Course: **CJ 2700 Introduction to Digital Forensics**

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 (3rd 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 the digital forensics process, including evidence processing, preservation, analysis, and presentation. Also includes digital evidence basics, data recovery, and some cyber law issues. Requires 6 hours of lab work each week.

Provides an introduction to the world of digital forensics by taking each student through the digital evidence process. Course will cover evidence collection, evidence handling, evidence preservation, evidence analysis, and digital evidence basics.

There are no additional fees for this course, and this course does not hold GE status.

COURSE FOCUS

Unit I: Course Introduction — Week 1

This module introduces a student to the world of digital forensics. It includes basic vocabulary, cyber crime descriptions, and provides an overview of modern digital forensics. For those students who have taken CJ 1900, some of this module will be a review.

Unit II: Digital Evidence Basics — Week 2

This chapter expands on the definition of digital forensics by elaborating on what digital evidence actually is from a physical/logical point of view.

Unit III: Computer Storage Basics — Week 3

Module three ends review material and introduces more advanced topics. To understand digital evidence it is necessary to understand basic computer storage. This module expands the understanding of computer storage. It explores computers and examines the very basics of storing bits.

Unit IV: File Structures and Metadata — Week 4

Understanding digital evidence is understanding digital storage and how the bits that make up digital storage form useful information. This module will continue the exploration of this process by examining how binary information is organized into useful information inside of computer files. It will also explore a side effect of this formation called file metadata that is commonly used in digital investigations.

Unit V: Imaging and Hashing — Week 5

In digital forensics examinations, the original evidence is typically not subjected to examination. Digital evidence is ephemeral and very fragile. Thus, the suspect's devices are accessed as few times as possible, and a clone of the evidence is examined as well. This module will examine this process and explain how it fits into the digital forensics process as a whole.

Unit VI: File System Basics — Week 6

This unit explores how bits are organized on volumes for the storage of files. This module will go into more detail about basic disk layout, describe a side effect of bit storage called slack space, and present a sample file system to help create a deeper understanding.

Unit VII: Data Recovery — Week 7

This unit explores how data recovery is used in digital forensics by breaking it into various levels and discussing the admissibility of the recovered data at each level.

Unit VIII: Windows Forensics — Week 9

This is the first of three units that focus on specific operating systems. This unit discusses several common artifacts that are commonly investigated on Windows systems.

Unit IX: Unix Forensics Week 10

This unit introduces students to the Unix system and the digital forensic tools needed for acquisition and analysis. This modules seeks to introduce students to the very basics of Unix systems and also introduces digital tools that will be further explored in the Digital Triage Module.

Unit X: Digital Triage Week 11

The previous module mentions using a Unix system as a digital forensics tool. This module introduces the concept of digital triage and further explores Unix as an examination tool through digital triage.

Unit XI: Mac Forensics Week 12

This is the last of three units that focus on specific operating systems. This unit discusses several common artifacts that are commonly investigated on Mac systems.

Unit XII and Unit XIII: Network Basics and the Internet Weeks 13 and 14

These modules introduce the use of the Internet as a digital forensics tool and a source for digital evidence. This unit also gives a basic understanding of how the Internet works.

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 as the course progresses.

Modules	**Objectives**	**Activities**
Module I Course Introduction	**Performance Objective One:** Student will be able to define digital forensics **Performance Objective Two:** Student will be able to identify and discuss three types of digital forensic investigations **Performance Objective Three:** Student will identify and define three different categories of cyber crime **Performance Objective Four:** Student will be able to list and define three different digital forensic roles	• Personal Introduction • Enrollment Survey • Online Discussion (Original Post and 2 replies) • Digital Workbook: Module 1 • Study Questions
Unit II Digital Evidence Basics	**Performance Objective Five:** Student will be able to detail how digital media stores data **Performance Objective Six:** Student will be able to list nine steps in basic search and seizure of digital media protocol **Performance Objective Seven:** Student will be able to list six physical and digital hazards which	• Digital Workbook: Module 2 • Online Discussion (Original Post and 2 replies)

	can potentially destroy digital artifacts and what can be done to protect evidence. **Performance Objective Eight:** Student will be able to list the three primary arenas where search and seizures are likely to occur and describe processes for each arena.	• Study Questions • Quiz covering Modules 1 and 2 • Lab 1: Digital Forensics Research
Unit III Computer Storage Basics	**Performance Objective Nine:** Student will be able to list four best evidence practices including: authenticating evidence, inadmissibility of hearsay, levels of certainty, being recognized as a expert **Performance Objective Ten:** Student will be able to define and differentiate the concerns of law and the concerns of scientific knowledge. reconciled in forensic examination	• Digital Workbook: Module 3 • Online Discussion (Original Post and 2 replies) • Study Questions
Module IV File Structure and Metadata	**Performance Objective Eleven:** Student will be able to explain how binary data is transformed into human readable information **Performance Objective Twelve:** Student will be able to perform short binary to numeric translations as well as short binary to ASCII conversions **Performance Objective Thirteen:** Students will be able to perform binary to color translations **Performance Objective Fourteen:** Student will demonstrate the use a hex editor to perform low-level analysis **Performance Objective Fifteen:** Student will be able to locate and identify five different file signatures in file structures. **Performance Objective Sixteen:** Student will be able to define file metadata and explain its use in digital investigation	• Digital Workbook: Module 4 • Online Discussion (Original Post and 2 replies) • Read Chapter 15 in Textbook • Read "Document Metadata and Computer Forensics," Jeffrey R. Jones • Lab 1: Binary Translations • Lab 2: File Signatures and Metadata Hunt
Unit V Imaging and Hashing	**Performance Objective Seventeen:** Student will be able to describe and follow the digital forensics process **Performance Objective Eighteen:** Student will be able to image digital media utilizing the DD command and FTK Imager 100% of the time	• Digital Workbook: Module 5 • Online Discussion (Original Post

