Operating System and File System Forensics (CIS 6386)
Spring 2023 Syllabus

Instructor:

Dan Purcell, MSDF
Daniel.Purcell@ucf.edu

Course Description:

This course will provide students with an understanding of common file systems and operating system artifacts. Students will learn the general components of the FAT and NTFS file systems, including in-depth examination and analysis to fully understand how file systems store data on digital media. Students will explore artifacts from common operating systems such as Microsoft's Windows and Apple's macOS. The course will highlight the most common file systems and operating system artifacts to better prepare students for real-world computer/digital forensics.

Prerequisites:

Computer Forensics I (CGS 5131) or permission of the instructor is required in order to take this course. Students must have previous actual or instructional experience conducting forensic examinations utilizing both command-line and/or graphical user interface tools.

Course Overview:

This course is designed to explore common file systems encountered by a forensic examiner. Likewise, the course is designed to explore operating system artifacts that may be of value to an examiner. It would be impossible to cover every file system or operating system within a single semester. Furthermore, I want your learning experience to be valuable from a practical standpoint. As a practitioner in this field for 2+ decades, I have conducted hundreds of forensic examinations, attended numerous training events, and taught professionally. I have a good grasp on real-world forensics and hope to share my experiences and knowledge with all of you in hopes that you will leave this class and be able to perform a forensic examination on the file systems we cover in a sound manner. In short, the assignments will be meaningful and realistic of what you may find in the "field."

A weekly schedule has been created for this course, and the "flow" is straight forward. Weeks begin on Monday at 12:00 AM (Eastern Time) and end on Sunday at 11:59 PM (Eastern Time). In general, topics will span a two-week period with the first week covering the lecture material and readings while beginning your assignment for the posted topic. The first and second

week will be your week to complete the required assignment, although you will have the entire assignment for a minimum of two weeks. In addition to the lecture material, readings, and assignments (practical exercises or forensic exams), you will be ***required*** to participate in online discussions that I will establish during the term of each assignment. This model should be enough time for you to read through the material, research topics, discuss the topics with your peers, and complete the assignment in a timely manner. Note that some of the topic/assignment periods extend beyond two weeks due to the fact that the research and examination time (on your part) is quite extensive.

I realize we all have family and professional obligations (I do as well), but you are all in graduate school and voluntarily signed up for the course. It is your responsibility to complete the readings, discussions, review of lectures, and assignments by the deadline. I cannot stress how important it is for you to stay on task in order to meet the required deadlines. In the real world, your supervisor or client will expect the same, so please plan ahead and complete the requisite assignments in a timely manner.

Learning Objectives:

To ensure the learning objectives are achieved, you will review the lectures and complete the readings on the front-end of an assignment period and begin your assignment. Every assignment is a forensic examination with accompanying instructions, questions, and a forensic image file. I will provide you with a series of questions to answer, and you will provide the required answer. In some cases, you may be asked to explain your answer in terms of how you located, examined, and analyzed the data. I may ask you to validate your findings as well. Further, you may be asked to provide a conclusion in narrative format to corroborate an allegation or set of facts. Remember, this course is not just about "how does <insert forensic concept> works." The goal is to have you formulate a conclusion based on the technical facts coupled with the facts of the situation. This is a quality that I hope to mold in each of you.

- Examination and analysis of physical and logical disk structures + FAT File System
- Examination and analysis of the NTFS file system
- Data carving techniques within a file system
- Examination and analysis of the Windows 10 Registry
- Examination and analysis of Windows 10 artifacts
- Examination and analysis of macOS artifacts

Required Text:

File System Forensic Analysis by Brian Carrier, Publisher: Addison-Wesley, ISBN: 0-32-126817-2

Computer and Software Requirements:

This is a computer/digital forensics course, and therefore, you must have a modern computer that is capable of running Windows 7 (or higher) or an operating system that will run forensic tools. Your computer should have enough RAM, 8GB or more is ideal, to run forensic applications within Windows 7 (or higher) or the OS of your choosing. You must have at least 10-20 gigabytes of free disk space for forensic image files or other data for the assignments. Generally, your work is submitted via the Quizzes module within WebCourses, and you do not need to upload any documents unless otherwise stated.

