Computer Information Systems (Forensics Classes) Objectives for Course Challenges	
CIS 200 **Intro to Info Security:** Includes managerial and technical aspects of information security and its role in business including legal and ethical issues, risk management, security technologies, physical security and security maintenance.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe information security and its critical role in business. • Describe what drives the need for information security. • Describe the need for risk management. • Identify and assess risks. • Write procedures for assessing and controlling risk including plans for continuity. • Describe various security technologies and types of physical security and how both are used in business. • Discuss the process of implementing security in business including identifying and describing forms of personnel security. • Describe the steps involved in information security maintenance including how external influences, such as legislative requirements, affect business.
CIS 201 **Digital Forensics and the Law:** Covers legal issues relevant to information security and digital forensics professionals. Topics: electronic discovery, expert testimony, electronic surveillance, evidence retention, preservation and spoliation, privacy issues, Sarbanes Oxley and other legislation.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe how electronic discovery differs from digital forensics. • List and describe the common legal issues related to electronic evidence. • Create a document review, retention, and destruction policy. • Write an acceptable use policy and employer privacy statement. • List and describe the generally accepted computer forensic procedures. • Explain and list the various legislation and regulations that impact technology. • Analyze and critique forensic analysis reports. • Design the verbiage for a production of document requests. • Analyze and critique search warrants, affidavits, and subpoenas. • Explain how the Fourth Amendment pertains to computer privacy. • Summarize in writing the Washington State Laws that pertain to CyberCrime.
CIS 272 **Digital Forensics I:** Includes basic procedures and methodologies for digital forensics that must be mastered. Acquisition, identification and analysis of evidence, documentation	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe the origin of computer forensics and the relationship between law enforcement and industry. • Describe electronic evidence and the computing investigation process. • Discuss ethics and its impact on computer forensics. • Execute an investigation.

strategies, FAT file system, manual and automated analysis tools, working as an expert witness.	• Describe disk structures as well as the Microsoft boot process. • Identify where data can be hidden on different platforms. • Build both a forensic boot floppy and a forensic workstation. • Describe the professional of computer forensics. • Use current forensics tools. • Perform email and graphic image recovery as well as investigations. • Demonstrate an understanding of a code of ethics and conduct related to the information security and digital forensics professions. • Identify standards of professionalism an ethical behavior for information security and digital forensics professional and apply these standards successfully to ethical dilemmas. • Demonstrate an understanding of issues related to privacy and determine how to address them technically and ethically.
CIS 273 **Digital Forensics II:** Covers advanced topics, NTFS, Registry, Event Logs, Internet History and creating analysis reports. Includes an introduction to processes for conducting testing and verification and processing multiple cases from start to finish. Course maps to the CSFA Certificate.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Demonstrate the ability to properly document a computer forensics investigation/analysis and create reports. • Demonstrate the ability to create forensically sound image files and working copy drives from both live and at-rest computer systems using a variety of commercial and open source tools. • Demonstrate an understanding of various techniques to overcome encryption and passwords using a variety of commercial and open source tools. • Describe the differences between the FAT 16 and FAT 32 file systems and boot records. • Describe the function and layout of master boot records, the NTFS Master File Table, and partition tables including how partitions can be hidden and restored. • Identify and describe the Windows registry keys that would be examined relevant to a computer forensics investigation. • Demonstrate the ability to forensically examine an image from a NTFS system as well as recover deleted files and file fragments using both manual and automated methods. • Demonstrate the ability to create a curriculum vita and properly document experience and education for work in the field of computer forensics. • Demonstrate an understanding of a code of ethics and conduct related to the information security and digital forensics professions. • Identify standards of professionalism and ethical behavior for information security and digital forensics professionals, and apply these standards successfully to ethical dilemmas. • Demonstrate an understanding of issues related to privacy and determine how to address them technically and ethically.

