DEPARTMENT OF COMPUTER SCIENCE

About

Chair: Bing Zhou, Ph.D. (bxz003@shsu.edu)

Contact Information: (936) 294-3846

Websites:
Department of Computer Science (http://cs.shsu.edu)
Cyber Forensics Intelligence Center (https://df.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.

Highlights

Sam Houston State University provides a comprehensive computing environment for students. The Division of Informational Technology 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. 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 Cyber Forensics Intelligence Center, 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
- Master of Science in Computing and Data Science
- Master of Science in Digital Forensics
- Master of Science in Information Assurance and Cybersecurity
- Graduate Certificate in Cyber Security
- Graduate Certificate in Data Assurance
- Graduate Certificate in Data Science
- Graduate Certificate in Digital Investigation

Student Organizations and Activities

The student chapter, ACM@SHSU - The student chapter sponsors field trips, campus visits by guest speakers, and occasional student/faculty outings.

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 5050. Independent Study. 1-3 Hours.
Students work on a specific research topic under a faculty member's supervision. The specific topic or problem is chosen from current trends and future research directions, which are not covered in the current Computer Science graduate curriculum. Therefore, the course content will vary based upon the topic that both the student and the mentoring faculty member choose. Variable Credit (1 to 3).
Prerequisite: Consent of instructor.

COSC 5300. Computer Science Internship. 3 Hours.
Students engage in a supervised work environment that provides on-the-job computer science related experience within a public, non-profit, or private organization. Under the supervision of a faculty internship coordinator, students apply computing knowledge and theory learned in the classroom to real-world applications, gain practical software coding and development skills, and get professional networking opportunities for their careers in computing and data science. Students are required to complete 240 hours of internship experience in analyzing, designing, developing, testing, implementing, and maintaining software.
Prerequisite: Department Approval.

COSC 5301. Quantitative Foundations of Computer Science. 3 Hours.
Students are provided the fundamental quantitative methods needed in the area of computer science (CS). Topics may 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 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 5302. Computer Science Core Topics. 3 Hours.
Students are provided a solid foundation of Computer Science core concepts, fundamental principles, generalizations, and theories essential to pursuing the CS graduate program. Topics may 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 may 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.
Students engage in a survey of topics in artificial intelligence. Topics may 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.
Students engage in a survey of contemporary topics in database systems. Topics may include: relational database theory, database design issues, normalization, functional dependency, transaction management, indexing, query processing, security integrity issues, data recovery, concurrency problems, optimization, distributed database systems, the client/server model, object-oriented databases, logic/knowledge based systems, and other related topics.

COSC 5319. Algorithm Design and Analysis. 3 Hours.
Students focus on how to design and analyze computing algorithms with emphasis on correctness, -efficiency, and feasibility. Topics may include asymptotic analysis, recurrences and divide-and-conquer algorithms, greedy algorithms, dynamic programming, graph algorithms, and randomized algorithms. Computational complexity theory and computability will also be discussed.

COSC 5320. Computer Architecture & Organization. 3 Hours.
Students are introduced to Computer Architecture and Organization. Topics may 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.
Students study 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.
Students explore real-time and fault-tolerant computing systems. Topics may 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.
Students are provided the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. Students study methodologies for the design of operating system security and forensic techniques for operating systems as well as the identification of best practices in the administration, testing, and security for operating systems.

COSC 5326. Networks & Data Communications. 3 Hours.
Students are introduced 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.
Students engage in a comprehensive study of computer operating systems. Topics may 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 5329. Mobile Application Development. 3 Hours.
Students learn to create applications for various mobile platforms. Topics may include mobile application development frameworks, software engineering, mobile interface design, programming languages, data management, and application distribution.

COSC 5330. Malware. 3 Hours.
Students are provided an in-depth approach to the identification and deconstruction of malicious software, including static and dynamic analyses, malware deconstruction, and rootkit elimination. The course requires the use of virtual machines to isolate live malware samples, and access to a high-speed internet connection. Credit: 3 hrs.