If you do not have a Windows machine presently (Mac or Linux), you can use a number of virtualization products such as VMware, Virtual Box, HyperV, and others. You can also download a 90-day VM of Windows 7, 8, or 10 from Microsoft at https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/.

You may use ***any forensically sound software tool*** of your choice in this course. In the end, it is up to you to validate your own software tools. I will not accept the excuse of "my tools reported x, y, or z" when you are responsible for validation (proper and accurate functionality). Cross-validate your tools with other forensically sound software! The University of Central Florida does not endorse any software manufacture or product. However, **UCF provides access to Forensic Explorer by GetData Software (FREE)**. To achieve the learning objectives of this course and ability to examine digital evidence, forensic software or tools are required.

- Forensic Explorer (FREE!!): Forensic Explorer (FEX) is a forensic software suite that provides a wide range of functionality for various file systems and operating system artifacts. It is free for UCF students. To install FEX, you will need a Windows 7 or higher computer with internet access. You will connect to the UCF VPN, and in order to run FEX, you'll have to maintain that connection. Please follow the instructions in the links provide below.
    - UCF VPN: https://ucf.service-now.com/ucfit?id=kb_article&sys_id=ff89f4764f45e200be64f0318110c763
    - Installing Forensic Explorer: http://www.cs.ucf.edu/~czou/msdf/Forensic%20Explorer%20installation.pdf
    - Forensic Explorer User Manual: http://www.cs.ucf.edu/~czou/msdf/Forensic%20Explorer%20v5%20User%20Guide.en.pdf

- X-Ways Software Technology AG - WinHex Specialist (NOT FREE): WinHex Specialist is a powerful disk-level tool for basic forensic examinations. The software is approximately $145 as of November 2021. This tool is NOT required for the course, as you can complete nearly all of the assignments with Forensic Explorer.

- Sleuthkit (FREE!!): The Sleuthkit was primarily developed by Brian Carrier, the author of our class book. This forensic software application features a Windows-based GUI interface with a number of core forensic functions that will serve you well in this course. This product is FREE! https://www.sleuthkit.org/index.php

- FTK Imager (FREE!!): This free application is widely used to obtain a forensic image from media sources. However, it also contains a number of features for examination and analysis. While limited, it can be a very effective tool in this course. https://accessdata.com

Course Policies:

Attendance: A large part of the educational experience is contained in the lectures and class interaction. Therefore, class attendance, meaning active participation online, is ***required***. If you need to miss a class the instructor must be notified in advance. Failure to do so will result in a lower grade and/or points deducted from your grade. Online participation will be graded on the basis of the frequency, quality and originality of online discussion postings. The quality aspect of online discussions will be evaluated first, originality second, and only then will quantity be assessed. Discussions will close as noted in the thread. Participation is also assessed from throughout the entire semester. Missing a discussion during the required time period will result in reduced points for each discussion thread that you miss.

Late Work: Assignments/quizzes and discussions are due by listed deadline. **Late work will not be accepted.** Please turn your work in on time!

Participation: Class participation is expected and an integral part of your grade. Be active in class. You will be required to participate in class discussions (topics) for the assignment period, and likewise, you will be required to interact with questions from your peers in an effort to bolster problem solving and peer review. Discussions and participation is 30% of your final grade! ***Merely posting the required thread for the assignment period without interacting with your peers will result in a poor participation grade.***

Writing Requirements: You are expected to write at a graduate level. Attention to proper grammar and spelling coupled with logical structure is a must in this class. In the real world, you will be judged by your writing so please pay attention to this requirement now. I will deduct points for sloppy work! I will host the questions within WebCourses for you to enter your answers within the appropriate area. This will allow immediate feedback of your grade unless the answer requires human interaction such as a narrative answer. Other answers such as absolute values can be graded instantly (upon final submission).

