Dixie State University
St. George, Utah
CJ 2700-01 Introduction to Digital Forensics
Spring 2015 (January 12th - May 8th)

Class Details

Credit Hours: 3.00   Class Hours: MWF 9:00-9:50
Location: UNV PLZ D 201 B   Prerequisite: None (CJ 1900 Recommended)

Instructor

Gary Cantrell   Office: UNV PLZ D 201 A
Email: cantrell@dixie.edu   Office Hours: TR 10:30 - 3:00
Phone: 435.879.4422   (or by appointment)

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 each week on a Windows based machine. Course lab fee is required.

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

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 polices 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. Important information, homework submission, and quizzes will be handled at the beginning of class, and class will begin at the assigned time whether you are there or not It is highly recommended that late students obtain announcements from other students.
2. Cell phone use during class is prohibited. Any student violating this policy will be asked to leave for the day. Continual violations of this policy will result in removal from class.
3. Texting in class is obvious, distracting, and very rude. It will be considered cell phone use. See the above rule pertaining to cell phone use.
4. Students who cannot take a quiz or test at the scheduled time may take the test or quiz prior to the scheduled examination time at the discretion of the instructor.
5. Non-pre-scheduled make up tests will only be offered in the case of emergencies and will cost student a letter grade on the test. Proof of emergency such as a doctor's excuse will be requested.
6. Extra credit is generally provided that allows a student to miss 1 to 2 quizzes. Therefore, no make up quizzes will be offered ever.
7. Late homework and lab assignments may receive a deduction of 20% per day including weekends and holidays. An assignment is considered late once the instructor has completed collecting them.

8. Students are expected to attend all class sessions. It will be up to the student to get information missed due to a non-pre-scheduled absence. In my classes there is a direct correlation between attendance and grades.
9. 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.
10. Unless otherwise stated, using Google or any other search engine during class is cheating.
11. Students are expected to be active listeners. Putting one's head down during a lecture is rude. If you are feeling sleepy during class, you are welcome to stand at the back of the room for a while. This will not be considered rude or pointed out by the instructor. This policy applies doubly so for guest/student speakers.
12. There is no reason for computer use for other than taking notes during a lecture or looking up supplementary information. Working on other assignments, looking at social network sites, or any other activity during a lecture is rude and distracting. You will be asked to leave.
13. When answering homework questions, 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.

Lab Policies

1. 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.
2. This lab is only open to students currently in the digital forensics program.
3. The lab is generally open from 8 to 5 every school day.
4. Do not enter the lab when a class is already in session unless you have already cleared it with the instructor for that day.
5. 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.
6. Unless you have been assigned a hard drive do not expect work you have saved to remain from class to class.
7. 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.
8. 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.
9. 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)

Grading Scheme

			Points	Grade
Midterm	100 points		465 >=	A
Final	100 points		450 – 464	A -
Labs	200 points		430 – 449	B+
Quizzes	100 points		415 – 429	B
			400 – 414	B-
			380 – 399	C+
			365 – 379	C
			350 – 364	C-
			300 – 349	D
			< 300	F

Note: The instructor reserves the right the reduce a students final grade by 1 letter for lack of participation, failure to observe class room policies, or failure to observe lab policies. There will only be a <u>single</u> warning given prior to this reduction.

DSU Policies, Procedures, & Semester Dates

Click on this link - http://www.dixie.edu/reg/syllabus/ - for comprehensive information on the Semester Dates, the Final Exam Schedule, University resources such as the library, Disability Resource Center, IT Student Help Desk, Online Writing Lab, Testing Center, Tutoring Center, and Writing Center. In addition, please review DSU policies and statements with regards to Academic Integrity, Disruptive Behavior and Absences related to university functions.

If you are a student with a medical, psychological, or learning disability or think you might have a disability and would like accommodations, contact the Disability Resource Center (652-7516) in the North Plaza. The Disability Resource Center (http://dixie.edu/drcenter/) will determine eligibility of the student requesting special services and determine the appropriate accommodations related to their disability.

Class Room Etiquette

As you professor, I try to maintain a comfortable and positive learning environment for each student. I do not discriminate based on age, class, sex, religion, sexuality, race or any other category, and I will not tolerate discrimination or negativity toward any group. Come and speak to me immediately if you feel there is anything I can do to better establish a positive learning environment in my classroom.

Course Outline:

Week of	Topic
Jan 12, 14, 16	Syllabus Review, Course Introduction
Jan 21, 23	Digital Evidence Basics, Identification, Collection
Jan 26, 28, 30	Binary Translations
Feb 2, 4, 6	Digital Storage and Command Line Basics
Feb 9, 11, 13	Imaging and Hashing
Feb 18, 20	File Structure and Metadata
Feb 23, 24, 26	Report Writing
Mar 2, 4, 6	Mid Term Review, Midterm Practical, Midterm
Mar 9-13	Spring Break
Mar 16, 18, 20	File System Basics
Mar 23, 25, 27	Data Recovery
Mar 30, Apr 1, 3	Data Recovery Continued…
Apr 6, 8, 10	Basic File Analysis
Apr 13, 15, 17	Open Source Forensic Tools
Apr 20, 22, 24	Digital Triage
Apr 27, 29	Network Basics and the Internet
May 6	Final Exam 10:00 - 12:00

For other important dates including withdrawal dates and holidays see the school calendar at: http://dixie.edu/reg/?page=calendar