Digital Forensics 290 – Hardware Forensics

Instructor: David Collins
Office: AB1 212-D
Phone: 294-3522
E-mail: dcc002@shsu.edu

Course Purpose/Objectives:

This course is an in depth treatment of hardware forensics. Topics will include data encoding schemes, hard disk geometry, forensically sound preview and data acquisition, bag and tag procedures, transportation and storage procedures, forensic imaging, file system analysis, data recovery and reporting, scripting, and cell phone forensics. We will explore a variety of techniques to search for and recover data including using existing forensics tools, manual examination and recovery of file system data using a hex editor, and programming custom utilities.

Prerequisites:

DF 138

Text/Materials:

Required text:

File System Forensic Analysis, Brian Carrier. ISBN – 0-321-26817-2

IMPORTANT - The textbooks are not optional. You are responsible for assignments and readings from the texts as they are assigned from the first class day. If the books are not available at a university bookstore, you are responsible for acquiring them from another source. Assignment deadlines will not be extended for those without the required textbooks.

Attendance:

Attendance is required. We will complete in class assignments and labs on a regular basis. If you are not in class when an in class assignment is done, then you will not receive credit for that assignment. Exceptions to this rule are on a case by case basis and must include a scheduled meeting with me along with an official note from a doctor, coach or other person in some official capacity to justify the absence. The same applies to absences in general. If you know you must be absent on a particular day, you must provide me with official documentation of the reason for the absence in order to prevent absence penalties.

IMPORTANT – Your final course grade will be lowered one letter grade for 5 absences and by 2 letter grades for 10 absences and so on. Do not get into this situation as it applies no matter what your grades are.

Assignments:

Homework

I will assign homework as necessary throughout the semester. Homework is an opportunity to demonstrate your knowledge. I expect clear, comprehensive explanations of processes and concepts in written homework assignments. All homework must be neat and must have name class and assignment name on the first page. Deviation from this standard will result in a loss of some or all points. If I cannot read your work you will receive few if any points.

Labs

Labs are a major portion of your grade. We will use lab machines with VMWare running various operating systems and file systems. We will also make use of disk imaging hardware and previewing hardware as well as live CD's. Becoming proficient enough to complete the labs will require time outside of class in the lab. The lab is generally available during working hours. Lab time outside of working hours is not guaranteed, and must be scheduled on a case by case basis

Some labs will be completed in groups. All group members must participate in the completion of group labs. This includes demonstration. Any deviation from this from any group member will result in a loss of some or all points for the group member or members who fail to participate appropriately. This participation requirement includes live demonstrations. A group member who fails to attend a live demonstration may lose some or all points for the lab.

The lab manager will coordinate lab use and you are expected to adhere to lab rules. Failure to adhere to lab rules will result in removal from the course with a grade of 'F'.

YOU ARE ENCOURAGED to spend time outside of class in the lab working on your projects and experimenting with the lab hardware and software. The lab manager will conduct a familiarization class to introduce you to lab procedures.

Late work will not be accepted without a scheduled meeting with me along with an official note from a doctor, coach or other person in some official capacity to justify the reason for the late work.

Group Work: All assignments are individual unless specifically stated otherwise by me. I will periodically allow work to be completed in groups, but I will specifically indicate which ones. Any violation of this policy will result in a zero on the assignment for all parties and possible further action as indicated in the **Academic Honesty** section of this syllabus.

DO NOT:

Disrupt the class in any way.
Leave class early unless you have made prior arrangements.
Disrupt the class if you come in late (make every effort to be on time)

A 100 point grade reduction will be incurred for each instance of an above action.
Disruptive behavior will be reported to the Dean of Student Life, Campus Security or both.
Students who disrupt the class more than once will receive an "F" for the course

Grading:

Your final grade is computed as a percentage from the number of points earned divided by the number of points possible. The minimum percentage to earn an A is 90%, a B is 80%, a C is 70%, and a D is 60%. Programs and lab assignments must be unique creations of individual students and free of syntax errors to be worth many points.

Location: AB1-204
Time: TTH: 8:00 – 9:20

Office Hours (AB1-212D): MWF 8:00 – 9:00
MWF 10:00 – 1:00
TTH 12:30 – 2:00

IMPORTANT! I want you to go through the debugging process as it is the only real way to learn to solve problems. That said, I encourage you to come by and see me if you are having trouble with a concept. I will be happy to work with any student who is having trouble with any of the concepts presented in the class.

Email:

Email communication is the best way to communicate with me outside of my office hours during the semester. I will not respond to Email that does not follow appropriate etiquette. At a minimum, your email must include your name, and specifics of your question. It must not include common IRC chat lingo or shorthand. If your email does not conform to the above mentioned minimum requirements, then your email will not be answered. Please be professional in your communication. If you are missing g a grade on Blackboard you may email me a short note informing me of a possible mistake. I will file this note and check on it. I will not, however, discuss grades via email or any other electronic communication. If you have a question about a grade you received, you are required to make an appointment with me in my office so we can discuss it.

Exams:

There will be 3 major exams and a final. The final exam will be comprehensive. Tests are writing intensive and require that you understand the material. Prepare to use the exam as an opportunity to demonstrate your mastery of the subject matter. Answers with little detail or that demonstrate a lack of mastery of the subject matter will result in few if any points.

Cheating on exams or homework WILL NOT be tolerated. A grade of "F" for the course and appropriate disciplinary action will be awarded to any student caught cheating.

Academic Honesty:

All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain complete honesty and integrity in t the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The University and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including but not limited to cheating on an examination or other academic work which is to be submitted, plagiarism, collusion and the abuse of resource materials.

Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the University. Cellular phones and pagers must be turned off before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking at inappropriate times, wearing inappropriate clothing, or engaging in any form of distraction. Inappropriate behavior in the classroom shall result in a directive to leave the class. Students who are especially disruptive also may be reported to the Dean of Students for disciplinary action in accordance with University policy.

Any situation which requires examination of possible academic dishonesty will be dealt with according to the policies and procedures set forth in Academic Policy Statement 810213.

Visitors in the classroom:

Unannounced visitors to class must present a current, official SHSU identification card to be permitted in the classroom. They must not present a disruption to the class by their attendance. If the visitor is not a registered student, it is at the instructor's discretion whether or not the visitor will be allowed to remain in the classroom.

Americans with Disabilities Act:

It is the Policy of Sam Houston State University that no otherwise qualified disabled individual shall, solely by reason of his/her handicap, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination under any academic or Student Life program or activity. Disabled students may request assistance with academically related problems stemming from individual disabilities by contacting the Director of the Counseling Center in the Lee Drain Annex or by calling (936) 294-1720

Religious Holidays:

University policy allows for students to observe religious holy days without penalty. If you intend to miss class as a result of the observance of a religious holy day or as a result of the necessary traveling time required for religious observance, such an absence will not be penalized so long as you have notified the instructor in writing of the dates and times of class sessions that are missed. The deadline for notification is the 12th class day. Students absent from class as a result of religious observance are required to submit any due assignments immediately on their return to the classroom. Makeup tests and quizzes will also be provided on return to the class.