Department of Computer Science

nue I
., Academic Building One
Huntsville, Texas
P.O. Box 2090 • 77341-2090
(936) 294-3846
Fax • (936) 294-4312

COURSE SYLLABUS

DFSC 5316-01 – File System Forensics. CRN: 80808
Fall 2017 - August 23rd to December 7th 2017

Location: Online Course - SHSU Distance Education.
Via Blackboard Learning Management System – http://blackboard.shsu.edu

Instructor	Office	E-mail	Phone:
Dr. Narasimha Shashidhar	AB1 216B	karpoor@shsu.edu	936-294-1591

Office hours: Online via email/Skype/Phone as needed and Class forums/Virtual Office on Blackboard.

Course description: **Welcome to File System Forensics!**
This course deals with file system forensic analysis with a focus on the file system and the disk. The file system of a computing device is where most files are stored and is typically where most evidence is found; it is also the most technically challenging part of forensic analysis. In this course, we attempt to study in detail about different file systems and disc layout. This knowledge will naturally allow you, a digital forensic investigator/analyst, to more easily find evidence, recover deleted data, and validate your tools. We will be using many open source tools for analysis, including The Coroners' Toolkit (TCT), Sleuth Kit and Autopsy. This is an exciting topic and I am confident that all of you will find it fun and inviting.

Catalog description: This course focuses on the important concepts associated with the structures, encoding, boot process and storage technologies of modern computers, and the implications of those concepts regarding the analysis of volumes and file systems for forensics purposes. Credits: 3. Prerequisites: None.

Textbook and Reference Book:

Forensic Discovery 1st Edition by Dan Farmer and Wietse Venema (Text Book)
Hardcover: 240 pages
Publisher: Addison-Wesley Professional; 1 edition (January 9, 2005)
ISBN-10: 020163497X
ISBN-13: 978-0201634976
Amazon Link: http://amzn.to/2b6yoX0

File System Forensic Analysis by Brian Carrier. (Reference)
Paperback: 600 pages
Publisher: Addison-Wesley Professional; 1st edition (March 27, 2005)
ISBN-10: 0321268172
ISBN-13: 978-0321268174
Amazon Link: http://amzn.to/1s4r1P5

The authors have made the electronic version of the textbook available online for free here:

HTML: http://www.porcupine.org/forensics/forensic-discovery/
PDF: Available On Blackboard.

It used to be the case that the reference book by Brian Carrier was available as an electronic access via the SHSU library for free, ProQuest Safari Books Online.

Here is the link: http://bit.ly/1v1hr4j

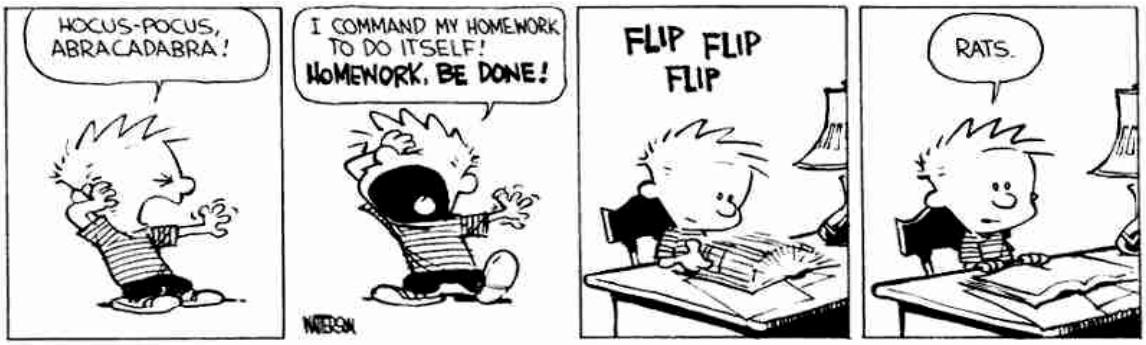
However, it appears that this title is no longer carried by the ProQuest portal anymore. I have provided the link above which is of course broken at this time. I am hoping that the library will make this title available soon. Please check the ProQuest library often and let us all know if the book is available online. The ProQuest library is also a wonderful resource for several other books in Forensics and/or general computing. To use the ProQuest e-library, you will be expected to authenticate yourself with your SHSU username and password to access the book.

To this end, you don't have to necessarily purchase the print versions of either book. However, both these titles are an excellent resource for File System Forensics and perhaps worth purchasing.

Reference Books: Our SHSU ProQuest Safari Books Library Collection has many more books on File Systems and Digital Forensics. I strongly recommend you to explore this collection by searching for relevant topics on their online database. It is of course a good idea for you to study a couple of additional books as part of your academic training in this area. I will post references to these books; online articles etc. during the course of the semester and at times these additional materials may be needed to supplement the information given in the textbook and also to complete the assignments successfully.

