3 Hours.
This course is designed to cover the theoretical and practical aspects of cryptography and steganography including specification, design, and programming. Topics include digital signatures, symmetric and asymmetric (public key) algorithms, hash functions, cryptographic algorithms, cost to break algorithms including key safety, Diffie-Hellmann, RSA, key stores, Secure Socket Layers, Virtual Private Networks (VPN), Certificate Authorities, and important cryptanalysis and steganalysis strategies.

COSC 5313. Artificial Intelligence. 3 Hours.
A survey of topics in artificial intelligence. Topics include: history of AI, knowledge representation, knowledge acquisition, search techniques, control strategies, and AI languages. Applications include natural language processing, neural nets, and expert systems.

COSC 5318. Database Systems. 3 Hours.
A survey of contemporary topics in database systems. Topics include: relational database theory, database design issues, cryptography, security integrity issues, data recovery, concurrency problems, optimization, distributed database systems, the client/server model, object-oriented databases, stenography, data compression, data warehouse, data mining, logic/knowledge based systems, and other related topics.

COSC 5319. Algorithm Design and Analysis. 3 Hours.
A number of important concepts and algorithms, with emphasis on correctness and efficiency, are reviewed. The advanced treatment of sorting, searching, hashing, and dynamic storage management is provided. Advanced data structures, such as advanced tree structures, graphs, and networks, are introduced. Applications to distributed file structures, database management systems, internet/intranetworks are covered.

COSC 5320. Comp Architecture & Organizatn. 3 Hours.
An introduction into Computer Architecture and Organization. Topics include computer evolution and performance issues, the computer systems including system buses, internal and external memory, input/output, and operating system support, CPU issues including computer arithmetic, instruction sets, addressing modes, RISC and superscalar organization, control unit issues, microprogramming, and parallel organization.

COSC 5321. Parallel Computing. 3 Hours.
This course is a study of large-scale parallel processing systems. The central themes are theoretical models, machine architecture, computer algorithms, and programming languages that model, support, describe and implement parallel processing.
Prerequisite: COSC 5319.

COSC 5322. Real-Time and Embedded Systems. 3 Hours.
This course emphasizes real-time and fault-tolerant computing systems. Topics include interrupt processing, real-time programming and scheduling, fault-tolerant architectures and systems, and robotic programming. Extensive programming will be done.

COSC 5325. Operating System Security. 3 Hours.
This course will provide the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. The course will cover methodologies for the design of operating system security and forensic techniques for operating systems. Also covered will be the identification of best practices in the administration, testing and security for operating systems.

COSC 5326. Networks & Data Communications. 3 Hours.
An introduction to the basic techniques for interconnecting computers and peripherals for decentralized Computer. Network components, digital communications, interconnection architectures, communications protocols for geographic and local area networks and interprocess communications are covered.

COSC 5327. Operating Systems. 3 Hours.
A comprehensive study of computer operating systems. Topics include: computer architecture, concurrent processes, multi-threaded systems, scheduling, memory management, I/O management, file systems, networking and the client/server model, distributed systems, and computer security.

COSC 5330. Malware. 3 Hours.

COSC 5332. Computer Graphics. 3 Hours.
A study of modern Computer Graphics programming techniques. Topics include: representations, transformations, and analysis of 2-dimensional and 3-dimensional objects; techniques for hidden surface/edge removal, illumination and shading, volume rendering, animation, and image data compression; and practical experience in graphics software libraries and applications.

COSC 5335. Database Security. 3 Hours.
Database security has an immense impact on the design of today?s electronic information systems. This course will provide an overview of database security concepts and techniques and discuss new directions of database security in the context of a connected commercial world. This course provides the information needed to develop, deploy and maintain a secure database solution. It exposes the pitfalls of database design, their means of identification and the methods of exploiting vulnerabilities.

COSC 5340. Special Topics. 3 Hours.
Topics and courses are selected to suit individual needs of students. The course may be repeated for additional credit.
Prerequisite: Approval by the graduate advisor.

