STEVENSON UNIVERSITY
SCHOOL OF GRADUATE AND PROFESSIONAL STUDIES
Reprinted with permission from Stevenson University.

GRID OF PROGRAM AND CORE COURSE AND CONCENTRATION OBJECTIVES FOR MS IN FORENSIC STUDIES

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
1. Examine the history, philosophy and development of law enforcement and the judicial and correctional systems within the United States.	Analyze, with substance, specific criminal justice issues			
	Evaluate law enforcement goals and policy			
	Analyze the challenges that face corrections officials who must attempt to strike the appropriate balance between a variety of objectives: safety, security, staff morale, constitutional standards, rehabilitation, punishment, etc			
	Discuss issues and challenges involving the police and constitutional law, plea bargaining and trial matters and issues facing the corrections systems			

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
	Discuss the interdisciplinary concepts of criminal justice, drawing from the fields of criminology, sociology, law, history, psychology and political science			
2. Research and analyze internet resources on topics related to the presentation of evidence at trial				Work productively as part of a team
				Apply rules of evidence
				Investigate a complex forensic problem by conducting research in their fields (forensic accounting, computer forensics, criminalistics, and investigations);
				Create engagement letters, CVs, examiner reports, exhibits, and testimony for use in a simulated proceeding
				Participate in a simulated proceeding as either a witness or an interrogator
				Create reports that reflect the results of this research;

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
3. Analyze a topic in the field of forensic studies and compose a scholarly article on that topic.			Define an issue relative to an approved forensic studies topic and conduct research and analysis on the chosen topic	
			Utilize a variety of research sources and technological tools Chronicle research through journaling	
			Write an academic article based on research that is suitable for publication in a scholarly journal	
			Contribute an original piece of writing to the current body of knowledge in a scholarly field	
			Contribute an original piece of writing to the current body of knowledge in a scholarly field	
			Edit and peer review scholarly work by others	
			Facilitate a writing partnership with another student	
			Defend work orally	
4. Evaluate the Federal Rules of Evidence applicability to legal proceedings and their impact on the administration of justice.		Analyze, with substance, specific evidentiary issues, both procedural and substantive		Work productively as part of a team
		Critically reflect on, and write about, legal issues related to the admissibility of evidence in litigation		Apply rules of evidence

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
		Examine federal evidence law and supporting case law		Investigate a complex forensic problem by conducting research in their fields (forensic accounting, computer forensics, criminalistics, and investigations)
				Create engagement letters, CVs, examiner reports, exhibits, and testimony for use in a simulated proceeding
				Participate in a simulated proceeding as either a witness or an interrogator
				Create reports that reflect the results of this research
5. Interpret, analyze and report on evidence				Work productively as part of a team
				Apply rules of evidence
				Investigate a complex forensic problem by conducting research in their fields (forensic accounting, computer forensics, criminalistics, and investigations)
				Create engagement letters, CVs, examiner reports, exhibits, and testimony for use in a simulated proceeding

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
				Participate in a simulated proceeding as either a witness or an interrogator
				Create reports that reflect the results of this research
6. Integrate professional ethical standards in all activities and work.				Work productively as part of a team
				Apply rules of evidence
				Investigate a complex forensic problem by conducting research in their fields (forensic accounting, computer forensics, criminalistics, and investigations)
				Create engagement letters, CVs, examiner reports, exhibits, and testimony for use in a simulated proceeding
				Participate in a simulated proceeding as either a witness or an interrogator
				Create reports that reflect the results of this research

MS in Forensic Studies Program Objectives	FSCOR 601 Criminal Justice	FSCOR 604 Evidence	FSCOR 606 Forensic Journal Research and Review	FSCOR 702 Mock Trial Capstone
7. Develop and present evidence pertinent to a trial				Work productively as part of a team
				Apply rules of evidence
				Investigate a complex forensic problem by conducting research in their fields (forensic accounting, computer forensics, criminalistics, and investigations)
				Create engagement letters, CVs, examiner reports, exhibits, and testimony for use in a simulated proceeding
				Participate in a simulated proceeding as either a witness or an interrogator
				Create reports that reflect the results of this research