Course requirements:

Assignments: Students will be required to complete assignments at the end of each section. 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 typeset homework assignments. All homework must be neat and must have your name, class and assignment name on the first page. Turn in neat, typeset solutions. In doing homework assignments, you are forbidden from referring to any resources other than your own course notes, the class notes or other material suggested by me. In particular, you are not allowed to consult your friends. You are not allowed to use material from previous years of this course, and you are not allowed to use the Internet to "find" solutions.



Research: Students must study and critique/create a summary of at least TWO (2) high quality research articles that complement the class material before the midterm. Students will also

engage in research and will produce ONE (1) original research article before the end of the semester. More information on these topics will be made available during the course of the semester.

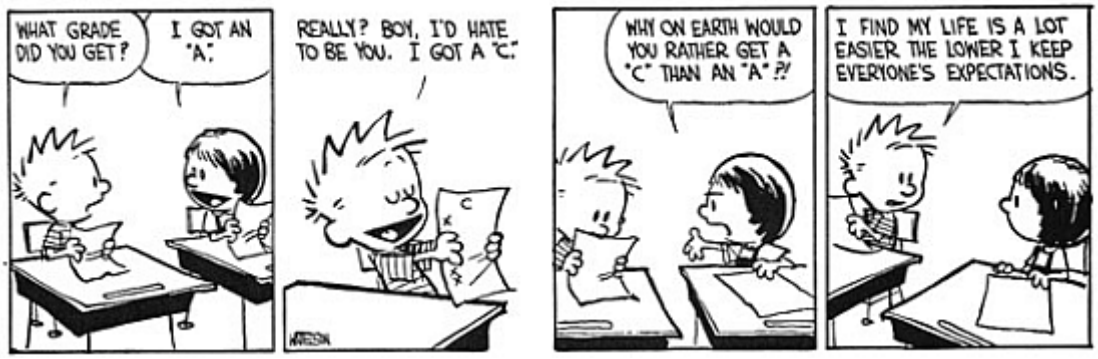
Exams: There are no exams in this course.

Grading plan:			
	Assignments	50%	(roughly 5 Assignments)
	Summary Article	20%	
	Research Paper	30%	

Grading Criteria:

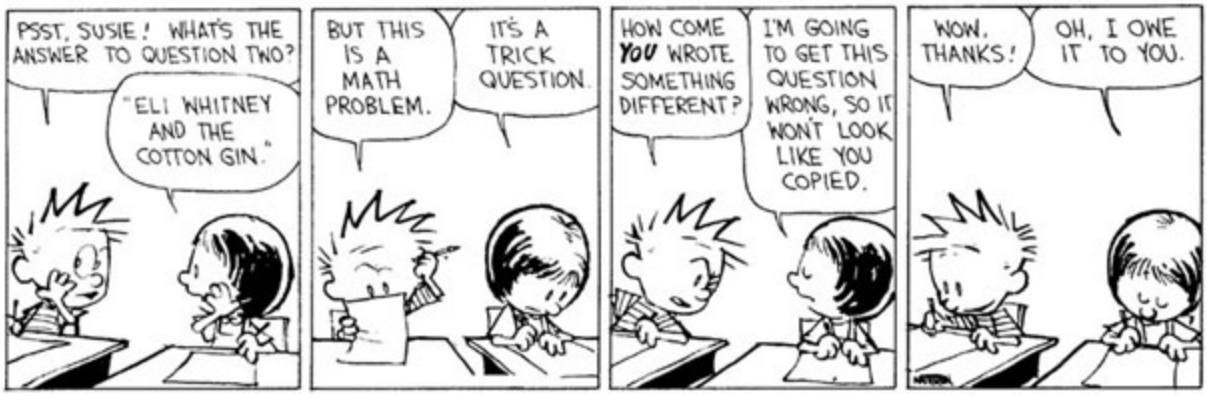
>= 90	⇒	A
>= 80 but < 90	⇒	B
>= 70 but < 80	⇒	C
>= 60 but < 70	⇒	D
< 60	⇒	F

Grade-related questions: It is not possible to provide answers to questions such as the following during the course: "What scores do I have to get for the rest of this class in order to get such and such grade?" "What is the cutoff score for such and such a grade?" "What were the cutoff scores, or what was the grade distribution, in previous years the class was taught?" Late work will not be accepted without a really good justification of the reason for the late work.



Group Work: All assignments and in-class work are individual unless specifically stated otherwise. 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.