COSC 6049. Thesis. 1-3 Hours.

COSC 6312. Multimedia Forensics. 3 Hours.
This course examines the theory and practice of multimedia security and forensics. Topics include image processing, JPEG compression, audio compression (MP3, Advanced Audio Coding, and VOIP), MPEG compression, multimedia source identification, biometrics, steganography, steganalysis, multimedia forgery detection, and pattern recognition techniques for multimedia analysis, multimedia forensics software, and advances in multimedia forensics.
Prerequisite: Approval by the graduate advisor.

COSC 6313. Neural Networks. 3 Hours.
An introduction into Neural Networks. Topics include discussion of variety of standard neural networks, with architecture, training algorithm, and applications; and development of neural network expert systems.

COSC 6314. Data Mining/Knowldge Discovery. 3 Hours.
An introduction into Data Mining and Knowledge Discovery. Topics include discussion of variety of mining techniques. Mining of complex data such as multimedia database, text database, and world-wide-web will be introduced. The applications and trends in data mining will also be discussed.
Prerequisite: COSC 5318.

COSC 6315. Machine Learning. 3 Hours.
This course provides the principles, design, and implementation of a broad range of machine learning algorithms. Topics include computational learning theory, machine learning algorithms, and algorithm assessment techniques. Both a computational aspect (how to compute the answer) and a statistical aspect (how to ensure that future predictions are accurate) of each machine learning algorithm are discussed.
Prerequisite: COSC 5319.

COSC 6318. Language and Compiler Design. 3 Hours.
A comprehensive study of computer programming languages. Topics include: language design principles, formal grammars, procedural operating environment, language standardization, and language support for parallel and distributed programming. Language paradigms to be discussed will include procedural programming, logical programming, functional programming, and object-oriented programming.

COSC 6319. Software Engineering. 3 Hours.
This course emphasizes strategies, techniques, and methodologies that deal with the complexity in developing large-scale information systems. Methods for Software engineering methodologies, conventional as well as object-oriented, are discussed. Software measurement and management are discussed. Formal mechanisms for system specification, software development, and project management are introduced.
Prerequisite: Approval by the graduate advisor.

COSC 6347. Programming Practicum. 3 Hours.
The practicum provides the student an opportunity to develop their programming and analytical skills by applying concepts and techniques learned in organized classes to real world projects under the supervision of faculty and/or supervisory Computer professionals. Prerequisite: Eighteen hours of Computer and Information Science graduate level coursework. Student must register for this course every semester the practicum is in progress but only three hours of practicum will apply to the student?s degree plan.
Prerequisite: Student must register for this course every semester the practicum is in progress but only three hours of practicum will apply to the student's degree plan.

COSC 6348. Thesis. 3 Hours.
.

Computer Science Technology

CSTE 5319. Critical Anlysis-Instruc Sftwr. 3 Hours.
This course examines the instructional and educational value of commercially available software for the pre-k through 12th grade. The course builds upon a foundation of instructional theory to identify appropriate characteristics of instructional software and explores the effectiveness of instructional software in the classroom. This course may not be counted toward the M.S. in Computer and Information Science, Information Assurance and Security or Digital Forensics.

CSTE 5336. Educational Multimedia. 3 Hours.
This course explores the uses of multimedia in the classroom and extends the teachers skill base in the development of appropriate multimedia examples to support and enhance the middle school and high school curricula. Throughout the course students will gain experience in still and motion digital editing, audio and animation production. This course may not be counted toward the M.S. in Computer and Information Science, Information Assurance and Security or Digital Forensics.
Prerequisite: CSTE 5319 and Graduate standing.

CSTE 5337. Desgn Instrctnl Mat For Web. 3 Hours.
This course examines the development of web sites for instructional purposes. The course looks at the systematic design of instruction, a process that examines the development of appropriate course goals, the identification of measurable objectives that meet those goals and intelligent approaches to assessing student performance. This design approach is then applied to the development of web-based materials, providing opportunities for skills acquisition in a variety of multimedia applications and their incorporation into a web site. The course culminates in the development of a geometry web site for use in schools. This course may not be counted toward the M.S. in Computer and Information Science, Information Assurance and Security or Digital Forensics.
Prerequisite: CSTE 5336.

