DIGITAL FORENSICS
INFORMATION ASSURANCE

COURSE SYLLABUS
DFIA 467- Mobile Device Forensics
CRN: 1906-4 CR HRS.

Instructor:	Prof. Josh Brunty *CCME, CCTI, CCO, CCPA*	**Class Meets:**	MWF 11:00-11:50AM W 12:00-12:50PM (LAB)
Office:	WAEC 2001	**Classroom:**	WAEC 1232
Phone:	304-696-5602	**Office Hours:**	MWF 10:00-11:00AM
Email:	josh.brunty@marshall.edu		TR 9:30-11:00AM

Course Description (from catalog):

Identification, preservation, collection, analysis, and reporting techniques and tools used in the forensic examination of mobile devices such as cell phones and GPS units.

More Description:

This three (4) credit hour Mobile Device Forensics course (CRN #1906), through lecture, demonstration, and practical “hands-on” training, is designed to provide students theories and practices of identification, preservation, collection, analysis, and reporting techniques and tools used in the forensic examination of mobile devices such as cell phones and GPS units.

Course Format:

This Mobile Device Forensics course will meet every MWF from 11:00am-11:50am and Wednesday from 12:00-12:50pm (LAB) in the Weisberg Applied Engineering Complex (WAEC) Room 1232 (Digital Forensics Laboratory). The class will consist of lecture/demonstration with accompanying labs and/or exercises.

Students will be given multiple in-class, instructor-led lab exercises that focus on a variety of mobile forensic methodologies. Students will also complete various out-of-class end of module practical laboratory exercises throughout the course of the semester.

The Cellebrite Certified Operator (CCO) portion of the course aims to teach data extraction team members such as technically savvy investigators, digital forensic examiners, IT staff, internal affairs investigators, first responders, and personnel designated to handle extraction of digital evidence how to perform extractions on a variety of devices. These extractions include logical, file system and physical extractions from mobile devices as well SIM cards, and external storage such as SD cards. Students will gain a basic understanding of how to open the extractions in Physical Analyzer software, conduct basic searches and how to create bookmarks and reports. The Cellebrite Certified Physical Analyst (CCPA) portion of course designed for technically savvy investigators, digital evidence analysts and forensic practitioners. As this course focuses on the analysis and advanced search techniques using UFED Physical Analyzer, participants will not be conducting extractions from devices in this course. UFED Physical Analyzer software will be used extensively to explore recovered deleted data, database contents, advanced search and analysis techniques, verification and validation, and reporting.

For this portion of the course there will be a number of in-class and out-of-class, hands-on laboratory exercises completed by the student. At the conclusion of the semester you will sit for the CCO certification exam as your final examination. You must earn an 80% or better to earn the CCO credential. You will have one (1) attempt to pass the exam.

Required Texts, Additional Reading, & Other Materials:

- Required Texts:
  - UFED Student Lab Kit (F-UFD-04-008) Edition: N/A. Available from MU Bookstore
- Students will need to create Tophat user account and purchase a Tophat subscription plan for use within this course. Subscription plans vary from 4 month access, semester access, to lifetime access. Tophat can either be purchased online or through MU Bookstore. Tophat will be used to track attendance, class quizzes, reviews, etc. The join code for this course is 409478 and the course homepage is https://app.tophat.com/e/409478 Tophat can be used from either a PC or via the Android/iOS app on a mobile device. Students can also text-in answers to +1 (315) 636-0905 via SMS. This is ideal for poor wifi or older mobile devices.
- Assigned readings and laboratory exercises are an essential component of this course and provide students with a baseline of knowledge that will be expanded upon through more detailed and complex in-class lectures and discussions. Students will be required to complete assigned readings prior to the class period in which the material will be discussed.
- Supplemental course materials (e.g., handouts, reading assignments, lab exercises, etc.) will be posted to the MUOnline http://www.marshall.edu/muonline

Desired Objectives/Outcomes:

This course is designed to build on the material learned in previous foundational courses and apply those concepts. This course places a strong emphasis on utilization of mobile forensic tools and techniques and hands on exercises to emphasize the procedures that students will utilize in the field when analyzing mobile devices. This course uses advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators.