COSC 5332. Computer Graphics. 3 Hours.
Students study modern Computer Graphics programming techniques. Topics may include: representations, transformations, and analysis of 2-dimensional and 3-dimensional objects; techniques for hidden surface/edge removal, illumination and shading models, rendering, and practical exercises, using Modern OpenGLgraphics 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. Students are provided an overview of database security concepts and techniques and discuss new directions of database security in the context of a connected commercial world. Students are provided the information needed to develop, deploy, and maintain a secure database solution. The pitfalls of database design, their means of identification and the methods of exploiting vulnerabilities are exposed. Topics may include database authentication, accounts security, wallets, encrypting data while transit and at-rest, database auditing and virtual private database.

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.
This course focuses on the execution of the research project outlined in Thesis 1. During the graduating semester, students will carry out their research plan, analyze data, and draw meaningful conclusions. They will also develop strong academic writing skills for the preparation of a comprehensive thesis document. This course emphasizes effective project management, data analysis, and scholarly writing to ensure students are well-prepared to present their research findings and defend their thesis successfully. Course Equivalents: COSC 6349
Prerequisite: COSC 6348.

COSC 6312. Multimedia Forensics. 3 Hours.
Students examine the theory and practice of multimedia security and forensics. Topics may 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.
Students are introduced to Neural Networks. Topics may 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/Knowledge Discovery. 3 Hours.
Students explores the emerging techniques and methodologies in Data Mining for the automatic extraction of latent information and knowledge from ever-evolving huge data. Topics include discussion of variety of data mining and computational algorithms as well as the logic behind the data mining approaches. Students will learn a comprehensive framework to collect, clean, process, extract novel information from large-scale data, and evaluate the result. Recent trends and applications will also be discussed. Course Equivalents: COSC 6414
Prerequisite: COSC 5318.

COSC 6315. Machine Learning. 3 Hours.
Students are provided with the principles, design, and implementation of a broad range of machine learning algorithms. Topics may 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. Recent trends and application are covered, as well.
Prerequisite: COSC 5319.

COSC 6318. Language and Compiler Design. 3 Hours.
Students engage in a comprehensive study of computer programming languages. Topics may 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.
Students explore 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 6321. Distributed Computing. 3 Hours.
Students exam the principles and theories of distributed systems, which include MapReduce, Raft Algorithm, Remote Procedure Call (RPC), etc. In addition, real distributed systems, such as Google File Systems (GFS) and Distributed Transactions, are discussed as examples of recent distributed systems. The course emphasizes both lectures and programming labs, in order to help students validate their understanding through hands-on exercises.
Prerequisite: Graduate Standing.

COSC 6331. Data Visualization. 3 Hours.
Students organize and derive meaning from data by using visual presentation tools and techniques. Topics may include cognitive science, perceptual psychology, data management, data visualization theory, visual designs, evaluations of visual designs, and visualization application programming.
Prerequisite: Graduate Standing.

COSC 6332. Computer Vision. 3 Hours.
Students learn both theoretical and practical aspects of computer vision problems and applications. Topics may include camera models, multi-view geometry, image reconstruction, image processing, image classification, object detection, computational photography, and applications of deep learning techniques to computer vision problems.
Prerequisite: Graduate Standing.

COSC 6333. Deep Learning. 3 Hours.
Students examine the architectures, platforms, tools, trends, and research directions of deep learning. Topics may include the relevant algorithms, techniques, and methodologies of convolutional neural networks, recurrent neural networks, auto-encoders, generative adversarial networks, gated recurrent units, long short-term memory networks, deep reinforcement learning, and recent new deep learning architectures. Students get hands-on practices for analyzing real-world large data with deep learning open-sourced frameworks and software tools.
Prerequisite: Graduate Standing.