CSTE 5338. Dev Of Tech Infrastructre-Schl. 3 Hours.
Prerequisite: CSTE 5337.

CSTE 7315. Educational Network Design. 3 Hours.
This course examines the technical, environmental, and policy issues involved in the development of educational technology infrastructures, focusing on network design and evaluation.

CSTE 7325. Technology Sustainability. 3 Hours.
This course will examine the potential and the challenges associated with initiating and maintaining green and cost-efficient technology infrastructures based on environmental awareness initiatives.

CSTE 7335. Mgmt Application Analysis. 3 Hours.
This course provides a systematic and rational approach to the analysis, evaluation, and implementation of course management systems from the standpoints of pedagogical success, user friendliness, and cost effectiveness.

CSTE 7336. Instructional Design Assmt. 3 Hours.
This course applies instructional design theory to the development, analysis, evaluation, and assessment of various digital instructional designs.

CSTE 7380. Inst Tech Research Methods. 3 Hours.
This course focuses on the research questions, approaches, and measures typically employed by instructional technology researchers.

Digital Forensics

DFSC 5310. Princple& Policy-Info Assuranc. 3 Hours.
An investigation into the development of security planning and policy formation, risk management, security education, training and awareness programs. This course examines physical and electronic approaches to data protection and derives appropriate assessment strategies for determining the assurance quality of target systems.

DFSC 5315. Network and Cyber Security. 3 Hours.
This course provides the framework and procedures for securing computer systems and data networks. Topics include the methodologies for the design of security systems, establishing security protocols, and the identification of best practices in administration, testing, and response protocols for secure communications systems.

DFSC 5316. File System Forensics. 3 Hours.
This course focuses on the important concepts associated with the structures, encoding, boot process and storage technologies of modern computers, and the implications of those concepts regarding the analysis of volumes and file systems for forensics purposes.

DFSC 5317. Digital Security. 3 Hours.
This course introduces the student to basic security needs. The course will include, but not be limited to examination of individual vs. government privacy issues, federal encryption standards, the different layers of security currently available, cryptography, and strategies for evaluation and selection of security methods.

DFSC 5318. Cyber Law. 3 Hours.
The focus will be on how the law impacts digital security in diverse ways. Discussion will emphasize the concept of criminal intent, the digital victim and address jurisdictional issues and provide an overview of legal terms and issues with which the security manager must address.

DFSC 5325. Organization System Security. 3 Hours.
This course provides advanced study of system security concepts as applied to the protection of organizational systems including (1) principles of security modeling, accountability and access control, (2) the ISO model for network infrastructure design and protection, (3) communication security and control management, (4) auditing and monitoring, (5) incident management, and(6) law, investigations and ethics.
Prerequisite: DFSC 5310.

DFSC 5327. Digital Forensics Investigatn. 3 Hours.
This course explores tools for the recovery of information on hardware or hidden within other formats. Topics also include cryptographic analysis, password recovery, the bypassing of specific target operating systems, and obtaining data from a digital device that has been destroyed.

DFSC 5328. Software Forensic Evidence Mgt. 3 Hours.
Analysis of investigative techniques and tools in the detection, investigation and analysis of digital crimes. This course examines the nature of cyberevidence and the tracking and identification of cybercriminals.

DFSC 5336. Business Continuity Management. 3 Hours.
This course examines identification and assessment of threat, risk, vulnerability and business continuity in case of disaster, as applied to enterprise IT systems. It incorporates the physical safeguards and policies necessary to meet the requirements for the protection of data in a fixed site. This course also discusses techniques and strategies designed to keep enterprise data in service under critical circumstances.

DFSC 5340. Spcl Tpcs In Digital Forensics. 3 Hours.
Topics and courses are selected to suit individual needs of students. The course may be repeated for additional credit.
Prerequisite: Approval by the graduate advisor.