In this course, learning outcomes are gauged as followed:

Course Student Learning Outcome	How Practiced in This Class	How Assessed in This Course
Explain and understand the underlying technology of mobile devices and wireless networks, emphasizing how the data they contain can be used as evidence.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)
Utilize and gain proficiency of specialized mobile forensic tools such as Cellebrite, and other mobile forensic software tools.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)

Understand core forensic methodology as it relates to mobile devices. Understand proper evidence handling procedures for mobile devices	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)
Be able to create physical and logical acquisitions of various mobile devices.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)
Be able to extract data from SIM cards in a forensically sound manner	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)
Understand the underlying technologies and be able to extract data from various mobile operating systems and platforms such as Android & iOS	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class & Out-of-Class Laboratory Exercises, CCO Certification (Final Exam)
Students will be confident in analyzing and examining digital evidence that will stand up to standards required for criminal and/or civil cases.	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, CCO Certification (Final Exam)
Students will obtain knowledge that will allow successful completion of field-recognized certifications (i.e. Cellebrite Certified Operator-CCO, and Cellebrite Certified Physical Analyst- CCPA)	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, CCO Certification (Final Exam)

University Policies:

By enrolling in this course, you agree to the University Policies listed below. Please read the full text of each policy by going to www.marshall.edu/academic-affairs and clicking on "Marshall University Policies." Or, you can access the policies directly by going to http://www.marshall.edu/academic-affairs/policies/

Academic Dishonesty/ Excused Absence Policy for Undergraduates/ Computing Services Acceptable Use/ Inclement Weather/ Dead Week/ Students with Disabilities/ Academic Forgiveness/ Academic Probation and Suspension/ Academic Rights and Responsibilities of Students/ Affirmative Action/ Sexual Harassment

Attendance Policy and Make-up Work:

Attendance is REQUIRED for this course. Students must attend 90% of class sessions to be allowed to sit for the CCO examination. There will be NO EXCEPTIONS whatsoever to this rule. This class is predominately lab and project based, with a good majority of our time devoted to class time computer work and hands-on tutorials with forensic tools and other plugins that are only available in the laboratory environment. With that said, any missed classes will put the student behind, and make it difficult to pick up with the next class lessons. However, in the event that you MUST miss class, it is the student's responsibility to meet with the instructor to discuss absences due to illness or other reasons. Any excused absences must adhere to the University's excused absence policy.

Regular attendance in this class is crucial to your success as a student. The only way to benefit from class discussions and hands-on learning activities is to be here. Being present and on time for all class meetings is expected. Period. The following is the attendance policy of the DFIA program:

Excused Absences:

- University-sponsored academic activities (performing arts, debate and individual events, honors classes, ROTC); official athletic events; other university activities (student government).
- Student Illness or Critical Illness/Death in the Immediate Family:" Immediate Family" is defined as a spouse/life partner, child, parent, legal guardian, sibling, grandparent or grand- child. **Routine doctor appointments are not excused. Appointments should be scheduled around your classes.*
- Short-Term Military Obligation
- Jury Duty or Subpoena for Court Appearance
- Religious Holidays

Student's Responsibility:

- Provide appropriate documentation to Dean of Student Affairs for excused absence. Learn how the process works here: http://www.marshall.edu/student-affairs/excused-absence-form/
- Request opportunity to complete missed work immediately upon return to class**.**
- Be aware that excessive absences—whether excused or unexcused—may affect your ability to earn a passing grade.
- Regardless of the nature of the excused absence, you are responsible for completing all coursework prior to the end of the semester.