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



I warmly welcome you all to this course and guarantee that you will learn much from it and enjoy it thoroughly. My only request is that you are prepared to work hard and sincerely.

Email: Email communication is naturally the best way to communicate with me. Please understand that 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. I will try to respond to your emails promptly.

Course Summary:

My intention is to study the text book in its entirety – cover to cover. After studying the book and related reference materials/papers you should be able to perform file system analysis including:

- Hard Disk Analysis/Evidence Acquisition
- Volume (including multiple disk volumes) Analysis
- Partition Analysis
- Specific file systems – FAT, NTFS, EXT2/3, UFS1/2
- Use open source tools as appropriate to complete the analysis
- Firm understanding of several analysis tools including open source and proprietary tools

Blackboard will be the only source of all course related material including homework problem sets and additional notes. Please familiarize yourselves with the course environment. While I will try to provide all the prerequisite foundations materials required for the course, students are expected to possess a certain level of computing maturity and the desire to learn new concepts and naturally willing to work hard in this process to succeed in the course

Additional goals supported by this course include: a) developing a strong technical foundation in the computational sciences, b) an understanding and sensitivity for security and professional ethics, c) appreciation for the need to pursue professional and related learning activities for life. Students are expected to: a) employ critical thinking in seeking optimal problem solutions, b) maintain and increase their professional knowledge/skill sets, c) develop their ability to express their skills using tools and related analysis techniques and d) to extend the discipline through original cognitive processes..

In the next few pages, I outline a tentative course schedule. Of course, this outline is subject to changes as the semester progresses. In general, I strive to ensure that we attain a greater depth of understanding as opposed to merely "*covering*" course material. I am certain that you will agree that this is a better strategy rather than a superficial attempt to dabble in several different topic areas of File System Forensics, which is a vast field!

<u>Tentative</u> Course Outline: (Subject to changes as the semester progresses) (Sunday is the end of a week)

Week #	Lesson Title	Assigned Readings and Assignments
1 and 2 08/24-09/03	Welcome and Introduction to File System Forensic Analysis. Getting Oriented with Blackboard Textbook Chapters 1-2 + Other Reading Material	Assignment 1 Due on 09/03
3 and 4 09/04-09/17	Textbook Chapters 3-4 + Other Reading Material	Assignment 2 Due on 09/17
5 and 6 09/18-10/01	Textbook Chapters 5-6 + Other Reading Material	Assignment 3 Due on 10/01
7 and 8 10/02-10/15	Textbook Chapters 7-8 + Other Reading Material Identify Research Project/Topic to work on	Assignment 4 Due on 10/15
9 and 10 10/16-10/29	Begin Work - Research Paper Summary/Critique	Assignment 5 Due on 10/29 Research Topic Due on 10/29
11 and 12 10/30-11/12	Begin Work - Research Paper	Assignment **X** Due on 11/12 Paper Summary Due on 11/12
13 and 14 11/13-11/26	Work on Research Paper	Preliminary Draft due 11/26
15 and 16 11/27-12/07	Wrap Up: Complete Research Paper and Submit	Due: Last Class day, 12/07

Note: Your research articles summary and research paper do not have to be independent activities. You are welcome to extend your articles summary to a project and then extend that to a research paper.

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and some group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback. You are encouraged to actively participate in the discussion forums on Blackboard in an effort to learn from your classmates. I will periodically monitor these discussion forums and offer comments to facilitate discussions. This serves to enrich the "virtual" classroom and make the material more exciting, inviting and above all fun!

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours

▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to merely reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Class participation

In accordance with University Policy (http://www.shsu.edu/students/guide/polpro/attendance.html), regular attendance is required; however, no points will be awarded or subtracted based on your attendance. You are responsible for all material covered in every class, regardless of whether you attended or not. It is your responsibility to obtain notes, assignments, etc., from fellow class members if you miss a class.

Academic dishonesty

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 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. No cheating on an examination or assignments is allowed. A score of zero will be given to the student if such a case occurred.

Rules of conduct

Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Please turn off or mute your cellular phone and/or pager before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking among each other at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a, minimally, a directive to leave class or being reported to the Dean of Students for disciplinary action in accordance with university policy.

Americans with Disabilities Act

According to University policy requests for accommodations must be initiated by the student. A student seeking accommodations should go to the Counseling Center and Services for Students with Disabilities (SSD) for instructions.

Religious Holidays

An institution of higher education shall excuse a student from attending classes or other required activities, including examinations, for the observance of a religious holy day, including travel for that purpose. A student whose absence is excused under this subsection may not be penalized for that absence and shall be allowed to take an examination or complete an assignment from which the student is excused within a reasonable time after the absence.