STEVENSON UNIVERSITY
SCHOOL OF GRADUATE AND PROFESSIONAL STUDIES
MS IN FORENSIC STUDIES

OUTCOMES FOR CONCENTRATION IN ACCOUNTING

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
1. Apply investigative techniques for fraud detection in financial reporting.	Integrate computer forensics with fraud and litigation support investigations		Identify and explain the various schemes used by executives, owners, managers and employees to commit fraud	Define and explain their responsibilities in detecting financial statement fraud	Define and explain their responsibilities in detecting tax fraud	Identify appropriate law enforcement agencies to investigate various types of white collar crimes
			Quantify the losses from these schemes	Differentiate between basic financial fraud schemes	Differentiate between basic tax fraud schemes	Illustrate the role of various anti-crime professionals
			Illustrate the human factors in fraud	Detect red flags of financial statement fraud	Detect red flags of tax fraud	
			Devise fraud prevention and detection strategies			
2. Analyze financial statements for false and misleading statements.	Evaluate content and meaning of key elements in electronic evidence traces		Identify and explain the various schemes used by executives, owners, managers and employees to commit fraud	Differentiate between basic financial fraud schemes	Differentiate between basic tax fraud schemes	

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
			Quantify the losses from these schemes	Detect red flags of financial statement fraud	Detect red flags of tax fraud	
			Illustrate the human factors in fraud			
			Devise fraud prevention and detection strategies			
3. Assess fraud risk and adequacy of internal control structures			Identify and explain the various schemes used by executives, owners, managers and employees to commit fraud			
			Quantify the losses from these schemes			
			Illustrate the human factors in fraud			

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
			Devise fraud prevention and detection strategies			
4. Evaluate security requirements and internal controls for accounting systems in business software.		Explain the features of an advanced accounting information system and databases Identify basic control concepts and explain the fundamentals of the COSO framework				
		Produce formal diagrams explaining the flow of data in the major accounting cycles in an advanced accounting system				
		Identify the categories of controls and the associated risks to ensure integrity of the system for processes, availability, and change management				

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
		Describe and document the major risks associated with the expenditure and general ledger reporting cycles and evaluate the adequacy of various control procedures for dealing with those threats				
		Understand the implications of new IT developments, such as XBRL, for internal and external reporting				
		Examine the systems implementation and conversion process				
5. Investigate and analyze financial evidence.	Develop evidence acquisition strategies for digital evidence		Identify and explain the various schemes used by executives, owners, managers and employees to commit fraud	Differentiate between basic financial fraud schemes	Differentiate between basic tax fraud schemes	

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
	Interpret digital evidence findings		Devise fraud prevention and detection strategies	Detect red flags of financial statement fraud	Detect red flags of tax fraud	
	Identify and locate electronic evidence			Develop and implement audit procedures that can detect fraud	Develop and implement audit procedures that can detect fraud	
6. Synthesize accounting, auditing, computer, and investigative skills.	Discuss elementary concepts about the forensic examination of computer media		Identify the role and function of a forensic accountant	Develop and implement audit procedures that can detect fraud	Develop and implement audit procedures that can detect fraud	
7. Analyze legal elements of white collar crime.	Integrate computer forensics with litigation activities		Identify and explain the various schemes used by executives, owners, managers and employees to commit fraud			Describe the causes and consequences of white collar crime
			Quantify the losses from these schemes			Discuss the various laws that are used in the prosecution of white collar crime
						Identify appropriate law enforcement agencies to investigate various types of white collar crimes

Accounting Track Outcomes	FSAAC 620 Forensic Information Technology	FSAAC 622 Advanced Accounting Information Systems	FSAAC 624 Fraud: Accounting	FSAAC 626 Investigation and Analysis: Auditing	FSAAC 628 Investigation and Analysis: Tax	FSAAC 668 White Collar Crime
						Differentiate various types of white collar crimes and how they are committed
						Discuss key cases that serve as examples of various types of white collar crimes
			Illustrate the human factors in fraud			Discuss sentencing and other remedies available to punish white collar crime