COSC 6335. Big Data Analytics. 3 Hours.
Students examine advanced analytic techniques, methodologies, and tools for processing big data whose volume, velocity, and variety are unconventional. Topics include types and characteristics of big data, flexible data storage and cost-effective data processing techniques and methodologies, trends and research directions, and hands-on practices for collecting, storing, manipulating, visualizing, and analyzing big data. Particularly, students acquire hands-on big data analytics and data science skills with open-source computing platforms and tools.
Prerequisite: Graduate Standing.

COSC 6338. Data Science Capstone. 3 Hours.
Students conduct team-based capstone projects, which require student teams to apply the knowledge and skills they gained throughout the computer science graduate programs. Particularly, students target to solve real world data science problems and demonstrate their skills in data engineering, machine learning, data mining, big data analytics, data visualization, and other data science-related subjects. Through active learning, students develop effective oral, visual, and written scientific communication skills.
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.
This course is designed to guide Computer Science Master's students in the initial stages of their thesis research. In the proposal semester, students will work closely with faculty advisors to identify a research topic, conduct a comprehensive literature review, and formulate a research proposal. The course will emphasize the development of strong research questions, the exploration of relevant methodologies, and the creation of a robust research plan. By the end of this course, students will have a well-defined research proposal ready for approval.

Digital Forensics

DFSC 5050. Independent Study. 1-3 Hours.
Students work on a specific research topic under a faculty member's supervision. The specific topic or problem will be chosen from current trends and future research directions, which are not covered in the current Digital Forensics curriculum, and Information Assurance and Security graduate curriculum. Therefore, the course content will vary based upon the topic that both the student and the mentoring faculty member choose. Variable Credit (1 to 3).
Prerequisite: Consent of instructor.

DFSC 5310. Principle and Policy in Information Assurance. 3 Hours.
Students engage in an investigation into the development of security planning and policy formation, risk management, security education, training and awareness programs. Students examine physical and electronic approaches to data protection and derive appropriate assessment strategies for determining the assurance quality of target systems.

DFSC 5315. Network and Cyber Security. 3 Hours.
Students are provided the framework and procedures for securing computer systems and data networks. Topics may 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.
Students focus 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.
Students are introduced to basic security needs. Topics may include, but are not 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.
Students focus on how the law impacts digital security in diverse ways. Discussion will emphasize the concept of criminal intent, the digital victim as well as 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.
Students engage in an 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 Investigation. 3 Hours.
Students explore tools for the recovery of information on hardware or hidden within other formats. Topics may 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 Management. 3 Hours.
Students engage in an analysis of investigative techniques and tools in the detection, investigation, and analysis of digital crimes. Students examine the nature of cyberevidence and the tracking and identification of cybercriminals.

DFSC 5336. Business Continuity Management. 3 Hours.
Students examine identification and assessment of threat, risk, vulnerability, and business continuity in case of disaster, as applied to enterprise IT systems. Students explore the physical safeguards and policies necessary to meet the requirements for the protection of data in a fixed site. In addition, techniques and strategies designed to keep enterprise data in service under critical circumstances are discussed.

DFSC 5338. Ethical Hacking. 3 Hours.
Students learn penetration testing and vulnerability analysis of information technology systems. Topics may include in-depth methodologies, techniques, and tools to identify and exploit vulnerabilities, and also assess security risks to networks, operating systems, and software applications.

DFSC 5340. Special Topics 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.
Students focus on philosophies, tactics, and targets of cyber terrorist organizations. The course may include 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.
Student examine the theory and practice of multimedia security and forensics. Topics may 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.
Students are provided 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 are explored.

DFSC 6347. Directed Management and Development Project. 3 Hours.
Students are provided the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. Students cover methodologies for the design of operating system security and forensic techniques for operating systems. In addition, the identification of best practices in the administration, testing, and security for operating systems is covered. Continuous enrollment in DFSC 6347 is required until graduation.
Prerequisite: 24 hours graduate coursework.