Unexcused Absences:

- If you miss two classes, I will issue a warning.
- If you miss a third class: You will receive an automatic one letter grade deduction in the course.
- We will conference to discuss your standing and develop a plan of improvement. If you meet its criteria, you may have the chance to earn back the letter grade deduction.
- If you miss a fourth class, the previous letter grade deduction stands, regardless of improvement plan results. Subsequent missed classes will result in an additional letter grade deduction for each absence

Assignment Submission & Late Policy:

The course includes a number of projects and assignments. All assignments are due on their due date and must be submitted through via MUOnline (unless otherwise noted by the instructor). NO LATE ASSIGNMENTS WILL BE ACCEPTED. Please do not procrastinate in working on your assignments or trying to submit through MUOnline as many others have done in the past. If you wait until the last night to start on the project or the last minute to submit, chances are, you will fail. Most Laboratory Projects are due by Friday @ 11:59PM

All electronic submissions MUST follow this file naming convention:
DFIA467_LastName_FirstInitial_Assignment Name.extension.
("DFIA467_brunty_j_project1.ext")

Assignments must be submitted in the format specified by the instructor for a given assignment. I WILL NOT accept projects submitted in non-approved formats or naming conventions.

Course Requirements & Grading Policy:

Student materials and grades will be returned as soon as graded to the student and can be viewed via MUOnline. Should you wish to appeal a grade, test question, etc, you need to follow this procedure. You should send an email via MUOnline to the Graduate Assistant and CC me. The title of the email must read "GRADE APPEAL – Assignment Name" (i.e. Lab Project 1, Exam 1, etc). The body of the email must include the question, question number, your answer, and why you think you deserve credit. For tests and quizzes in MUOnline, this should be done immediately after completion, before you leave class. You can copy and paste this information to make things simple. I will get back to you as soon as possible.

Students will be evaluated in this course based on their performance in the following categories:

Attendance & In-Class Quizzes (25%)- Attendance will be taken each day of class via Tophat. It is the student's responsibility to make sure that the sheet is signed. Each class will be worth five (5) points. and will be calculated as a score at the end of the semester. Any in-class quizzes given by the instructor via Tophat will also factor into this percentage calculation.

In-Class & Out-of-Class Laboratory Exercises (25%) – During both the CCO & CCPA portion of the course there will be a number of hands-on lab exercises that we will work on both in-class and out-of-class. The due dates for these labs will be announced each week & will be distributed via and due via MUOnline

Final Exam- (50%) – This final exam will cover the proficiency gained from the Cellebrite Certified Logical Operator (CCO) portion of the course. A score of 80% or better is required to obtain the CCO credential, however you will be graded for the course on your raw score on this exam. You will only have one (1) attempt at this exam. The date of the CCO can be found in the course schedule below. You must attend 90% of classes over the course of the semester in order to sit for the CCO certification (no exceptions).

The above categories will be graded as follows:

Attendance/In-Class Quizzes	25%
CCO & CCPA Laboratory Exercises	25%
CCO Examination (Final)	50%
Total	**100%**

This class will employ a weighted grading system. To determine your grade in this course, fill in your percentage score for each evaluation category below, multiply each score by its weight, and then add the values in the final grade column to find your overall grade out of 100. In addition to handing graded assignments back to you in class, I will post grades for individual assignments and exams on blackboard. However, please remember that you **must** use the weighted grading system shown below to determine an accurate portrayal of your overall course grade. I am happy to meet with you to discuss your course progress/grade during office hours throughout the semester.

Evaluation Category	**Your Score (Out of 100)**	**Weight**	**Contribution to Final Grade**
Attendance/Quizzes (average)		X .25 =	
CCO & CCPA Laboratory Exercises (average)		X .25 =	
CCO Exam (Final)		X .50 =	
Final letter grades are calculated using the following scale: 90-100 A 80-89 B 70-79 C 60-69 D Below 60 F		**Final Grade (out of 100)**	

There will be a number of out-of-class labs and hands-on assignments as part of this course. In addition, extra practice and competency with both the hardware & software used in the course will ensure a respectable grade on your final CCO certification exam. As such, you will be given card access to the Digital Forensics Laboratory (WAEC 1232) to work on assignments and practice labs when classes aren't in session. Open lab schedules will be posted during the first or second week of classes. If you do not have an RFID-enabled access card you can obtain your first one free-of-charge from the campus ID office located on the first floor of Drinko Library . In addition, you will also need to complete the required COS IT Conduct form before the end of the first week of classes online by visiting http://www.marshall.edu/cosweb/agreements/?a=j3qw3 Usage of the computers and course files will not be permitted until the online form is completed.