STEVENSON UNIVERSITY
SCHOOL OF GRADUATE AND PROFESSIONAL STUDIES
MS IN FORENSIC STUDIES

OUTCOMES FOR CONCENTRATION IN COMPUTER FORENSICS

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
1. Identify corporate liability in handling and preserving electronic data.	Evaluate civil litigation issues stemming from contemporary technology law	Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Interpret and apply the applicable laws and statutes that govern the search and seizure of digital evidence	Perform an acquisition of electronic media	Write a detailed forensic analysis report that documents all relevant findings	Compare and contrast various sources of network data	Compare and contrast the differences between classical computer forensics (ie, media analysis) and network/cloud forensics,	Compare and contrast the differences between classical computer forensics (ie, media analysis) and network/cloud forensics	Analyze current industry trends with respect to mobile device usage and data storage
	Outline electronic discovery and incident response processes, including how digital evidence is identified, collected and preserved		Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis		Create a report, which describes an IDS implementation	Distinguish the primary sources of network-based data used in forensic analysis	Distinguish the primary sources of network-based data used in forensic analysis	
	Examine and work with the legal and evidentiary standards and practices that govern civil matters involving technology law enforcement		Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure						

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
	activities								
	Analyze the findings in a civil technology law litigation involving digital evidence								
	Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence								
	Display effective, clear, compelling oral and written communication skills and fluency in the language of technology								
	Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence								

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
2. Perform the steps in the collection, handling, and preservation of digital evidence.	Evaluate civil litigation issues stemming from contemporary technology law	Explain the physical level disk structures, and data addressing of digital media	Collect properly and preserve digital evidence, to include volatile date, to be used during a computer forensic examination and presented in a court of law	Perform an acquisition of electronic media	Identify and recover malicious files from a victim file system	Compare and contrast various sources of network data	Compare and contrast the differences between classical computer forensics (ie., media analysis) and network/cloud forensics,	Compare and contrast the differences between classical computer forensics (i.e., media analysis) and network/cloud forensics	Conduct forensic examinations of mobile devices using industry tools and industry best practices
	Outline electronic discovery and incident response processes, including how digital evidence is identified, collected and preserved	Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis	Analyze a compromised host running a Windows operating system	Compare and contrast various protocols as seen in network traffic	Distinguish the primary sources of network-based data used in forensic analysis	Analyze the primary sources of volatile data on a computer system,	
	Examine and work with the legal and evidentiary standards and practices that govern civil matters involving technology law enforcement activities	Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence			Recover artifacts from captured network traffic	Analyze network-based data to form an understanding of network attacks and incidents	Assemble volatile data and preserve it for forensic analysis,	

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
	Analyze the findings in a civil technology law litigation involving digital evidence					Install and configure an intrusion detection system	Analyze the primary sources of volatile data on a computer system,	Distinguish the primary sources of network-based data used in forensic analysis	
	Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence					Create IDS rules, which will generate alerts on certain conditions	Assemble volatile data and preserve it for forensic analysis	Analyze network-based data to form an understanding of network attacks and incidents	
	Display effective, clear, compelling oral and written communication skills and fluency in the language of technology					Analyze firewall logs			
	Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence								
3. Identify forensic tools and their use		Convert data between ASCII, Decimal, Hexadecimal and	Collect properly and preserve digital evidence, to include volatile	Analyze a Windows-based computer recovering user	Identify evidentiary information located within the	Compare and contrast various sources of network data	Analyze the primary sources of volatile data on a computer	Analyze the primary sources of volatile data on a computer	Conduct forensic examinations of mobile devices using industry

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
in recovering operating systems, artifacts and data, and the classes of forensic tools and the tasks they perform.		Binary representations	date, to be used during a computer forensic examination and presented in a court of law	and system artifacts	Windows Registry		system,	system	tools and industry best practices, Analyze network service provider call detail records,
		Deconstruct and explain the various components of a Master Boot Record, Partition Table, and Volume Boot Record	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis	Identify and recover malicious files from a victim file system	Compare and contrast various protocols as seen in network traffic	Assemble volatile data and preserve it for forensic analysis	Assemble volatile data and preserve it for forensic analysis	Geo-locate devices by triangulating data from call detail records,
		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure		Analyze a compromised host running a Windows operating system	Recover artifacts from captured network traffic			Generate custom forensic reports based on forensic examinations of mobile devices and the correlation of network service provider call detail records
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence			Install and configure an intrusion detection system			