DFSC 6310. Cyber Warfare & Terrorism. 3 Hours.
This course will focus on philosophies, tactics, and targets of cyber terrorist organizations. The course includes discussion of emerging cyber war trends and the roles of the private sector and U.S. Government in responding to, mitigating and preventing electronic offensive actions.

DFSC 6312. Multimedia Forensics. 3 Hours.
This course examines the theory and practice of multimedia security and forensics. Topics include image processing, JPEG compression, audio compression (MP3, Advanced Audio Coding, and VOIP), MPEG compression, multimedia source identification, biometrics, steganography, steganalysis, multimedia forgery detection, and pattern recognition techniques for multimedia analysis, multimedia forensics software, and advances in multimedia forensics.

DFSC 6313. Wireless Network Security. 3 Hours.
This course provides advanced study of the full range of algorithms, mechanisms, and technologies in securing various types of wireless communication networks, such as cellular networks, Wireless Local Area Networks, Bluetooth Networks, Mobile Ad Hoc Networks, and Wireless Sensor Networks. Research and applications will be explored.

DFSC 6347. Directed Mgt & Development Prj. 3 Hours.
This course will provide the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. The course will cover methodologies for the design of operating system security and forensic techniques for operating systems. Also covered will be the identification of best practices in the administration, testing and security for operating systems. Continuous enrollment in DFSC 6347 is required until graduation.
Prerequisite: 24 hours graduate coursework.

DFSC 6410. Cyber Forensics Principles. 4 Hours.
This course explores the skill set and conceptual understanding required by digital and cyber forensic scientists and researchers operating in a heterogeneous hardware, software, and network environment. Topics may include hardware and software principles, forensic protocols, data acquisition and discovery of date evidence, applicable law, the design, benefits and limitations of commercial tools, analysis techniques, and report writing.

DFSC 7106. Seminar in Digital Forensics. 1 Hour.
This course immerses students in emerging trends and issues in digital and cyber forensics. The content of the course may vary from semester to semester but includes analysis of current research, security concerns, standards publications, and professional issues.

DFSC 7300. E-Discovery. 3 Hours.
This course explores the initial phase of litigation to find and provide relevant electronic information and records, or electronically stored information, related to a legal case. Technical content of this course includes records management policies and procedures, and E-Discovery applications and technologies for locating and extracting information and records from massive volumes of data in timely and cost efficient ways.

DFSC 7320. Ethics for Digital Forensics. 3 Hours.
This course examines the ethical issues surrounding the collection, preparation, interpretation, and reporting of digital evidence. The American Academy of Forensic Sciences' "Code of Conduct" and the Digital Forensics Certification Board?s ? Code of Ethics and Standards of Professional Conduct? are critically examined and explored. Students examine case materials that feature ethical conflicts and approaches to resolving ethical dilemmas.

DFSC 7330. DF Laboratory Management. 3 Hours.
This course examines techniques to cost-effectively establish and manage a computer forensics laboratory, and its subsequent support to successfully conduct computer-related criminal investigations. Topics include case and evidence management, development of laboratory policies and procedures, funding a digital forensic lab, competency and proficiency testing, equipment validation and verification, lab accreditation from organizations such as the American Society of Crime Lab Directors (ASCLD), and compliance with ISO standards.

DFSC 7340. DF Tools & Techniques. 3 Hours.
This course explores the use of commercial and open-source tools for the identification, collection, and analysis of digital evidence. Topics include the principles of locating and seizing digital evidence, best practices in evidence management, protocols for comprehensive analysis, and a comparative analysis of digital and cyber forensic tool performance.

DFSC 7341. DF Infrastructure. 3 Hours.
This course focuses on the development of laboratory policies and procedures, funding a digital forensics lab, training and certification of examiners, competency and proficiency testing. Topics include validation and verification of digital forensics equipment, compliance with ISO standards, and management of the forensic laboratory.