Incomplete Grade: A grade of "I" (Incomplete) may be assigned by the instructor when a student is unable to complete a course due to extenuating circumstances, and when all requirements can be completed in a short time following the end of the term. The student is responsible to arrange with the instructor for the completion of the requirements of the course.

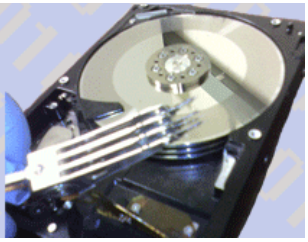
Ethics: Computers and related technology are very powerful tools in our lives and in this class. If you use a computer or related technology to conduct an unethical or illegal act, you will receive an immediate "F" for the course - no questions asked! If you cheat, plagiarize, or perform any unethical conduct, you will receive an immediate "F" for the course - again, no questions asked. If you opt to conduct yourself in this manner, be prepared to face the consequences. I can't be any clearer. Everyone is expected to remain professional and courteous at all times. Flaming, profanity, or otherwise acting unprofessional will result in dismissal from this course.

Copyright: **The course materials, including but not limited to, the recorded lectures, forensic image files, student assignment documents (including those completed by you with correct or incorrect answers), and other course materials, are owned by Dan Purcell. I reserve all rights with respect to all content herein. If I discover that you have used, reposted, uploaded, shared, or otherwise distributed the copyright materials outside the scope of this class, in addition to other remedies provided by law, I reserve the right to bring legal proceedings against you seeking monetary damages and an injunction to stop you using those materials. You are prohibited from reposting, uploading, sharing, or otherwise distributing the course materials in any form. You could also be ordered to pay legal costs.**

Communications:

All communications for the course will be conducted through the WebCourses (the course website). I will host a general discussion area for the course topics and weekly assignments. ***There will be an "Ask the professor" discussion thread for technical, assignment, or related questions. Please post your questions in the discussion thread so everyone can view the question and answer. I do not want to answer the same question in separate emails to each of you.*** We all learn better when we learn as a group, so please make sure that you post your questions in the proper discussion thread. I encourage each of you to research the topic and problem-solve each issue in a collective manner. Remember, 30% of your grade is class participation, and answering questions is a vital part of that grade!

If you have a private or urgent matter, you can email me at daniel.purcell@ucf.edu. I will respond to discussion questions and email within a reasonable amount of time. I do not have an office at UCF, nor do I have an office telephone number through the university. The discussion area, WebCourses email through the course website, and my UCF email account are the only means to contact me. Please contact me in that order.



Assignments:

At the onset of the assignment period, you will be presented with a lecture on the topic, which you must download and view. Required readings will accompany the topic as well. Likewise, you can download the assignment at the onset of the assignment period. Discussion topics will be posted at the same time or during the assignment period. Students will accomplish six (6) forensic examinations (aka: assignments) throughout the duration of the course. As stated previously, you will have a minimum of two weeks to complete each assignment. Each assignment will require you to perform a forensic examination on the media using forensic or non-forensic software. You will answer a series of objective or investigative questions in a worksheet provided to you with each assignment. Prior to the deadline, you will enter your answers into the ***Quizzes*** module of WebCourses. Please read the weekly schedule at the end of this document. The general description of each assignment is listed below.

1. Assignment #1: This assignment will focus on physical and logical disk structures wherein you will be asked to identify and interpret data in the master boot record, volume boot record, and system areas of the volume(s). An emphasis partition schemes will be present in this assignment. In addition, you will be asked to interpret data in the FAT file systems.