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
4. Apply the concepts of system policies, auditing, and data recovery, and perform forensic recovery operations using the latest tool sets.		Explain the physical level disk structures, and data addressing of digital media	Collect properly and preserve digital evidence, to include volatile date, to be used during a computer forensic examination and presented in a court of law	Perform an acquisition of electronic media	Identify evidentiary information located within the Windows Registry	Recover artifacts from captured network traffic	Assemble volatile data and preserve it for forensic analysis	Assemble volatile data and preserve it for forensic analysis	Conduct forensic examinations of mobile devices using industry tools and industry best practices
		Deconstruct and explain the various components of a Master Boot Record, Partition Table, and Volume Boot Record	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Analyze a Windows-based computer recovering user and system artifacts	Identify and recover malicious files from a victim file system	Install and configure an intrusion detection system	Distinguish the primary sources of network-based data used in forensic analysis	Distinguish the primary sources of network-based data used in forensic analysis	
		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis	Analyze a compromised host running a Windows operating system	Create IDS rules, which will generate alerts on certain conditions			

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence			Analyze firewall logs			
5. Configure logging utilities to track key events and preserve forensic evidence.		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Analyze a Windows-based computer recovering user and system artifacts	Identify evidentiary information located within the Windows Registry	Recover artifacts from captured network traffic	Compare and contrast the differences between classical computer forensics (ie, media analysis) and network/cloud forensics,	Compare and contrast the differences between classical computer forensics (ie, media analysis) and network/cloud forensics,	Conduct forensic examinations of mobile devices using industry tools and industry best practices
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis	Identify and recover malicious files from a victim file system	Install and configure an intrusion detection system	Distinguish the primary sources of network-based data used in forensic analysis	Distinguish the primary sources of network-based data used in forensic analysis	

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
						Create IDS rules, which will generate alerts on certain conditions			
						Analyze firewall logs			
6. Identify the classes of system exploits and the vulnerabilities they attack.		Explain the physical level disk structures, and data addressing of digital media	Collect properly and preserve digital evidence, to include volatile date, to be used during a computer forensic examination and presented in a court of law	Analyze a Windows-based computer recovering user and system artifacts	Identify evidentiary information located within the Windows Registry	Compare and contrast various sources of network data	Analyze the primary sources of volatile data on a computer system,	Analyze the primary sources of volatile data on a computer system	Predict future security concerns based on current malware and exploits
		Compare and discuss the differences between a single disk volume and a multi-disk volume	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of		Identify and recover malicious files from a victim file system	Compare and contrast various protocols as seen in network traffic	Analyze network-based data to form an understanding of network attacks and incidents,	Analyze network-based data to form an understanding of network attacks and incidents	

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
			digital evidence						
					Analyze a compromised host running a Windows operating system	Recover artifacts from captured network traffic	Analyze network traffic to identify ongoing anomalies	Analyze network traffic to identify ongoing anomalies	
						Create IDS rules, which will generate alerts on certain conditions			
7. Defend the network and system against hacking exploits and evaluate and select appropriate countermeas			Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Analyze a Windows-based computer recovering user and system artifacts	Identify evidentiary information located within the Windows Registry	Compare and contrast various protocols as seen in network traffic	Analyze the primary sources of volatile data on a computer system,	Analyze the primary sources of volatile data on a computer system	Analyze current industry trends with respect to mobile device usage and data storage,
			Inventory, document via detailed notes,	Use forensic tools to perform critical tasks such as	Identify and recover malicious files from a victim	Install and configure an intrusion detection	Analyze network-based data to form an	Analyze network-based data to form an	Conduct forensic examinations of mobile devices

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
ure products.			and establish a chain of custody, for use in a court of law, on all digital evidence collected during a seizure	hash analysis and file signature analysis	file system	system	understanding of network attacks and incidents	understanding of network attacks and incidents	using industry tools and industry best practices
				Prepare a detailed report describing the results of a forensic examination	Analyze a compromised host running a Windows operating system	Create IDS rules, which will generate alerts on certain conditions	Analyze network traffic to identify ongoing anomalies	Analyze network traffic to identify ongoing anomalies	Analyze network service provider call detail records
						Analyze firewall logs			
8. Design an appropriate recovery strategy, create a disaster recovery plan, and develop a plan to test the recovery plan.		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Analyze a Windows-based computer recovering user and system artifacts	Write a detailed forensic analysis report that documents all relevant findings	Create IDS rules, which will generate alerts on certain conditions	Compose a written report of a network incident	Compose a written report of a network incident	Conduct forensic examinations of mobile devices using industry tools and industry best practices
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis		Create a report, which describes an IDS implementation			