	Performance Objective Nineteen: Student will be able to successfully use at least two hashing techniques to include FTK Imager 100% of the time	and 2 replies) • Read online article "What is forensic hard drive imaging?" • DD Worksheets • FTK Imager Worksheets • Imaging and Hashing worksheets • Lab 4 Imaging and Hashing
Unit VI File Systems Basics	**Performance Objective Twenty:** Student will be able to describe basic disk layout and define the terms sector, cluster, head, cylinder, and arm. **Performance Objective Twenty-One:** Student will be able to identify and define slack space as well as list 4 items of evidentiary value that might be discovered there. **Performance Objective Twenty-Two:** Student will be able to describe the FAT file system and interpret a FAT table with 85% accuracy.	• Digital Workbook: Module 6 • Online Discussion (Original Post and 2 replies) • Read Chapter 17 in textbook • Logical vs Physical worksheet • Slack Space Worksheet • Fat Table Interpretation worksheet • Lab 5: On Disk File System Interpretation
Unit VII Data Recovery	**Performance Objective Twenty-Three:** Student will be able to identify five levels of data discovery **Performance Objective Twenty-Four:** Student will be able to explain the admissibility of evidence recovered at each level	• Digital Workbook: Module 7 • Read "Computer Evidence Destroyed," Gordon E. Pelton • Recycle Bin 1 worksheet • Recycle Bin 2

		worksheet • Recently Deleted File Recovery on a FAT System • File Carving Worksheet • Disk Wiping Demonstratio n • Lab y: Data Recovery
Unit VIII Windows Forensics	**Performance Objective Twenty-Five:** Student will identify and extract five evidentiary artifacts within the windows registry **Performance Objective Twenty-Six:** Student will be able to identify and describe the NTFS file system **Performance Objective Twenty-Seven:** Student will be able to identify, describe, and create alternate data streams	• Digital Workbook Module 8 • Read Chapter 17, pp. 534-548 in Textbook • Explore your Registry worksheet • ADS Creation Worksheet • Lab 7: Windows Artifacts Investigation
Unit IX Unix Forensics	**Performance Objective Twenty-Eight:** Student will be able to identify and describe the Unix file system **Performance Objective Twenty-Nine:** Student will be able to use a Unix system as an acquisition and examination machine	• Digital Workbook Module 9 • Reading Chapter 18 • Controlled Mounting worksheet • Piping Exploration worksheet
Unit X Digital Triage	**Performance Objective Thirty:** Student ill be able to explain the process followed for digital triage **Performance Objective Thirty-One:** Student will be able to demonstrate at least one digital triage tool.	• Digital Workbook Module 10 • Read "Research toward a Partially-Automated,

		and rime Specific Digital Triage Process Model? Sections 1-2 • Live Digital Triage • Getting into the Triage Environment • Lab 8 Digital Triage and Basic Linux Commands
Unit XI Mac Forensics	**Performance Objective Thirty-Two:** Student will be able to identify and describe the Mac file system **Performance Objective Thirty-Three:** Student will	• Digital Workbook Module 11 •
Units XII and XIII Network Basics and the Internet	**Performance Objective Thirty-four:** Student will be able to describe and identify network basics **Performance Objective Thirty-five:** Student will be able to explain the creation of the Internet and describe how it functions **Performance Objective Thirty-six:** Student will be able to define the three types of computer addresses **Performance Objective Thirty-seven:** Student will be able to provide examples of network forensics in the form of IP address tracing **Performance Objective Thirty-eight:** Student will be able to explore digital investigations on the Internet	• Digital Workbook Module 12 • Read Chapter 21, 22, and 23 •
Finals Week	**Performance Objective Thirty-Nine:** Given a suspect email, the student will be able to identify the sender IP, the host IP, the email provider address and contact information. **Performance Objective Forty:** The student will be able to formulate social engineering tactics to coax information via human interaction during the course of the digital investigation.	• Final Practical • Final Written

Grades and assignments

I. The tested material for quizzes will cover the chapters from the assigned reading and additional readings as designated on the posted schedule. Each quiz will cover the readings 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. The tests will cover concepts introduced in the readings, the online discussions, and the module labs. A good way to prepare for midterms and finals is to study the provided modules and study questions.
III. Labs – Ten lab assignments are included in this course. The purpose of the lab assignments is to provide hands-on experience in the field of digital forensics. The majority of these labs can be completed at home. However, for those labs which may require on campus equipment, alternate activities will be provided for those students residing beyond a reasonable distance from the Dixie Campus area.
IV. Discussion Posts – Students are required to participate in the discussion board, to post one original post per discussion topic. Students are also required to thoughtfully respond to the posts of two fellow students. There is no extra credit or make-up work.

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/