2. Assignment #2: This assignment will focus on the NTFS file system and the core files/objects that make up the file system. Special emphasis will be on the master file table ($MFT) and how to manually interpret values. Students will manually parse the $MFT for both allocated and deleted MFT entries. Be prepared to manually parse through data structures to interpret values! This assignment is quite extensive and requires a significant amount of time. *NOTE: In addition to the NTFS chapters in Brian Carrier's book, I also recommend the* ***Quick Reference Guide*** *(2.0) app for iPad/iPhone/iPod Touch as published by Lock and Code (****https://lockandcode.com****). This is not required, but I highly recommend it now and in the future!*

3. Assignment #3: The Windows Registry contains a goldmine of information for examiners. In this assignment, you will examine the Windows Registry and better understand the structure of the various hives (files), what they contain, and how to interpret values. In addition, you will learn how to recover deleted registry subkeys or values that may have deleted by the user or the operating system.

4. Assignment #4: Microsoft Windows operating systems produce a number of valuable "artifacts" within system files and user profiles that may be very valuable in a forensic examination. In this assignment, you will examine recycle bin records, link files, thumbnail files, prefetch files, and other "artifact" files.

5. Assignment #5: Understanding file signatures (file headers) and their corresponding data types is a key skill in forensic examinations. In this assignment, you will learn how to manually parse the unallocated area of the media to recover data. While there are forensic tools that will

recover "data carve" understanding how to perform recovery manually will provide with the skills necessary to validate you automated forensic tools and also give you a fundamental skill to do so when the automated tools cannot do it. This lesson will correlate with the file system(s) on the volume where you recover data (ex: FAT or NTFS).

6. Assignment #6: Apple Corporation is producing many computer systems and devices such as the Mac series, iPhone, Apple Watch, iPad, etc. In this assignment, we will explore the HFS+ and APFS file systems along with the partitioning schemes now used in APFS. We will look at security and encryption schemes that are now layered into the Mac. We will also look at the macOS features and forensic artifacts. The assignment will focus on common artifacts and files or locations where forensic examiners should consider. This lesson was updated in 2021 and 2022.

For each assignment, you will be able to view a description of the item on the course homepage. In the sidebar of WebCourses, the "**Assignments**" link provides you with the assignment worksheet, forensic image file, and corresponding lecture video. The course content may be stored in a standard ZIP file. I use WinRAR to compress the data, and you may opt to use the same utility to decompress the data. For all of the assignments, you will enter your answers into the "**Quizzes**" area in WebCourses. The assignment and quiz will be available for the term of the assignment.

NOTE: In each of the assignments, you will find redundancy on specific "forensic" concepts such as physical and logical disk structure, hashing, file size, etc. This is intentional and by design. One of the goals is to reinforce some of the basic competencies that you learned in Computer Forensics I and II or other courses in the MSDF curriculum. By the end of the semester, you will understand why the redundancy exists!

Tests/Quizzes/Exams:

The quiz module is used for the entry of assignment answers, but there are no traditional quizzes or tests that follow a topic in this course, nor is there a final examination. Further, there are no papers, essays, or other writing assignments Your grade is largely based on the forensic examinations (assignments), weekly discussions, and participation, which entails responding to your peers in the discussion area (questions and issues - ie: problem solving).

Grading Policies:

Requirement	Weight
Assignments	70%
Class Discussions & Participation	30%

Grading Scale:

90 - 100	=	A	60 - 60.99	=	D
80 - 89.99	=	B	0 - 59.99	=	F
70 - 79.99	=	C			

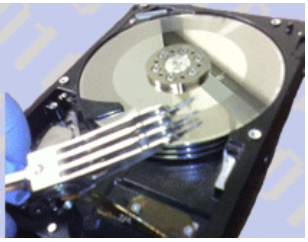
The discussion and participation grade is calculated as follows:

- There are 7 ***required*** discussions (6 for the assignment periods and 1 intro during week #1). The required discussions are 10 points each for a total of 70 points. In order to achieve 10 points, you must adequately answer any questions, discuss the scope of the topic, and cite your resources, if applicable.
- Participation is rated on the number and quality of posts that you make throughout the semester for each required discussion topic beyond the initial post noted above. Interaction with your classmates is fundamentally necessary to achieving a successful participation grade. There are a total of 30 possible points for participation.
- The required discussions points (70) and participation points (30) equate to a total of 100 points for 30% of your final grade.
- If you opt to not participate, you will receive zero (0) points for participation!

