

Dixie State University  
St. George, Utah  
CJ 2700 Introduction to Digital Forensics  
Fall 2014 (August 25th - December 12th)

---

**Class Details**

Credit Hours: 3.00

Location: On Line

Class Hours: Variable

Prerequisite: None (CJ 1900 Recommended)

**Instructor**

Joan Runs Through

Email: [runsthrough@dixie.edu](mailto:runsthrough@dixie.edu)

Phone: 435.879.4422

Office: University Plaza D 203

Office Hours: MTWR 8:30 - 9:30

(or by appointment)

**Course Description**

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 Materials**

“Digital Evidence and Computer Crime,” Eoghan Casey

ISBN: 978-0-12-374268-1

Various articles and white papers as assigned by instructor

Students are required to have access to a PC (Windows-based) computer and High speed internet.

**Program Goals**

The Criminal Justice Program helps students who are seeking a career in law/law enforcement develop the skills and motivation necessary to succeed in a career in law

enforcement. Students seeking a degree(s) in Criminal Justice/Integrated Studies will receive an education in the following areas, which include, but are not limited to the following: how to examine procedural requirements for the judicial processing of criminal offenders; rights of the accused; general court procedures, trial preparation; laws of evidence; crime scene investigation; corrections; juvenile delinquency/justice; ethical decision making; how to develop writing/problem solving skills through oral argument and writing; how to develop critical thinking skills; and a general understanding of constitutional law.

### **Course Objectives**

This course is designed to provide students with an introduction to the multidisciplinary field of digital forensics in an effort to provide them with a good understanding of the breadth and depth of the field. On completion students will be able to do the following:

1. Provide the steps for search and seizure of digital evidence on computers, personal digital devices, and data storage devices.
2. Understand how the 1st and 4th amendments apply to the search and seizure of digital evidence.
3. Be able to describe the basics behind digital media and digital storage.
4. Know when digital evidence is admissible in a court of law and when it is not.
5. Have the ability to trace email communications back to their source.
6. Be able to explain the entire process of a digital evidence examination including seizure, imaging, analysis, and presentation.

### **Course Core Skill Set**

CJ 2700 is housed in the Criminal Justice department. However, it is a technical skills based course. Students will need to have at least rudimentary computer skills. CJ1900 is suggested for those who are interested in digital forensics but just want a digital forensics elective. CJ2700 is more technical in nature.

The instructor will be willing to help those who need extra assistance, but if you feel you lack many of the skills listed below you should consider taking CJ1900 prior to or instead of this course. If you feel you lack most or all of the skills listed below, you should consider taking a computer literacy course, and CJ1900 prior to this course.

Although Linux tools are demonstrated in class, most of the hands on work for this course will be conducted on a PC. The lab is available to all digital forensics students for lab assignment work, but if you expect to work at home you must have access to a PC with a recent version of Windows.

Suggested CJ2700 skill set:

Copying and pasting between programs  
Basic word processor and spread sheet skills  
Ability to retrieve and store files on external media like flash drives  
Can follow along as instructor demonstrates how to use various PC-based digital forensics tools/software  
Follow directions for executing PC command line analysis programs  
Uncompress and compress files using common programs  
Download and install PC programs on request  
Basic internet surfing and searching/research skills  
General interest and knowledge in computer use

### **Disclosure - (VERY IMPORTANT)**

This course attempts to model the real world as closely as possible. In so doing, we often use real data sets obtained from cell phones, hard drives, and other digital devices. These data sets are typically obtained through donations or online through sites like EBay or Shop Goodwill. We use these datasets either by themselves or as a base for creating training sets.

Since these data sets are obtained from “the wild,” it is extremely likely they will contain explicit adult content in the form of adult pornographic materials, and explicit language. We do not have any desire to expose our students to such materials. Therefore, we attempt to perform some filtering, but it is impossible to completely eliminate all offensive material without destroying its real world aspect.

If you are not willing to view such material, we advise you not to take this course. This is a digital forensics course, and outside academics you will be repeatedly exposed to such materials.

### **Course Policies**

The following general course policies apply to this course. Deviation from these policies is unlikely, but the instructor is not unreasonable. Please feel free to discuss your situation if you have an issue that needs resolving.

