The Practice of Digital Forensics (CIS 6207)
Spring 2023 Syllabus

Instructor:

Dan Purcell, MSDF
Daniel.Purcell@ucf.edu

Course Description:

The Practice of Digital Forensics course is designed to culminate key elements of the MSDF program as the capstone course for the program. The course will incorporate key learning objectives that will prepare students for a career in digital forensics, both as a practitioner and leadership roles within the discipline.

Prerequisites:

The Practice of Digital Forensics is the capstone course of the MSDF program. It is recommended that students take this course in their final year before graduation (no earlier). This course is required for graduation. *If you are majoring in another discipline and have not taken other computer or digital forensic courses at UCF, or you have no practical experience in this discipline, you should know from the onset that the 3rd assignment in this course is a forensic examination of digital evidence using forensic software (noted below).*

Course Overview:

This course is designed to cover the fundamental pillars of digital forensics. You can expect a course schedule that is enriching but also balanced to avoid "drinking through a firehose." The topics and schedule of this course are designed to progress logically beginning with the foundation of the forensic process and builds to court testimony. In fact, this course will also prepare you for management and leadership roles.

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, sometimes longer. You will have two weeks to listen to the lecture and complete assignment and required discussion topic posting. 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.

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.

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. Each assignment will require you to provide a written document with the exception of the forensic examination assignment.

- Understanding and applying the forensic process and terminology
- Understanding, creating, and validating policies
- Conducting a thorough forensic examination to achieve case objectives, identify evidentiary and exculpatory data, and properly apply forensic concepts and terminology.
- Creating a forensic report and conducting peer review for quality assurance
- Preparing for the judicial process and courtroom testimony
- Understand how to manage a digital forensics program and prepare budgetary documents
- Understanding and applying leadership concepts and principles throughout your career in digital forensics or a related discipline.

Required Text:

None

Computer and Software Requirements:

One of the assignments in this course requires you to perform a forensic examination of digital evidence, and therefore, you must have a computer that can run the software. The computer must be capable of running Windows 7 or higher. ***Windows 10 Pro or higher is preferred, so that you can examine BitLocker encrypted volumes.*** Your computer should have enough RAM to run forensic applications within Windows 7 (or higher) or the OS of your choosing. You will need a word processing application like Microsoft Word for some assignments and the ability to save it in PDF format. You must have at least 10 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 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! UCF provides Forensic Explorer (FEX) to all MSDF students or students enrolled in the MSDF courses under a different major or minor. Please see the information below on FEX and other forensic tools.

- 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

- 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

- Arsenal Image Mounter may be helpful for our forensic examination assignment. https://arsenalrecon.com/downloads/

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. 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 unless there is a qualified emergency or unforeseen situation.** 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 me 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 or direct on this topic. 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. Please know that this is a group learning environment, and your input is valued. If you see a question from your fellow student, answer it! Don't count on me to answer every question. 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 dpurcell@eecs.ucf.edu. I will respond to discussion questions and email within a reasonable amount of time. Please keep in mind that I have a fulltime job, and I do not work fulltime for UCF. 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. Although no books are required for this course, I will accompany each assignment with applicable publications or links. If the assignment requires you to conduct a forensic examination, I will provide the forensic image file in both E01 and DD formats (EnCase Evidence File format and a raw disk image). Discussion topics will be posted at the same time or during the assignment period. As stated previously, you will have a minimum of two weeks to complete each assignment.

1. Assignment #1: In this assignment, we will review the entire forensic process to include the seizure of evidence, preserving evidence, forensic media sterilization, acquiring evidence, examining media, analyzing data, interpreting results, and presenting your findings. Additionally, we will explore forensic terminology that examiners must be familiar with. The assignment will entail a scenario in which you will apply the forensic process and answer a series of questions.

2. Assignment #2: In this assignment, we will evaluate the purpose, structure, and major components of a policy. You will create a policy on a given topic related to digital forensic. We will also review the purpose and process of validating policy and building validation language into policy statements and associated procedures.

3. Assignment #3: In this assignment, you will conduct a forensic examination, based on a scenario, where we will review physical and logical disk structures, file systems, metadata, user artifacts, and other notable topics. This assignment will require you to examine a forensic image file and answer specific questions about your examination. ***NOTE: This assignment requires a Windows 10 or higher PC and forensic software (Forensic Explorer, FTK Imager, Autopsy, Arsenal Image Mounter, etc.).***

4. Assignment #4: In this assignment, you will create a forensic report that stems from Assignment #3. Your report will contain the essential elements of a forensic report to include the seizure of evidence, preservation of evidence, acquiring evidentiary media, examining data, analyzing data, providing and interpreting results, and presenting your findings. Details will be provided in the assignment directions.

5. Assignment #5: Based on the scenario presented in Assignment #3 that builds into Assignment #4, you will prepare an outline for trial preparation and testimony. Your examination notes, reports, and learning objectives from the lecture for this assignment will all come together to prepare you for trial and testimony. In addition, you will prepare a curriculum vitae (CV) as part of the assignment.

6. Assignment #6: In this assignment, we will focus on how to manage a digital forensics program and what you need to be mindful of as a supervisor or manager. You will write a paper on justifying a digital forensics program or program enhancement, to include budget preparation and management.