Important: ***The quiz module allows you to enter your assignment answers, as previously noted. The quiz module allows me to assess your answers electronically, thereby reducing grading time. Please note that the module is not perfect, and it doesn't account for errors on the fill-in-the-blank answers. I MANUALLY grade each quiz, even though the quiz module does most of the grading. Please do not email me about your grade until I make an announcement to the class that the grading process for each assignment has been completed. If you have questions thereafter, you are more than welcome to email me within WebCourses.***

Master of Science in Digital Forensics

An Interdisciplinary Program at UCF



Course Schedule

Week	Dates	Topic	Readings	Assignment	Due By
1	1/9/2023 – 1/15/2023	Course Introduction	Course Syllabus	Obtain books and materials, post your bio in discussion area	1/15/2023
2	1/16/2023 – 1/29/2023	Disk Structures & FAT	FSFA: 4-6, 8-10	Listen to Disk Structure / FAT lecture & start Assignment #1 + Discussion	1/29/2023
3	1/16/2023 – 1/29/2023	Disk Structures & FAT	FSFA: 4-6, 8-10	Listen to Disk Structure / FAT lecture & Assignment #1 + Discussion	1/29/2023
4	1/30/2023 – 2/26/2023	NTFS File System	FSFA: 11-13	Listen to NTFS lecture & begin Assignment #2 + Discussion	2/26/2023
5	1/30/2023 – 2/26/2023	NTFS File System	FSFA: 11-13	Listen to NTFS lecture & begin Assignment #2 + Discussion	2/26/2023
6	1/30/2023 – 2/26/2023	NTFS File System	FSFA: 11-13	Listen to NTFS lecture & begin Assignment #2 + Discussion	2/26/2023
7	1/30/2023 – 2/26/2023	NTFS File System	FSFA: 11-13	Listen to NTFS lecture & begin Assignment #2 + Discussion	2/26/2023
8	2/27/2023 – 3/19/2023	Windows Registry	Lecture Only	Listen to Windows Registry lecture & start Assignment #3 + Discussion	3/19/2023
9	2/27/2023 – 3/19/2023	Windows Registry	Lecture Only	Work On Windows Registry Assignment #3 + Discussion	3/19/2023
10	2/27/2023 – 3/19/2023	Windows Registry	Lecture Only	Complete Windows Registry Assignment #3 + Discussion	3/19/2023
11	3/20/2023 – 4/2/2023	Windows Artifacts	Lecture Only	Complete Windows Artifacts Assignment #4 + Discussion	4/2/2023
12	3/20/2023 – 4/2/2023	Windows Artifacts	Lecture Only	Complete Windows Artifacts Assignment #4 + Discussion	4/2/2023
13	4/3/2023 – 4/16/2023	Data Carving	FSFA: 8	Listen to Data Carving lecture & complete Assignment #5 + Discussion	4/16/2023
14	4/3/2023 – 4/16/2023	Data Carving	FSFA: 8	Listen to Data Carving lecture & complete Assignment #5 + Discussion	4/16/2023
15	4/17/2023 – 4/30/2023	macOS Exams	Lecture Only	Complete macOS Assignment #6 + Discussion	4/30/2023
16	4/17/2023 – 4/30/2023	macOS Exams	Lecture Only	Complete macOS Assignment #6 + Discussion	4/30/2023

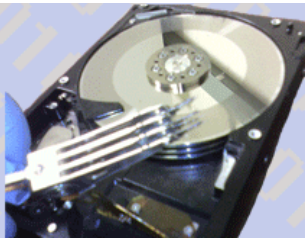
NOTE: "FSFA" is Brian Carrier's File System Forensic Analysis book as abbreviated above for applicable readings.