1. Lab work is accepted with a 10% drop in grade.
2. Deadlines are given for the tests. Late quizzes will be determined on a case to case basis.
3. You are responsible for information contained in the written modules, given in the video lectures, learned from the hands-on lab exercises, as well as other assigned readings. Please allow yourself 3 hours each week for lecture and readings and another 6 hours for lab work.
4. Extra credit is generally provided that allows a student to miss one quiz. Therefore, make up quizzes are discouraged.

5. Instructor has a zero tolerance policy for academic dishonesty of any kind. Any incidents of academic dishonesty will result in a failing grade for the assignment or course and possible disciplinary action according to DSC policy.
6. Quizzes are timed. Most are in the 10 to 15 minute range. This is to encourage students to read the material prior to attempting the test. You will not have time to “research” each question.
7. Quizzes are available throughout the week of the corresponding module until 11:59 on Sunday evening.
8. When answering homework questions or quizzes it is never acceptable to copy answers from online sources. This is plagiarism and will result in at the very least a 0 on the assignment.
9. Help is available for students working through assigned labs. Dr. Cantrell allows students from the online course to sit through any of his lectures or demonstrations. The online class is generally a day or two ahead of the on campus course.
10. The instructor for this course is happy to tutor any student either on campus or via Skype and can make appointments during daytime hours, after hours, or on weekends. Often a 30 minute tutoring session can eliminate hours of struggling.

### **Lab Policies**

1. The digital forensics computer lab is located in the University Plaza Building D Room 201.
2. The lab was built using one time grant funds . We ask that you be careful with all equipment and help us maintain it for as long as possible.
3. This lab is open to all students currently in the digital forensics program.
4. The lab is generally open from 8 to 5 every school day.
5. Do not enter the lab when a class is already in session unless you have already cleared it with the instructor for that day.
6. If you are working in the lab during a class you are not enrolled in, you may not ask the instructor questions, you must remain quiet, and be respectful of the class in session.
7. Unless you have been assigned a hard drive do not expect work you have saved to remain from class to class.
8. These computers are not as restricted as most on campus labs. Under no circumstances change/add passwords or alter default settings unless asked to do so.
9. After hours access can be granted to students enrolled in certain upper division courses. All students requesting after hours access will be asked to sign a waiver and provide a key deposit.
10. Food and drink is allowed in the lab on a reasonable limited basis. All drink containers must be placed on coasters.

### **Challenge Projects**

Optional extra credit projects may be given throughout the semester. These will be assigned at the discretion of the instructor and no other extra credit will be offered. These projects will be designed to provide a deeper understanding of course topics, and typically provide replacement points. The instructor strongly encourages students to take advantage of these opportunities to offset any absences they might have.

### **Grade Challenges**

A student may challenge the number of points given on a test or quiz question if they provide the challenge in a written format. The following rules apply to a challenge.

1. Challenge explanation limited to one page per question challenged
2. Challenge must be made 7 days from when student was first provided grade
3. Challenge packet must contain the original assignment submission
4. Challenge can only be made once per question
5. Student must provide a complete and valid reference for any materials they wish to use backing up their challenge
6. Most importantly challenge must explain in detail why the original answer deserves more points not an excuse as to why the student missed the question (“My dog ate my notes and I was unable to study.” is not a valid challenge)

### **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

**Note:** The instructor reserves the right to reduce a student's final grade by 1 letter for lack of participation, failure to observe classroom policies, failure to observe lab policies, and failure to complete skills-based labs. There will be a single warning given prior to this reduction.

### **Other Useful Information:**

College approved absences: Dixie College Policy explains in detail what needs to happen if you anticipate being absent from class because of a college-sponsored activity (athletic events, club activities, field trips for other classes, etc). Please read this information and follow the instructions carefully! The policy can be found at: <http://www.dixie.edu/humanres/policy/sec5/523.html>

Dmail: Important class and college information will be sent to your Dmail account. This

information includes your DSC bill, financial aid/scholarship notices, notification of dropped classes, reminders of important dates and events, and other information critical to your success in this class and at DSC. All DSC students are automatically assigned a Dmail account. If you don't know your user name and password, go to [www.dixie.edu](http://www.dixie.edu) and select "Dmail," for complete instructions. You will be held responsible for information sent to your Dmail email, so please check it often.