CIS 274 **Intro to Network Security:** Covers communication, infrastructure, operational and organizational security, underlying principles used to secure networks, security technologies, intrusion detection, authentication, and cryptography basics. Maps to the Security+ exam.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Compare and contrast the three basic cryptographic functions. • Describe how cryptographic functions can be used to enable security services. • Describe authentication, integrity and confidentiality and how they relate to security systems. • Describe the use of public key technology in networks and the issues associated with key management. • Compare and contrast the various mechanisms that provide authentication services, authentication, authorization, access control as well as several security technologies that provide solutions for securing network access. • Given a network security scenario, decide on the proper authentication technology. • Describe security technologies used for establishing identity and how security technologies are implemented in corporate networks. • Identify strengths and weaknesses associated with protocols designed to authenticate users. • Describe the technologies that exist at the different TCP/IP layers, infrastructure security concepts and the protocols used for dial-in security. • Discuss how digital signatures are used for secure transactions. • Identify and describe the 3 categories of network security threats.
CIS 275 **Host System Security I:** In-depth coverage of the following Win 2K security features: Active Directory, Kerberos 5, smartcards, IPSec and PKI as well as plugging security holes, authenticate users, defend against attacks and add security practices into administrative tasks.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe the types of resources that need to be protected in a networked environment. • Create and write a security policy including procedures for forming a security organization/department. • Describe the functions of a security team, the procedures for selecting appropriate security components, and the major types of DOS attacks and how to protect against them. • Discuss the process of auditing logs and how the audit process should be implemented. • Describe how to conduct a security audit and how to conduct a post-mortem analysis of an attack.
CIS 277 **Security Implementation I:** Includes analyzing network traffic and vulnerability of various protocols, responding to attacks on FTP, HTTP, DNS, HTTPS and SSH with advanced attack detection	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe Ethernet operation and both IP and ARP security issues. • Demonstrate the ability to protect against IP abuse and to use a variety of tools to generate traffic. • List the tools available for frame capture/creation. • Perform frame level analysis. • Detect ARP and IP address spoofing.

using network and host based intrusion detection systems.-	• Capture and analyze ARP traffic and ICMP echo. • Compare and contrast a variety of traffic capture utilities. • Describe TCP/IP vulnerability and how to minimize attacks. • Analyze FTP and HTTP for their vulnerabilities. • Use dsniff to capture passwords. • Perform man-in-the-middle attacks on secure web connections and SSH v1. • Describe TCP/IP fingerprinting and advanced attack detection procedures. • Use the nmap utility to perform network sweep scans. • Examine system logs and statistics for signs of attack. • Configure portsentry for active response to port scans. • Use Snort to examine network traffic in decoded text format and to capture all network packets in tcpdump binary logs. • Use tethereal to analyze captured packets.
CIS 278 **Security Implementation II:** Includes planning, configuring and implementing firewalls, proxy servers and web filtering as well as the use of log consolidation tools.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Identify and implement security commands in internetworking devices such as routers, switches and firewalls. • Design firewall configuration strategies given a business scenario. • Demonstrate the ability to authenticate users and implement appropriate packet filtering. • Plan, develop, design and document a firewall strategy. • Compare and contrast Bastion Hosts. • Implement security for dial-in access, a secure VPN, and appropriate firewall troubleshooting procedures to fix a given problem.. • Demonstrate the ability to isolate, contain, document and recover as well as to respond to false alarms.
CIS 279 **Designing Network Security:** Includes analyzing various networks and business needs; designing and defending appropriate corporate security policies as well as secure networks.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Describe the types of resources that need to be protected in a networked environment. • Create a security policy. • Write procedures for forming a security organization/department. • Describe the functions of a security team. • Describe the procedures for selecting appropriate security components. • Describe the major types of DOS attacks and how to protect against them. • Describe how to conduct security audits. • Discuss the process of auditing logs and how the audit process should be implemented.

	• Describe how to conduct a post-mortem analysis of an attack.
CIS 293 **Digital Forensics III:** Covers detecting/documenting root kits, the Trojan horse theory and other advanced topics including the creation of hash sets of hacker tools and illicit programs to be made available to digital forensic professionals throughout the world. Topics may vary based on current trends.	The student will be able to demonstrate foundational knowledge and skills in forensics. In particular, the student will be able to: • Demonstrate methods to use VMware/Virtual PC as a forensic analysis tool. • Demonstrate how to find yet undocumented root kits and kernel level compromises using a variety of tools. • Demonstrate the ability to develop and use regular expressions to increase search effectiveness. • Demonstrate the ability to defend a particular opinion involving a network intrusion case where a Trojan was allegedly responsible. • Demonstrate the ability to create and verify hash sets of various formats including Hashkeeper, NSRL and FTK. • Demonstrate the skills and abilities needed to provide expert testimony in the classroom regarding complex digital forensic cases. • Demonstrate an understanding of a code of ethics and conduct related to the information security and digital forensics professions. • Identify standards of professionalism and ethical behavior for information security and digital forensics professionals and apply these standards successfully to ethical dilemmas. • Demonstrate an understanding of issues related to privacy and determine how to address them technically and ethically.