Dixie State College
St. George, Utah
CJ 3950 Digital Forensics Tools II
Spring 2015 (January 12th - May 8th)

Class Details

Credit Hours: 3.00
Location: UNV PLZ D 201 B
Class Hours: TR 9:00 - 10:15
Prerequisite: CJ 3900 (Grade C- or higher)

Instructor

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

Course Description

Continues the exploration of digital forensics tools from CJ 3900. This course explores more advanced digital forensic tools in use by digital forensics examiners. In addition advanced report writing will be covered to include digital forensics report formats, HTML with digital forensic report writing, and child exploitation reports. Commercial tool certification training and opportunities available dependent on time and funds. Requires 6 hours of lab work each week. Course fee required.

This course does not hold GE status.

Course Materials

Course material will be provided by the 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.

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 Objectives

This course is designed to provide student a more in dept understanding of the Windows artifacts that can be useful in a digital forensic examination. On completion of this course students will:

1. Be familiar with common Windows centric digital forensic artifacts such as the recycle bin, print spooler files, and link files.
2. Be prepared for the Windows portion of the ACE certification examination.
3. Gain more experience in report writing and case examination.
4. Gain advanced experience in the use of AccessData's Forensic tool kit including the ability to crack password
5. Get an overall view of how the Windows operating system fits into the realm of digital forensics.

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 wether you are there are 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 can not 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.
7. Late assignments will 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 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. This 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 open to all 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 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

Midterm	100 points
Final	100 points
4 Reports	200 points
Quizzes	100 points

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

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 13, 15	Syllabus Review, Course Introduction, X-Ways Installation and Configuration (Chap 1)
Jan 20, 22	Case Management and Imaging (Chap 2)
Jan 27, 29	Navigating the X-Ways Forensics Interface (Chap 3)
Feb 3, 5	Refine Volume Snapshot (Chap 4)
Feb 10, 12	The XWF Internal Hash Database and Reg Viewer (Chap 5)
Feb 17, 19	Searching in X-Ways Forensics (Chap 6)
Feb 24, 26	Open lecture, Lab day
Mar 3, 5	Midterm Review, Midterm
Mar 9-13	Spring Break
Mar 17, 19	Advanced Use of X-Ways Forensics (Chap 7)
Mar 24, 26	X-Ways Forensics Reporting (Chap 8)
Mar 31, Apr 2	X-Ways Forensics and Electronic Discovery (Chap 9)
Apr 7, 9	X-Ways Forensics and Criminal Investigations(Chap 10)
Apr 14, 16	Open Lecture, Group work
Apr 21, 23	Final Preparation, Lab Time
May 5	Final Exam 8:00 - 10:00

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