Disability Accommodations: Students with medical, psychological, learning or other disabilities desiring reasonable academic adjustment, accommodations, or auxiliary aids to be successful in this class will need to contact the DISABILITY RESOURCE CENTER Coordinator (Baako Wahabu) for eligibility determination. Proper documentation of impairment is required in order to receive services or accommodations. DRC is located in the North Plaza Building. Visit or call 652-7516 to schedule appointment to discuss the process. DRC Coordinator determines eligibility for and authorizes the provision of services.

College resources: Several college resources are available to help you succeed. Check out the links for each one to get more information.

If you need help understanding the content of your courses, go to the Tutoring Center located on the 4th floor of the Holland Centennial Commons in Room 431. You can visit them online at <http://dsc.dixie.edu/tutoring/>

If you need help writing papers, go to the Writing Center on the fourth floor of the Holland Centennial Commons in room 421. You can also visit them online at [http://new.dixie.edu/english/dsc\\_writing\\_center.php](http://new.dixie.edu/english/dsc_writing_center.php)

If you need to use a computer to do schoolwork on campus, go to the Smith Computer Center or in the Dixie College library on the second, mezzanine, or third floors of the HCC.

If you are assigned to take a test in the Testing Center, go to the North Plaza. You can get information on their website at <http://new.dixie.edu/testing/>

The Library has all kinds of information and resources. Visit the Dixie State College Library on the 2nd, and 3rd floors of the Holland Centennial Commons, or go to the library website at <http://library.dixie.edu/>

Classroom expectations: It is the responsibility of an instructor to manage the classroom environment to ensure a good learning climate for all students. This means not talking when the teacher is talking, following instructions, and speaking and acting respectfully to the professor and fellow students. If your behavior is disruptive, I will first let you know verbally that you are behaving inappropriately. If it continues, I will send you written notice that your behavior must change. As a last resort, I will drop you from the class. For more details, please see the disruptive behavior policy at:

<http://www.dixie.edu/humanres/policy/sec3/334.html>

Academic integrity: I believe that most students are honest, and I don't want to punish everyone for the few that aren't. However, I will not tolerate cheating, and if I discover that it has occurred, a zero grade will be given for that assignment or exam, and you will not be allowed to make it up. Repeated or aggravated offenses will result in failing the course. Any time you take credit for work you did not do, you are cheating. This includes getting the answers to homework problems from someone else, copying information from a library or internet source and presenting it as if it were your own words (plagiarism), looking at someone else's answers on an exam, and asking someone who has already taken a test about what questions it contains. I have tried to design assignments and exams to minimize the temptation to cheat, but it is not my job to prevent you from cheating. If you cheat and are not caught, it doesn't mean that you "beat the system." It means you violated the Student Code and forfeited your integrity, whether or not you are caught. You will pay the price, sooner or later. (See "Student Code" <http://www.dixie.edu/humanres/policy/sec5/533.html#appeals>).

**Course Outline:**

<b>Module 1: Course Introduction</b>	<b>Due Date</b>
M1: Syllabus Quiz 1	08/31/14
M1: Reading – Syllabus	08/31/14
M1: Reading – Course Introduction	08/31/14
M1: PPT – Course Introduction	08/31/14
<b>Module 2: Digital Evidence</b>	<b>Due Date</b>
M2: Quiz 2 – Over Course Introduction and Digital Evidence Basic	09/07/14
M2: Reading – Module 2 Digital Evidence	09/07/14
M2: PPT – Module 2 Digital Evidence	09/07/14
M2: Lab – Digital Forensics Research (Lab 1)	09/14/14
<b>Module 3: Computer Storage Basics</b>	<b>Due Date</b>
M3: Reading – Module 3 Computer Storage Basics	09/14/14
M3: Textbook Reading – Chapter 15	09/14/14
M3: PPT – Module 3 Computer Storage Basics	09/14/14
M3: Reading Quiz 3 – Over Chapter 15 and Reading Materials	09/14/14
M3: Lab – Computer Storage Basics (Lab 2)	09/21/14
<b>Module Z: Report Writing in Digital Forensics</b>	<b>Due Date</b>
MZ: Textbook Reading – Chapter 16	09/21/14
MZ Reading – Module 4 Digital Forensic Report Writing	09/21/14
MZ: PPT – Module 4 Digital Forensic Report Writing	09/21/14
MZ: Lab – Report Writing Scenario	09/28/14
<b>Module 4: File Structure and Metadata</b>	<b>Due Date</b>
M4: Reading – Module 5 File Structure and Metadata	09/28/14
M4: Reading – “Document Metadata and Computer Forensics”	09/28/14
M4: PPT – Module 5 File Structure and Metadata	09/28/14
M4: Lab – File Signatures and Metadata (Lab 3)	10/05/14

