

*Course:* **CJ 1900 Intro to Computer Related Crime**

*Credit Hours:* **3 credit hours**

*Instructor:* **Joan Runs Through**

*Office Phone:* **(435) 879-4420**

*Office Hours:* **Friday 8:00 a.m. to 12:00 p.m. Other hours by apt.**

**PREREQUISITES: None**

**REQUIRED TEXT:**

**Digital Evidence and Computer Crime (3<sup>rd</sup> Edition) by Eoghan Casey**

*All students are expected to read and understand everything outlined in this syllabus. Enrollment and participation online is implied agreement with the terms of this syllabus. If there are questions or concerns about the syllabus, feel free to discuss them with me.*

*This is an online course, which requires verification of your identity through the use of proctored assignments and/or tests. The student will receive an F in the course if these proctored assignments are not completed and are not compatible with coursework submitted throughout the semester.*

**COURSE DESCRIPTION**

Skills-based course introducing computer crime through an overview of the criminal acts that can be committed using a computer or the Internet, and how those acts can be successfully investigated. Also includes the legal aspects of search and seizure, proper procedures for handling digital evidence in relation to the rules of evidence, and the use of basic imaging equipment.

**COURSE FOCUS**

Unit I: Foundations of Digital Forensics

Week 1

In this chapter, the student is introduced to Locard's Exchange Principal and how it applies to digital forensics. The student has the opportunity to learn definitions for digital forensics and digital evidence. The volatile nature of digital evidence is discussed; as is the need for documentation and repeatability in order to maintain forensic soundness. Students become aware of the invasiveness of digital media and are able to identify four ways in which criminals use technology.

## Unit II: Language of Computer Crime Investigation

Week 2

In this chapter, the student has the opportunity to increase vocabulary regarding technology and criminology. The student will be introduced to the various fields of digital forensics as well as the roles played by forensic analysts and examiners. Students will also be introduced to the different roles computers play in crime.

## Unit III: Digital Evidence in the Courtroom

Week 3

In this chapter, the student will have the opportunity to explore the foundation of a case involving digital evidence. The student will learn proper evidence acquisition including seizing, storing, and accessing evidence, and verification that evidence is properly handled. The student will also learn the rights afforded citizens and law enforcement agents by the 4<sup>th</sup> Amendment and the Electronic Communications Privacy Act.

## Unit IV: Cybercrime Law

Week 4

In these chapters, the student will learn how the United States deals with cybercrime. The student will be able to compare and contrast these laws to those enforced in Europe. The major crimes discussed include Computer Fraud, Child Pornography and crimes against children, trademark infringement, forgery, extortion, and identity theft.

## Unit V: Computer Intrusions

Week 5

In this chapter, the student will have the opportunity to learn the scientific method and how to apply it to intrusion investigations. The student will be introduced to intrusion tactics and motivations. Live investigations will also be discussed as well as the risks in investigating live systems.

## Unit VI: Conducting Digital Investigations

Week 6

In this chapter, students will have an opportunity to revisit the scientific method and apply it to digital investigations. Students will learn five digital investigation process models as well as five activities inherent in conducting an investigation (a triggering event, authorization to precede, threshold considerations, transportation, verification, and case management).

## Unit VII: Handling a Crime Scene

Week 7

In this chapter, the student will have the opportunity to review several sources of digital crime scene processing guidelines. Students will learn to develop a plan for processing a crime scene and will acknowledge the role of authorization (i.e. warrants and legal authority) in crime scene processing.

## Unit VIII: Imaging

Week 8

This unit is a hands-on activity requiring the student to create a bit-for-bit image of a suspect drive. Students are encouraged to attend one of two trainings given on campus. Students who cannot attend a face to face class will be given an alternative simulation and will be assisted on-line. This simulation is preparation for the practical portion of the midterm.

## MIDTERM

## Unit IX: Applying Forensic Science to Computers

Week 9

In this chapter, the student will learn about the Standard Operating Procedures (SOPs) and the need for SOP's in the field and in the lab. Students will revisit forensic methodologies including preparation, survey, documentation preservation, examination and analysis, reconstruction, and reporting and how to apply these methodologies to stand-alone computer systems.

## Unit X: Investigative Reconstruction with Digital Evidence

Week 10

In this chapter, the student will be exposed to the connection between crime scene characteristics and modus operandi. The two most common types of reports (preliminary summary and full investigative report) will be introduced as will the field of victimology.

## Unit XI: Modus Operandi, Motive and Technology

Week 11

In this chapter, the student will have the opportunity to learn the unintended consequences new technologies may affect. While recognizing that technology is not evil, students will learn the destruction that application of technology can cause. Students will learn that "modus operandi" answers the "how" part of an investigation while the "motive" answers the why. Students will discuss current technology and how this technology is used as a tool in the hands of criminals.