Notable Dates:

For a complete list of holidays that UCF observes along with important academic dates, please visit https://calendar.ucf.edu/2023/spring for details.

Master of Science in Digital Forensics

An Interdisciplinary Program at UCF



About Dan Purcell:

I am a fulltime law enforcement officer with the Seminole County Sheriff's Office in Central Florida. I have served in various enforcement and investigative assignments in my career, both as a practitioner and supervisor. I have served on or regularly assisted several state and federal task forces such as the FBI's Innocent Images Task Force, United States Secret Service Electronic Crimes Task Force, and Internet Crimes Against Children Task Force. I was previously sworn as a United States Special Deputy Marshal for the U.S. Secret Service Electronic Crimes Task Force. I have participated in, managed, and led a number of task force programs, the SCSO computer/digital forensics program, the Child Sexual Predator Program and other grant program initiatives, and other high-tech crime initiatives/programs. I have testified as an expert witness in the field of computer/digital forensics in both state and federal courts.

I have served in various leadership capacities at the Sheriff's Office to include the ranks of Sergeant, Lieutenant, Captain, and Chief. Currently in my 28th year of fulltime law enforcement service, I presently lead the Department of Law Enforcement, which is comprised of uniformed patrol functions, investigative functions, special operations (Aviation, K9, SWAT, etc.), Communications (911 Center), Forensic Laboratory, and Judicial Services. I am a graduate of the Federal Bureau of Investigation (FBI) National Academy, 254th Session. The FBI National Academy, held in Quantico, VA, is regarded as the most prestigious law enforcement executive leadership training program in the world. I am also a graduate of the FBI Florida Executive Development Seminar and the FDLE Chief Executive Seminar programs.

In 2000, I also attend my first computer forensic course through the International Association of Computer Investigative Specialists (IACIS) and achieved the Certified Forensic Computer Examiner (CFCE) certification. Since that period, I have attended numerous basic, intermediate, advanced, and expert level courses in computer forensics and related investigations. I also have a B.A. in Criminal Justice Administration, Graduate Certificate in Computer Forensics (UCF), and a Master's of Science in Digital Forensics (UCF). I was one of five graduates in the first graduating class for the MSDF program here at UCF. I have also achieved and/or currently maintain the following certifications:

- Certified Forensic Computer Examiner (CFCE)
- EnCase Certified Examiner (EnCE)
- Certified Electronic Evidence Seizure Specialist (CEECS)
- Digital Forensics Certified Practitioner (DFCP)
- AccessData Certified Examiner (ACE)

I have been instructing computer/digital forensics and related investigative courses since 2001. I've instructed law enforcement, military, government, and private sector students in the field of computer/digital forensics on numerous skills levels (basic to expert/advanced levels). Since 2010, I have been the primary instructor for the Operating Systems and File System Forensics course at the University of Central Florida. I have also instructed portions of The Practice of Digital Forensics (CIS 6207) course in the past, and in 2020, I assumed the lead for the entire course. The course was rewritten from the ground up and modernized for your benefit!

Finally, I volunteered for the International Association of Computer Investigative Specialists (IACIS) from 2000 to 2015. I have served as a coach/mentor, regional manager, division administrator, and chairman in the IACIS Certification Committee. I served on the IACIS Board of Directors from 2009 to 2015 in the capacities of Director of Certification (2009-2010), Vice President (2010-2011), and Chairman of the Board (2011 to 2015). In 2015, I was honored with the prestigious designation as a Lifetime Member of IACIS. I have also developed course material and managed course development for IACIS. I led efforts to achieve accreditation as a certifying body, and in March of 2012, IACIS was approved by the Forensic Specialties Accreditation Board as an accredited certifying body, one of the first in the world.

Finally, if you are on LinkedIn, please consider connecting with your classmates and me. Networking and collaboration is key in the world of digital forensics.