DFSC 6410. Cyber Forensics Principles. 4 Hours.
Students explore 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 evidence, applicable law, the design, benefits and limitations of digital forensics tools, analysis techniques, and report writing.

DFSC 7106. Seminar in Digital Forensics. 1 Hour.
Students are immersed 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.
Students explore 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.
Students examine 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. Digital Forensics Laboratory Management. 3 Hours.
Students examine techniques to cost-effectively establish and manage a computer forensics laboratory, and its subsequent support to successfully conduct computer-related criminal investigations. Topics may 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. Digital Forensics Tools & Techniques. 3 Hours.
Students explore the use of commercial and open-source tools for the identification, collection, and analysis of digital evidence. Topics may 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.
Students focus on the development of laboratory policies and procedures, funding a digital forensics lab, training and certification of examiners, competency and proficiency testing. Topics may 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.
Students explore 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.
Students focus on the security, vulnerabilities, digital evidence retrieval, analysis, and maintenance in virtualized infrastructures and cloud environments. Topics may 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.
Students examine start-to-finish methodology and tools for managing network forensics investigation, enabling 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.
Students examine 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.
Students study and practice intrusion detection, vulnerability assessment, and penetration testing. Topics may 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.
Students explore 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. Students examine 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.
Students explore the concepts and techniques for analyzing, dissecting, debugging, and reverse engineering malicious software. Forensic techniques for protection and recovery from malicious code are examined in detail.

DFSC 7358. Live System & Memory Forensics. 3 Hours.
Students examine 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.
Students examines techniques used to conduct a digital forensic analysis of social networking websites and smart phone social networking applications. In addition, students explore 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. Digital Forensics Research Methods. 3 Hours.
Students examine appropriate techniques for the construction of sound research projects. 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 are addressed. 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.
Students examine 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.
Students examine 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.
Students focus 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 may include test design, test automation, test coverage criteria, and how to test software in cutting-edge software development environments. Topics may 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.

DFSC 8670. Dissertation II. 6 Hours.
Doctoral candidates develop and finalize their dissertation during this second step of the dissertation process. Under the direction of a dissertation chair and dissertation committee, each doctoral candidate writes a dissertation manuscript in preparation for the dissertation defense. Topics may vary with scopes and stages of individual research projects, and they may include problem statement, research questions, literature review, proposed methodology, system implementation, data collection, data analysis, platform presentation, and dissertation publication.
Prerequisite: Doctoral candidacy in the PhD program in Digital and Cyber Forensics.

Director/Chair: **Bing Zhou**

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

Kirk A Burns, MS (lib_kab@shsu.edu), *Senior Lecturer of Computer Science*, *Department of Computer Science*, MS, Sam Houston State University; BS, Sam Houston State University

Hyuk Cho, PHD (hxc005@shsu.edu), *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

ABM Rezbaul Islam, PHD (ari014@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Univ of North Texas; MS, Ajou University; BSC, Skakjalal Univ of Sci & Techno

Haodi Jiang, PHD (hxj024@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, New Jersey Institute of Techn; MS, Florida Int'L Univ; BE, Southwest University

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

Fan Liang, MS (fxl027@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, MS, Univ of Massachusetts-Dartmout; BS, Northwestern Polytechnic Univ; DSC, Towson State University

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

Xing Liu, MS (xxl020@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, MS, Lawrence Inst. of Tc; BE, Shanghai Univ of Engr Science; DSC, Towson State University

Van Vung Pham, PHD (vung.pham@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Texas Tech University; MS, Politecnico Di Milano; BS, President University

Amar Adnan Rasheed, PHD (axr249@shsu.edu), *Assistant Professor of Computer Science*, *Department of Computer Science*, PHD, Texas A&M University; MS, Northeastern Illinois Univ; BS, University of Bagdad

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

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

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

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