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
				Prepare a detailed report describing the results of a forensic examination					
9. Develop criteria for comparing intrusion detection systems and firewall products and configure such products to block unwanted transmissions .		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Analyze a Windows-based computer recovering user and system artifacts	Identify evidentiary information located within the Windows Registry	Compare and contrast various sources of network data	Compare and contrast the differences between classical computer forensics (ie., media analysis) and network/cloud forensics	Compare and contrast the differences between classical computer forensics (i.e., media analysis) and network/cloud forensics,	Predict future security concerns based on current malware and exploits.
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence		Identify and recover malicious files from a victim file system	Compare and contrast various protocols as seen in network traffic	Analyze network-based data to form an understanding of network attacks and incidents,	Analyze network-based data to form an understanding of network attacks and incidents	
					Analyze a compromised host running a Windows operating system	Create IDS rules, which will generate alerts on certain conditions	Analyze network traffic to identify ongoing anomalies	Analyze network traffic to identify ongoing anomalies	

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
10. Synthesize auditing, computer forensic, and investigative skills.		Convert data between ASCII, Decimal, Hexadecimal and Binary representations	Interpret and apply the applicable laws and statutes that govern the search and seizure of digital evidence	Perform an acquisition of electronic media	Identify evidentiary information located within the Windows Registry	Recover artifacts from captured network traffic	Analyze the primary sources of volatile data on a computer system, Assemble volatile data and preserve it for forensic analysis,	Analyze the primary sources of volatile data on a computer system,	Conduct forensic examinations of mobile devices using industry tools and industry best practices,
		Explain the physical level disk structures, and data addressing of digital media	Collect properly and preserve digital evidence, to include volatile date, to be used during a computer forensic examination and presented in a court of law	Analyze a Windows-based computer recovering user and system artifacts	Identify and recover malicious files from a victim file system	Install and configure an intrusion detection system	Analyze network-based data to form an understanding of network attacks and incidents,	Assemble volatile data and preserve it for forensic analysis	Analyze network service provider call detail records,
		Deconstruct and explain the various components of a Master Boot Record, Partition Table, and Volume Boot Record	Formulate and organize the necessary tools/equipment necessary to conduct an incident response or seizure of digital evidence	Use forensic tools to perform critical tasks such as hash analysis and file signature analysis	Analyze a compromised host running a Windows operating system	Create IDS rules, which will generate alerts on certain conditions	Analyze network traffic to identify ongoing anomalies	Analyze network-based data to form an understanding of network attacks and incidents	Geo-locate devices by triangulating data from call detail records,
		Explain the way various types of file systems allocate disk space, keep track of logical files, and handle deleted data	Inventory, document via detailed notes, and establish a chain of custody, for use in a court of law, on all digital evidence collected during a	Prepare a detailed report describing the results of a forensic examination	Write a detailed forensic analysis report that documents all relevant findings	Analyze firewall logs, Create a report, which describes an IDS implementation	Compose a written report of a network incident	Analyze network traffic to identify ongoing anomalies	Generate custom forensic reports based on forensic examinations of mobile devices and the correlation of network service provider call detail

Computer Forensics Track Outcomes	FSIS 640 Technology Law and Enforcement Activities	FSIS 642 File Systems Forensic Analysis	FSIS 643 Incident Response and Evidence Collection	FSIS 644 Windows Forensic Examinations	FSIS 646 Windows Intrusion Forensic Investigations	FSIS 650 Intrusion Detection Systems (IDS), Firewalls, Auditing	FSIS 662	FSIS 663	FSIS 664
			seizure						records
		Identify and recover deleted files and data from unallocated disk areas without the use of automated tools	Demonstrate the use of, and explain the strengths and weaknesses of available tools that are used to collect digital evidence					Compose a written report of a network incident	

STEVENSON UNIVERSITY
SCHOOL OF GRADUATE AND PROFESSIONAL STUDIES
MS IN FORENSIC STUDIES

OUTCOMES FOR CONCENTRATION IN INVESTIGATIONS

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
1. Analyze how criminals think and how their actions are affected by their way of thinking.	Properly phrase interview questions	Demonstrate an effect planning process to gather evidence as applied to various fact patterns and criminal scenarios		Analyze different criminological theories for their impact on policies within the criminal justice system	Direct an effort to develop a program to prevent fraud before it occurs	Describe the causes and consequences of white collar crime
	Discuss the methods to detect deception or truthfulness	Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence		Using scholarly criminological research, evaluate the impact of criminological theory, research, and policy on a contemporary crime topic or issue	Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts	Discuss the various laws that are used in the prosecution of white collar crime
					Use financial analysis and other investigative techniques to proactively detect and document fraud	Differentiate various types of white collar crimes and how they are committed