DFSC 7350. Operating System Forensics. 3 Hours.
This course explores required background knowledge, theory, and practical skills in operating system forensics, including hard disk data acquisition, volume analysis, file system data structure analysis, registry analysis, memory analysis, malware detection, and timeline analysis.
Prerequisite: DFSC 5316.

DFSC 7351. Cloud Computing Forensics. 3 Hours.
This course focuses on the security, vulnerabilities, digital evidence retrieval, analysis, and maintenance in virtualized infrastructures and cloud environments. Topics include the chain of cloud service providers, cloud customers and the complexity of dynamic chain of dependencies between them, and the approaches, methods, and tools that can be used in forensic analysis in virtual and cloud environments.

DFSC 7352. Network Forensic Analysis. 3 Hours.
This course examines start-to-finish methodology and tools for managing network forensics investigation, enables students to uncover powerful forensic evidence from routers, firewalls, intrusion detection and prevention systems, web proxies, and other network devices. Topics may include network evidence acquisition, packet analysis, network flow analysis, wireless network forensics, network log analysis, and network device forensics.
Prerequisite: DFSC 6410.

DFSC 7353. RAID & Remote System Forensics. 3 Hours.
This course examines the theories and practices of RAID (Redundant Array of Inexpensive Disks) and remote system forensics. Concepts addressed in this course include disk imaging, retrieval, maintenance, backup, analysis, and presentation of digital evidence from RAID and remote systems.
Prerequisite: DFSC 7340.

DFSC 7355. Intrusion Forensic Analysis. 3 Hours.
This course provides the study and practices of intrusion detection, vulnerability assessment, and penetration testing. Topics include traffic analysis, intrusion detection methods and systems, intrusion detection system evaluation, vulnerability assessment, methods, techniques, and tools for penetration testing, and system and network security evaluation and assessment.
Prerequisite: DFSC 6410.

DFSC 7356. Mobile Device Forensics. 3 Hours.
This course explores the required background knowledge, theory, and practical skills pertaining to mobile device forensics. Topics focus on the most widespread operating systems on the mobile market. This course examines mobile device evidence collection, data recovery and analysis techniques and tools, system file recovery, deleted file recovery, and the examination of unallocated space.
Prerequisite: DFSC 7350.

DFSC 7357. Malware Forensic Analysis. 3 Hours.
This course explores the concepts and techniques for analyzing, dissecting, debugging, and reverse engineering malicious software. Forensic techniques for protection and recovery from malicious code will be examined in detail.

DFSC 7358. Live System & Memory Forensics. 3 Hours.
This course examines advanced collection and analysis of digital evidence from systems and networks when they are running. Topics may include data acquisition, memory, network connections and traffic, user accounts and passwords, environmental variables, and system and application logs. The course also includes the comparison and evaluation of live forensic tools and techniques.
Prerequisite: DFSC 5316.

DFSC 7359. Social Network Forensics. 3 Hours.
This course examines techniques used to conduct a digital forensic analysis of social networking websites and smart phone social networking applications. This course also explores social media artifacts left on computers such as artifacts in Internet history files, cache, chat logs, web logs, comments and requests in blogs.

DFSC 7360. DF Research Methods. 3 Hours.
This course examines appropriate techniques for the construction of sound research projects. It addresses the identification of appropriate research questions and hypotheses, the critical analysis of sources, the development of explanatory models, the selection of appropriate testing mechanisms and the presentation and interpretation of results. Emphasis is placed on the development of research and writing capabilities. Case studies from current digital and cyber forensic research are presented.
Prerequisite: DFSC 7362.

DFSC 7362. Computational Forensics. 3 Hours.
This course examines principles and uses of computational intelligence methodologies and algorithms in soft computing and digital forensics. Students become familiar with core concepts of each algorithm and a broad perspective of emerging applications to practical problems in digital forensics. Topics may include fuzzy sets, rough sets, artificial neural networks, evolution computing, probabilistic reasoning, and their applications to digital forensics.