## Unit XII: Violent Crime and Digital Evidence

Week 12

In this chapter, the student will have the opportunity to learn the role of computers in crime and the information these computers can provide. Students will also have the opportunity to touch on small device forensics and the information that can be gleaned from hand-held units such as GPS units and cell phones.

## Unit XIII: Digital Evidence as Alibi

Week 13

In this chapter, the student will have the opportunity to learn the key elements in an alibi. Students will learn techniques to confirm or refute an alibi. Students will have the opportunity to trace their own digital footprints for a 24-hour period.

## Unit XIV: Sex Offenders on the Internet

Week 14

In this chapter, the student will have the opportunity to learn the methods in which sex offenders can be traced in cyberspace. Students learn the most common sex offenses on the internet and why the internet is attractive to sex offenders.

## Unit XV: Cyberstalking

Week 14

In this chapter, the student will explore the motivations behind cyberstalking as well as the traditional, physical forms of abuse that can accompany the stalking of the victim. The student will be introduced to the methods used by cyberstalkers to control their victims as well as victimological aspects helpful to a cyberstalking investigation.

**OBJECTIVES:** During the course the student will demonstrate skills learned through assignments and exams.

The following table lists Course Competencies/Objectives and further describes this focus. This schedule is tentative and subject to change and the course progresses.

Modules	Objectives	Activities
<p><b>Unit I</b> Foundations of Digital Forensics</p>	<p><b>Performance Objective One:</b> Student will be able to list four ways criminals use technology.</p> <p><b>Performance Objective Two:</b> Student will be able to apply Locard’s Exchange Principal to digital forensics.</p> <p><b>Performance Objective Three:</b> Student will be able to organize characteristics into two categories: Class and Individual.</p> <p><b>Performance Objective Four:</b> Student will be able to equate authentication of digital evidence to hashing.</p>	<ul style="list-style-type: none"> <li>• Personal Introduction</li> <li>• Enrollment Survey</li> <li>• Read Chapter One</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• Computer Desk Interactive Activity</li> <li>• Reading Quiz One</li> </ul>
<p><b>Unit II</b> Language of Computer Crime</p>	<p><b>Performance Objective Five:</b> Student will be able to define and differentiate the following terms: Digital Forensics, Computer Forensics, Network Forensics, Mobile Device Forensics, and Malware Forensics.</p> <p><b>Performance Objective Six:</b> Student will be able to define and differentiate the roles played by forensic examiners and forensic analysts.</p> <p><b>Performance Objective Seven:</b> Student will classify roles of computer in crime as either Fruit of the Crime, Evidence, or Instrumentality</p>	<ul style="list-style-type: none"> <li>• Read Chapter Two</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• View posted Law Enforcement Videos and identify role of computer in the crime described.</li> <li>• Reading Quiz Two</li> </ul>
<p><b>Unit III</b> Digital Evidence in the Courtroom</p>	<p><b>Performance Objective Eight:</b> Student will be able to list four considerations when searching and seizing evidence.</p> <p><b>Performance Objective Nine:</b> Student will be able to list four best evidence practices including: authenticating evidence, inadmissibility of hearsay, levels of certainty, being recognized as a expert</p> <p><b>Performance Objective Ten:</b> Student will be able to define and differentiate the concerns of law and the concerns of scientific knowledge. reconciled in forensic examination</p>	<ul style="list-style-type: none"> <li>• Read Chapter 3</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• Design a digital examination report format</li> <li>• Reading Quiz Three</li> </ul>

<p><b>Unit IV</b> Cybercrime Law: A United States Perspective/A European Perspective</p>	<p><b>Performance Objective Eleven:</b> Student will (with a partner) research and create instructional media regarding a US cybercrime law and its European counterpart.</p> <p><b>Performance Objective Twelve:</b> Student will identify the Fourth Amendment as the US standard against unreasonable searches and seizures.</p> <p><b>Performance Objective Twelve:</b> Student will identify software and media piracy as a crime.</p> <p><b>Performance Objective Thirteen:</b> Student will acknowledge the sovereign rights of foreign countries and anticipate difficulties and solutions regarding interjurisdictional investigations.</p>	<ul style="list-style-type: none"> <li>• Read Chapter 4</li> <li>• Read Chapter 5</li> <li>• Cooperative Learning Activity (Compare Contrast PPT with Partner)</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• View video clip regarding jurisdictional issues</li> <li>• Chapter 4 Quiz</li> <li>• Chapter 5 Quiz</li> </ul>
<p><b>Unit V</b> Computer Intrusions</p>	<p><b>Performance Objective Fourteen:</b> Student will be able to list four reasons criminals break into computers, and understand the need to determine an intruder's goals.</p> <p><b>Performance Objective Fifteen:</b> Student will be able to identify and define the following tactics used in computer intrusions: Phishing, spear phishing, drive-by download, cross site scripting.</p> <p><b>Performance Objective Sixteen:</b> Student will be able to describe the scientific method and how it applies to intrusion investigations.</p>	<ul style="list-style-type: none"> <li>• Read Chapter 13</li> <li>• Hacking Simulation</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• View the <a href="#">KGB and Me</a></li> <li>• Chapter 13 Quiz</li> </ul>
<p><b>Unit VI</b> Conducting Digital Investigations</p>	<p><b>Performance Objective Seventeen:</b> Student will be able to describe and use 5 investigation process models.</p> <p><b>Performance Objective Eighteen:</b> Student will define the stages of an investigation as: a triggering event, authorization to precede, threshold considerations, transportation, verification, and management.</p> <p><b>Performance Objective Nineteen:</b> Student will identify the scientific method as it applies to digital investigations as: Observation, hypothesis, prediction, experimentation/testing, conclusions.</p>	<ul style="list-style-type: none"> <li>• Read Chapter 6</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• View video and develop hypothesis</li> <li>• View (or Post) 1<sup>st</sup> PPT</li> </ul>