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
					Explain the value of interview and interrogation techniques to assist in documenting evidence of fraud	
2. Apply investigative and interviewing techniques in all phases of fraud investigations.	Examine the differences between an interview and interrogation	Identify the key attributes of the five fundamental elements (phases) of the investigative process	Integrate computer forensics with fraud and litigation support investigations		Direct an effort to develop a program to prevent fraud before it occurs	Identify appropriate law enforcement agencies to investigate various types of white collar crimes
	Identify the various categories of interviewees involved in an investigation	Identify appropriate legal tools and their capabilities and limitations			Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts	Illustrate the role of various anti-crime professionals

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
	Examine the various legal and regulatory issues when interviewing certain individuals	Demonstrate an effect planning process to gather evidence as applied to various fact patterns and criminal scenarios			Use financial analysis and other investigative techniques to proactively detect and document fraud	
	Properly phrase interview questions	Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence			Explain the value of interview and interrogation techniques to assist in documenting evidence of fraud	
	Discuss the methods to detect deception or truthfulness				Apply the requirements of the US Constitution, criminal laws and procedures, and professional ethics when conducting fraud investigations	

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
	Prepare an accurate, thorough, and concise Report of Interview					
3. Investigate and analyze physical and documentary evidence.		Identify the key attributes of the five fundamental elements (phases) of the investigative process	Develop evidence acquisition strategies for digital evidence			
		Identify appropriate legal tools and their capabilities and limitations	Interpret digital evidence findings			

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
		Demonstrate an effect planning process to gather evidence as applied to various fact patterns and criminal scenarios	Identify and locate electronic evidence			
		Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence	Evaluate content and meaning of key elements in electronic evidence traces			
4. Differentiate between public and private investigations and how they are conducted.	Examine the various legal and regulatory issues when interviewing certain individuals	Identify appropriate legal tools and their capabilities and limitations				

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
5. Conduct effective investigative interviews.	Examine the differences between an interview and interrogation	Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence				
	Identify the various categories of interviewees involved in an investigation					
	Properly phrase interview questions					

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
	Discuss the methods to detect deception or truthfulness					
	Prepare an accurate, thorough, and concise Report of Interview					
6. Conduct investigative research using the Internet, public records, and other sources of information.		Identify the key attributes of the five fundamental elements (phases) of the investigative process		Analyze different criminological theories for their impact on policies within the criminal justice system		Identify appropriate law enforcement agencies to investigate various types of white collar crimes

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
		Identify appropriate legal tools and their capabilities and limitations		Using scholarly criminological research, evaluate the impact of criminological theory, research, and policy on a contemporary crime topic or issue		Illustrate the role of various anti-crime professionals
		Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence				
7. Synthesize facts and observations into coherent, defensible conclusions.	Prepare an accurate, thorough, and concise Report of Interview	Identify the key attributes of the five fundamental elements (phases) of the investigative process			Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts	Describe the causes and consequences of white collar crime

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
	Prepare a Case Report based on the progressive Case Study	Identify appropriate legal tools and their capabilities and limitations				Discuss the various laws that are used in the prosecution of white collar crime
		Demonstrate an effect planning process to gather evidence as applied to various fact patterns and criminal scenarios				Identify appropriate law enforcement agencies to investigate various types of white collar crimes
		Apply logical planning and investigation by demonstrating, in a case study, (a) an applicable legal theory, (b) analytical skill in developing subsequent leads, and (d) appropriate strategies & tactics in pursuit of the evidence				Differentiate various types of white collar crimes and how they are committed

Investigations Track Outcomes	FSINV 600 Investigative Interviewing Techniques	FSINV 605 Investigative Techniques: Physical Evidence	FSAAC 620 Forensic Information Technology	FSLAW 602 Criminology	FSLAW 662 Fraud Investigation and Analysis	FSLAW 668 White Collar Crime
						Discuss key cases that serve as examples of various types of white collar crimes
						Discuss sentencing and other remedies available to punish white collar crime