DFSC 7364. Scientific Communications. 3 Hours.
This course examines aspects of scientific communication, specifically writing in the disciplines. The goal of this course is to enable students to write professionally in the field of digital and cyber forensic science. The course includes strategies on writing research papers, dissertations, grants, and conference presentations. Emphasis is placed on how to use multi-media effectively in presentations and technical communications.

DFSC 7365. Commercial Tool Verification. 3 Hours.
This course focuses on the principles and techniques in software testing, including the design of high quality tests, the theory behind criteria-based test design and its application in practice. Topics include test design, test automation, test coverage criteria, and how to test software in cutting-edge software development environments. Topics also include proving correctness, and static and dynamic analysis.
Prerequisite: DFSC 7340.

DFSC 7600. Internship. 6 Hours.
This is a ten-week, full-time internship in an approved digital forensic science laboratory. This opportunity allows graduate students to apply their theoretical knowledge, practical skills and abilities in a digital forensic science setting.

DFSC 8370. Dissertation. 3 Hours.
This course must be taken five times to obtain 15 hours of credit to satisfy degree requirements for the PhD in Digital and Cyber Forensics Science.
Prerequisite: Successful completion of requirements for admission to candidacy in the Digital and Cyber Forensic Science PhD program.

Chair: **Peter A. Cooper**

Min Kyung An, PHD (an@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Univ of Texas At Dallas; MS, Univ of Texas-Arlington; BS, Jeju National University

Hyuk Cho, PHD (hxc005@shsu.edu), *Associate Professor of Computing Science*, *Department of Computer Science*, PHD, Univ of Texas At Austin; MS, Univ of Texas At Austin; MA, Korea University; BE, Chonbuk National University

Peter A. Cooper, PHD (csc_pac@shsu.edu), *Professor of Computing Science and Chair, Department of Computer Science*, *Department of Computer Science*, PHD, Univ of Missouri-Columbia; MA, Univ of Missouri-Columbia; BS, Open University; DIPED, Univ of London Inst of Educ

Umit Karabiyik, PHD (uxk006@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Florida State University; MS, Florida State University; BS, Sakarya University

Li-Jen Yu Lester, EDD (lys001@shsu.edu), *Associate Professor of Computing Science*, *Department of Computer Science*, EDD, Sam Houston State University; MA, Sam Houston State University; BS, Tahan Institute of Technology

Qingzhong Liu, PHD (qxl005@shsu.edu), *Associate Professor of Computer Science*, *Department of Computer Science*, PHD, New Mexico Inst/Mining/Tech; ME, Sichuan University; BE, Northwestern Polytechnic Univ

Timothy J Mc Guire, PHD (csc_tjm@shsu.edu), *Associate Professor of Computing Science*, *Department of Computer Science*, PHD, Texas AM University; MS, Colorado State University; BS, Letourneau University

Khaled Mohamed Rabieh, PHD (rabieh@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Tennessee Tech University; MSC, Nile University; BSC, Ain Shams University

Narasimha Karpoor Shashidhar, PHD (nks001@shsu.edu), *Associate Professor of Computer Science*, *Department of Computer Science*, PHD, Univ of Connecticut; MS, Univ of Connecticut; BE, University of Madras

Gary W. Smith, PHD (csc_gws@shsu.edu), *Associate Professor of Computing Science*, *Department of Computer Science*, PHD, Texas AM University; MS, Oklahoma State University; BS, Texas AM University

Donggil Song, PHD (song@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Indiana University; MS, Seoul National University; BA, Seoul National University

Cihan Varol, PHD (cxv007@shsu.edu), *Associate Professor of Computing Science*, *Department of Computer Science*, PHD, Univ of Arkansas-Little Rock; MS, West Virginia University; BSC, Firat University

Mingkui Wei, PHD (mxw032@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, North Carolina State Univ; ME, Southeast University; BE, Nanjing Univ of Science Tech

Bing Zhou, PHD (bxz003@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, University of Regina; MS, University of Regina; BS, Shandong Univ of Technology