7. Assignment #7: During this assignment period, we will explore a number of leadership topics to prepare you for leadership roles in an organization and in the field of digital forensics. The assignment will focus on leadership strategies for advancing a digital forensics program and leading people.

I will provide thorough directions for each assignment, and you will either submit them through the Assignments or Quizzes area in Webcourses.

Discussions:

At the onset of the assignment period, a new discussion topic will appear for the assignment period. A range of modern topics related to digital forensics, cyber security, e-discovery, and modern technology will be provided. You will be required to provide a response to question(s) posed or discuss the topic as outlined. Examples may include legal cases, encryption, wireless technology, networking, hardware or software technology, leadership and management, etc.

Tests/Quizzes/Exams:

Each assignment is graded on a scale of 0-100, and the assignments account for 70% of your grade. During each assignment period, you will provide a written response to a specific topic in the discussion area of Webcourses for your classmates to view. Each post is graded as complete or incomplete. Complete means that you provided an adequate response to the prescribed topic that is written well, objective, substantive, and submitted by the deadline. Incomplete means you failed to meet the requisite expectations or did not answer at all by the deadline. As long as you satisfactorily complete each required discussion (including the intro during week one), you can achieve a maximum score that accounts for the remaining 30% of your grade.

Grading Policies:		**Grading Scale:**			
Requirement	Weight	90 - 100 =	A	60 - 60.99 =	D
Assignments	70%	80 - 89.99 =	B	0 - 59.99 =	F
Class Discussions & Participation	30%	70 - 79.99 =	C		

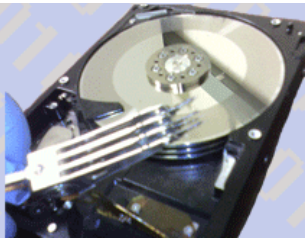
Notable Dates:

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

(This area intentionally left blank)

Master of Science in Digital Forensics

An Interdisciplinary Program at UCF

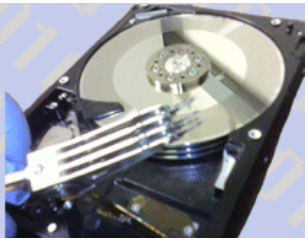


General Course Schedule

Week	Dates	Topic	Readings	Assignment	Due By
1	1/9/2023 – 1/15/2023	Course Introduction	Course Syllabus	Class familiarization & student introduction discussion post	1/15/2023
2	1/16/2023 – 1/29/2023	The Forensic Process & Terminology	Assorted in Assignment	Listen to lecture & complete Assignment #1 + Discussion Topic **Enter Answers in Quiz Module**	1/29/2023
3	1/16/2023 – 1/29/2023	The Forensic Process & Terminology	Assorted in Assignment	Listen to lecture & complete Assignment #1 + Discussion Topic **Enter Answers in Quiz Module**	1/29/2023
4	1/30/2023 – 2/12/2023	Policy Creation & Validation	Assorted in Assignment	Listen to lecture & complete Assignment #2 + Discussion Topic	2/12/2023
5	1/30/2023 – 2/12/2023	Policy Creation & Validation	Assorted in Assignment	Listen to lecture & complete Assignment #2 + Discussion Topic	2/12/2023
6	2/13/2023 – 3/5/2023	Forensic Examinations	Assorted in Assignment	Listen to lecture & complete Assignment #3 + Discussion Topic **Enter Answers in Quiz Module**	3/5/2023
7	2/13/2023 – 3/5/2023	Forensic Examinations	Assorted in Assignment	Listen to lecture & complete Assignment #3 + Discussion Topic **Enter Answers in Quiz Module**	3/5/2023
8	2/13/2023 – 3/5/2023	Forensic Examinations	Assorted in Assignment	Listen to lecture & complete Assignment #3 + Discussion Topic **Enter Answers in Quiz Module**	3/5/2023
9	3/6/2023 – 3/19/2023	Forensic Reporting & Peer Review	Assorted in Assignment	Listen to lecture & complete Assignment #4 + Discussion Topic	3/19/2023
10	3/6/2023 – 3/19/2023	Forensic Reporting & Peer Review	Assorted in Assignment	Listen to lecture & complete Assignment #4 + Discussion Topic	3/19/2023
11	3/20/2023 – 4/2/2023	Court Preparation & Testimony	Assorted in Assignment	Listen to lecture & complete Assignment #5 + Discussion Topic	4/2/2023
12	3/20/2023 – 4/2/2023	Court Preparation & Testimony	Assorted in Assignment	Listen to lecture & complete Assignment #5 + Discussion Topic	4/2/2023
13	4/3/2023 – 4/16/2023	Budgeting & Managing the D.F. Program	Assorted in Assignment	Listen to lecture & complete Assignment #6 + Discussion Topic	4/16/2023
14	4/3/2023 – 4/16/2023	Budgeting & Managing the D.F. Program	Assorted in Assignment	Listen to lecture & complete Assignment #6 + Discussion Topic	4/16/2023
15	4/17/2023 – 4/30/2023	Leadership in Digital Forensics	Assorted in Assignment	Listen to lecture & complete Assignment #7 + Discussion Topic	4/30/2023
16	4/17/2023 – 4/30/2023	Leadership in Digital Forensics	Assorted in Assignment	Listen to lecture & complete Assignment #7 + Discussion Topic	4/30/2023

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.