STEVENSON UNIVERSITY
SCHOOL OF GRADUATE AND PROFESSIONAL STUDIES
MS IN FORENSIC STUDIES

OUTCOMES FOR CONCENTRATION IN LEGAL

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
1. Apply investigative techniques for fraud detection.		Integrate computer forensics with fraud and litigation support investigations		Direct an effort to develop a program to prevent fraud before it occurs		Identify appropriate law enforcement agencies to investigate various types of white collar crimes
				Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts		Illustrate the role of various anti-crime professionals
				Use financial analysis and other investigative techniques to proactively detect and document fraud		
				Explain the value of interview and interrogation techniques to assist in documenting evidence of fraud		

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
				Apply the requirements of the US Constitution, criminal laws and procedures, and professional ethics when conducting fraud investigations		
2. Analyze legal elements of white collar crimes.	Analyze different criminological theories for their impact on policies within the criminal justice system	Integrate computer forensics with litigation activities	Analyze the findings in a civil technology law litigation involving digital evidence	Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts		Describe the causes and consequences of white collar crime
	Using scholarly criminological research, evaluate the impact of criminological theory, research, and policy on a contemporary crime topic or issue		Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence			Discuss the various laws that are used in the prosecution of white collar crime
						Identify appropriate law enforcement agencies to investigate various types of white collar crimes

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
						Differentiate various types of white collar crimes and how they are committed
						Discuss key cases that serve as examples of various types of white collar crimes
						Discuss sentencing and other remedies available to punish white collar crime
3. Analyze, synthesize, and evaluate rules, statutes and case law and apply them to a hypothetical factual			Evaluate civil litigation issues stemming from contemporary technology law	Apply the requirements of the US Constitution, criminal laws and procedures, and professional ethics when conducting fraud investigations		Describe the causes and consequences of white collar crime

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
situation.			Outline electronic discovery and incident response processes, including how digital evidence is identified, collected and preserved			Discuss the various laws that are used in the prosecution of white collar crime
			Examine and work with the legal and evidentiary standards and practices that govern civil matters involving technology law enforcement activities			Identify appropriate law enforcement agencies to investigate various types of white collar crimes
			Analyze the findings in a civil technology law litigation involving digital evidence			Differentiate various types of white collar crimes and how they are committed
			Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence			Discuss key cases that serve as examples of various types of white collar crimes
			Analyze the ethical issues arising in technology law and civil litigation matters involving digital evidence			Discuss sentencing and other remedies available to punish white collar crime

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
4. Perform legal research using computerized legal research tools.	Analyze different criminological theories for their impact on policies within the criminal justice system			Apply the requirements of the US Constitution, criminal laws and procedures, and professional ethics when conducting fraud investigations		Identify appropriate law enforcement agencies to investigate various types of white collar crimes
	Using scholarly criminological research, evaluate the impact of criminological theory, research, and policy on a contemporary crime topic or issue					Illustrate the role of various anti-crime professionals
5. Synthesize legal research and writing, computer, and investigative skills.		Discuss elementary concepts about the forensic examination of computer media	Display effective, clear, compelling oral and written communication skills and fluency in the language of technology	Apply the requirements of the US Constitution, criminal laws and procedures, and professional ethics when conducting fraud investigations	Identify, explain and apply the common law concepts that provide the framework for writing an objective memorandum	
					Analyze, synthesize, evaluate, and effectively present the law and the facts in an objective manner	
6. Analyze how criminals think and how their actions are affected by their way of thinking	Analyze different criminological theories for their impact on policies within the criminal justice system			Direct an effort to develop a program to prevent fraud before it occurs		Describe the causes and consequences of white collar crime

Legal Track Outcomes	FSLAW 602 Criminology	FSAAC 620 Forensic Information Technology	FSIS 640 Technology Law and Enforcement Activities	FSLAW 662 Fraud Investigation and Analysis	FSLAW 667 Legal Research & Writing	FSLAW 668 White Collar Crime
	Using scholarly criminological research, evaluate the impact of criminological theory, research, and policy on a contemporary crime topic or issue			Explain the different types of fraud, who commits it, and understand why they carry out fraudulent acts		Discuss the various laws that are used in the prosecution of white collar crime
				Use financial analysis and other investigative techniques to proactively detect and document fraud		Differentiate various types of white collar crimes and how they are committed
				Explain the value of interview and interrogation techniques to assist in documenting evidence of fraud		