Dixie State College
St. George, Utah
CJ 3950 Windows Forensics
Spring 2014 (January 6th - May 2nd)

Class Details

Credit Hours: 3.00
Location: Unv Plaza D RM 201
Class Hours: TR 9:00 - 10:15
Prerequisite: CJ 3900

Instructor

Gary Cantrell
Email: cantrell@dixie.edu
Phone: 435.879.4422
Office: University Plaza D Upstairs
Office Hours: MTWR 10:00 - 12:00,
(or by appointment)

Course Description

Digital forensics focused on the advanced search and filtering of Windows artifacts, including the recycle bin, file metadata and OLE items, print spools and remnants, unallocated data carving, Windows logs, and link files. In addition, Windows registry items, live registry capture, and carving registry key information from dumped memory files will be covered. Upon successful completion student will be prepared to take the AccessData Certified Examiner (ACE) test.

There are no additional fees for this course, and 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

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 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

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:

Week of	Topic
Jan 7, 9	Syllabus Review and Report Writing Refresher
Jan 14, 16	Module 7: Regular Expressions
Jan 21, 23	Module 7 cont., Report 1
Jan 28, 30	Module 8: Narrowing Your Focus
Feb 4, 6	Module 8 cont.
Feb 11, 13	Module 9: Filtering the Case, Report 1 review, Report 2
Feb 18, 20	Module 9 cont
Feb 24, 27	Module 10: Skill Builder Exercise
Mar 4, 6	Midterm Review, Report 2 review, Midterm
Mar 10-14	Spring Break
Mar 18, 20	Module 11: Common Windows XP Artifacts
Mar 25, 27	Module 11 cont.
Apr 1, 3	Module 12: Working with PR
Apr 8, 10	Module 12 cont.
Apr 15, 17	Module 13: Encrypting File Systems, Module 14: Skill Builder Exercise
Apr 22	Final Review, Report 4 Due