M4: Quiz 4 – Over “Document Metadata and Computer Forensics”	09/28/14
<b>Module 5: Imaging and Hashing</b>	<b>Due Date</b>
M5: Reading – Module 6 Imaging and Hashing	10/05/14
M5: Reading - Online Article	10/05/14
M5: PPT – Module 6 Imaging and Hashing	10/05/14
M5: Quiz 5 – Over Online Article and Materials	10/05/14
M5: Lab – Imaging and Hashing (Lab 4)	10/12/14
<b>Module 6: File System Basics</b>	<b>Due Date</b>
M6: Reading – File System Basics	10/12/14
M6: Textbook Reading – Chapter 17 pp 513-533	10/12/14
M6: PPT – Module 7 File System Basics	10/12/14
M6: Reading Quiz 6 – Chapter 17	10/12/14
M6: Lab – On Disk File System Interpretation (Lab 5)	10/19/14
<b>MIDTERM</b>	<b>Due Date</b>
Midterm Written Exam	10/15/14
Midterm Practical Exam	10/26/14
<b>Module 7: Data Recovery in Digital Forensics</b>	<b>Due Date</b>
M7: Reading - “Computer Evidence Destroyed,”	10/26/14
M7: Reading - Data Recovery in Digital Forensics	10/26/14
M7: PPT – Data Recovery in Digital Forensics	10/26/14
M7: Quiz 66– Over Article and Materials	10/26/14
M7: Lab – Data Recovery (Lab 6)	11/02/14
<b>Halloween Extra Credit</b>	<b>11/02/14</b>
<b>Module 8: Digital Evidence on Windows OS</b>	<b>Due Date</b>
M8: Reading – Module 9	11/09/14
M8: Textbook Reading – Chapter 17 pp 534-548	11/09/14
M8: PPT – Digital Evidence on Windows OS	11/09/14
M8: Lab – Digital Evidence on Windows OS (Lab 7)	11/16/14
<b>Module 9: Digital Forensics and Unix</b>	<b>Due Date</b>
M9: Textbook Reading – Chapter 18	11/16/14
M9: Reading – Module 9	11/16/14
M9: PPT – Digital Forensics and Unix	11/16/14
M9: Reading Quiz 8 (over module)	11/16/14
M9: Lab – Digital Forensics and Unix (Lab 8)	11/23/14
<b>Module 10: Digital Triage and Cyber Investigations</b>	<b>Due Date</b>
M10: Textbook Reading – Chapter 23	11/23/14
M10: reading – Module 11 Digital Triage and Cyber Investigations	11/23/14
M10: PPT – Digital Triage and Cyber Investigations	11/23/14
M10: Reading Quiz 9– Chapter 23	11/23/14
M10: Lab – Digital Triage and Cyber Investigations (Lab 9)	12/07/14
<b>Module 11: Network Basics</b>	<b>Due Date</b>
M11: Textbook Reading – Chapter 21	12/07/14
M11: Reading – Module 12 Network Basics	12/07/14
M11: PPT – Network Basics Lecture	12/07/14
M11: Reading Quiz 10 – Chapter 21	12/07/14
M11: Lab – Email Tracing and Phishing	12/14/14



Review for Final	12/14/14
<b>FINAL</b>	12/19/14