<p><b>Unit VII</b> Handling a Crime Scene</p>	<p><b>Performance Objective Twenty:</b> Student will be able to list the fundamental principles for digital crime scene processing</p> <p><b>Performance Objective Twenty-One:</b> Student will be able to develop a plan for processing a crime scene</p> <p><b>Performance Objective Twenty-Two:</b> Student will be able to appropriately label and document a digital crime scene and image a subject drive (bag and tag).</p>	<ul style="list-style-type: none"> <li>• Read Chapter 7</li> <li>• View (or post) US/EU Law PPT</li> <li>• Watch Bag and Tag Power Point</li> <li>• On Campus Imaging Training Group A</li> <li>• Chapter 7 Quiz</li> </ul>
<p><b>Unit VIII</b> Imaging</p>	<p><b>Performance Objective Twenty-Three:</b> Given a suspect drive student will be able to successfully perform a bit-for-bit image 100% of the time.</p>	<ul style="list-style-type: none"> <li>• View (or post) US/EU Law PPT</li> <li>• On Campus Imaging Training (or alternate simulation)</li> <li>• Midterm Practical Sign-up</li> </ul>
<p><b>Midterm</b></p>	<p>Midterm</p>	<ul style="list-style-type: none"> <li>• Midterm Practical</li> <li>• Midterm Written Exam</li> </ul>
<p><b>Unit IX</b> Applying Forensic Science to Computers</p>	<p><b>Performance Objective Twenty-Four:</b> Student will be able to apply forensic methodologies to stand-alone computer systems.</p>	<ul style="list-style-type: none"> <li>• Reading Chapter 16</li> <li>• View (or post) US/EU Law PPT</li> <li>• Chapter 16 Quiz</li> </ul>
<p><b>Unit X</b> Investigative Reconstruction with Digital Evidence</p>	<p><b>Performance Objective Twenty-Five:</b> Student will identify the three categories of evidence used to reconstruct crimes: relational, functional, temporal.</p> <p><b>Performance Objective Twenty-Six:</b> Student will identify and describe the two most common types of reports: preliminary summary and full investigative report.</p>	<ul style="list-style-type: none"> <li>• Read Chapter 8</li> <li>• View (or post) US/EU Law PPT</li> <li>• Watch Video Regarding Detective's Facebook case</li> <li>• Matching Game (evidence to</li> </ul>

		category) <ul style="list-style-type: none"> <li>Chapter 8 Quiz</li> </ul>
<b>Unit XI</b> Modus Operandi, Motive, and Technology	<p><b>Performance Objective Twenty-Seven:</b> Student will be able to classify criminal acts into discrete categories.</p> <p><b>Performance Objective Twenty-Eight:</b> Through the matrix of offense behaviors, the student will be able to take a specific offense and apply it to each behavior.</p>	<ul style="list-style-type: none"> <li>Read Chapter 9</li> <li>View (or post) US/EU Law PPT</li> <li>Chapter 9 Quiz</li> </ul>
<b>Unit XII</b> Violent Crime and Digital Evidence	<p><b>Performance Objective Twenty-Nine:</b> Student will be able to identify the role of computers in violent crime as providing 3 areas of information (victim, offender, computer as a tool)</p> <p><b>Performance Objective Thirty:</b> Student will be able to identify the information a mobile device can provide.</p> <p><b>Performance Objective Thirty-One:</b> Student will be able to differentiate and identify a primary crime scene from a secondary crimes scene.</p>	<ul style="list-style-type: none"> <li>Read Chapter 10</li> <li>Current Event Project</li> <li>View (or post) US/EU Law PPT</li> <li>Workplace Scenario Activity</li> <li>Chapter 10 Quiz</li> </ul>
<b>Unit XIII</b> Digital Evidence as Alibi	<p><b>Performance Objective Thirty-Two:</b> Student will identify the key pieces of information in an alibi as time and location.</p> <p><b>Performance Objective Thirty-Three:</b> Student will identify at least two sources of time and location information.</p>	<ul style="list-style-type: none"> <li>Read Chapter 11</li> <li>View (or post) US/EU Law PPT</li> <li>Online Discussion (Original Post and 2 replies)</li> <li>Digital Footprints Project</li> <li>Chapter 11 Quiz</li> </ul>
<b>Unit XIV</b> Sex Offenders on the Internet	<p><b>Performance Objective Thirty-Four:</b> Student will be able to list three reasons as to why the Internet is attractive to sex offenders.</p> <p><b>Performance Objective Thirty-Five:</b> Student will be able to identify the top two common sex offenses on the internet.</p> <p><b>Performance Objective Thirty-Six:</b> Student will identify two methods to reveal sex offenders.</p>	<ul style="list-style-type: none"> <li>Read Chapter 12</li> <li>Watch Det Ence interview regarding Crimes against Children</li> <li>Online</li> </ul>

<p><b>Unit XIV</b> Sex Offenders on the Internet</p>	<p><b>Performance Objective Thirty-Four:</b> Student will be able to list three reasons as to why the Internet is attractive to sex offenders.</p> <p><b>Performance Objective Thirty-Five:</b> Student will be able to identify the top two common sex offenses on the internet.</p> <p><b>Performance Objective Thirty-Six:</b> Student will identify two methods to reveal sex offenders.</p>	<ul style="list-style-type: none"> <li>• Read Chapter 12</li> <li>• Watch Det Ence interview regarding Crimes against Children</li> <li>• Online Discussion (Original Post and 2 replies)</li> <li>• Chapter 12 Quiz</li> </ul>
<p><b>Unit XV</b> Cyberstalking</p>	<p><b>Performance Objective Thirty-Seven:</b> Student will be able to identify two methods through which stalkers choose their victims.</p> <p><b>Performance Objective Thirty-Eight:</b> Student will trace email to sender IP and host IP.</p> <p><b>Performance Objective Thirty-Nine:</b> Student will find address and contact information for host IP</p>	<ul style="list-style-type: none"> <li>• Read Chapter 14</li> <li>• View Email Tracing PPT</li> <li>• Email Tracing Activity</li> <li>• View (or Post) US/EU Law PPT</li> <li>• Watch video with Dir. Matthews Discussing cyberstalking case</li> <li>• Chapter 14 Quiz</li> </ul>

### Grades and assignments

- I. There will be a total of 15 quizzes consisting of 5-10 multiple choice questions. Each quiz will be worth 5 points for a total of 75 points. The tested material will cover the chapters from the assigned reading as designated on the posted schedule. Each quiz will cover the chapter(s) assigned for that week and will not be comprehensive. These quizzes are designed to test your knowledge of key concepts covered in the reading material. While open book, these quizzes have a ten-minute time limit, so read and study before taking them.
- II. Midterm and Final – The midterm and final are not comprehensive and are worth 100 points each. Both the midterm and the final will have a written (50 pts)

and a practical exercise (50 pts) that will be graded. The tests will cover concepts introduced in the reading and the online discussions.

III. Projects – Each student (in a partnership) will be expected to upload a 5-8 minute presentation on an assigned Cyber Law statute. These will be uploaded to canvas at assigned times. Students will be required to view all student presentations and post a comment or question. Material in the powerpoints will be covered on the midterm and final exams. Other small projects will be assigned throughout the terms for a total of 50 points.

IV. Weekly Posts – Weekly posts are required to discussion questions and other topics for a total of 15 posts at 5 points per post or 75 total points.

There is no extra credit or make-up work.

#### Point Breakdown

Posts 15 @ 5 pts/post	=	75
Quizzes 15@ 5pts/quiz	=	75
Midterm – test	=	50
Midterm – practical	=	50
Final - test	=	50
Final – practical	=	50
Projects	=	<u>50</u>
Total	=	200

#### Grade Breakdown

A 100-93%	A- 92-90%	
B+ 89-87%	B 86-84%	B- 83-80%
C+ 79-77%	C 76-74%	C-73-70%
D+ 69-67%	D 66-64%	D- 63-60%
F 59%	or below	

#### Dixie State College's Policies

The following link will allow you to view information on the following school policies, important dates, the final exam schedule, and helpful resources such as:

Disability Resource Center  
Library Information  
IT Help Desk  
Online Writing Lab  
Testing Center  
Tutoring Center  
Writing Center  
Semester Schedule  
Academic Dishonesty/Academic Integrity Policy  
Disruptive Behavior Policy  
Absences Related to College Functions  
Reasonable Accommodation Policy

<http://new.dixie.edu/reg/syllabus/>