Communication:

I will post course content on MUOnline (e.g., syllabus, assignments, readings, etc.), so be sure to check for new materials regularly. Your MU e-mail address will be used to make any general announcements, last minute schedule changes, etc. I recommend that you monitor your MU email and MUOnline accounts at least once a day. Also, I will only respond to emails that you send me from your official MU email address – it is the only way for me to be sure that I am

responding to you (and not someone else pretending to be you).

Classroom Learning Environment:

To foster the best possible environment for learning, we will follow "Brunty's Maxims" They are as follows:

- ✓ *Don't Lie…*
- ✓ *Don't Cheat…*
- ✓ *Don't Steal…*
- ✓ *Don't play on your cellphone unless directed to do so.*
- ✓ *Don't have conversations that distract the class.*
- ✓ *Don't disparage other students- Treat everyone with respect.*
- ✓ *Don't be late for class*
- ✓ *ALWAYS be professional. Take advantage of your time here. Ask questions. Participate.*

Students who violate these maxims will be asked to leave class.

Course Schedule and Due Dates:

NOTE: This is a tentative schedule and it may change as the class progresses. Due dates, Lab Projects, etc. are listed in the notes section**.**

Date	Day	Topic	Notes
8/21	M	Module 0 (Course Introduction)	
8/23	W	CCO Module 1 (Introduction)	
8/25	F	CCO Module 1 (Introduction)	
8/28	M	CCO Module 2 (Forensic Handling)	
8/30	W	CCO Module 2 (Forensic Handling)	
9/1	F	CCO Module 2 (Forensic Handling)	
9/4	M	**No Class- Labor Day Holiday**	
9/6	W	CCO Module 3 (UFED Touch/4PC)	
9/8	F	CCO Module 3 (UFED Touch/4PC)	
9/11	M	CCO Module 3 (UFED Touch/4PC)	
9/13	W	CCO Module 4 (Extraction Methodology)	
9/15	F	CCO Module 4 (Extraction Methodology)	
9/18	M	**No Class- Out for Conference**	
9/20	W	**No Class- Out for Conference**	
9/22	F	CCO Module 4 (Extraction Methodology)	✓ Derbycon 7.0 (Louisville, KY 9/20-24
9/25	M	CCO Module 5 (Intro to Analysis)	
9/27	W	CCO Module 5 (Intro to Analysis)	

9/29	F	CCO Module 5 (Intro to Analysis)	
10/2	M	CCO Module 6 (Creating Reports)	
10/4	W	CCO Module 6 (Creating Reports)	
10/6	F	CCO Module 6 (Creating Reports)	✓ All CCO Labs DUE via 10/6 @ 11:59PM via MUOnline
10/9	M	CCPA Module 2 (Physical Analyzer Overview)	
10/11	W	CCPA Module 2 (Physical Analyzer Overview)	
10/13	F	CCPA Module 2 (Physical Analyzer Overview)	
10/16	M	CCPA Module 3 (Android Overview)	✓ Android Lab (MUOnline)
10/18	W	CCPA Module 3 (Android Overview)	
10/20	F	CCPA Module 3 (Android Overview)	
10/23	M	CCPA Module 4 (iOS Overview)	✓ iOS Lab (MUOnline)
10/25	W	CCPA Module 4 (iOS Overview)	
10/27	F	CCPA Module 4 (iOS Overview)	
10/30	M	CCPA Module 5 (Analysis)	
11/1	W	CCPA Module 5 (Analysis)	
11/3	F	CCPA Module 5 (Analysis)	
11/6	M	CCPA Module 6 (SQLite Wizard)	
11/8	W	CCPA Module 6 (SQLite Wizard)	
11/10	F	CCPA Module 6 (SQLite Wizard)	
11/13	M	CCPA Module 7 (Verification & Validation)	
11/15	W	CCPA Module 7 (Verification & Validation)	
11/17	F	CCPA Module 7 (Verification & Validation)	✓ Hackercon/SecureWV 11/17-19 (Charleston, WV)
11/20	M	**No Class- Thanksgiving Holiday**	
11/22	W	**No Class- Thanksgiving Holiday**	
11/24	F	**No Class- Thanksgiving Holiday**	
11/27	M	CCPA Module 8 (Plug-in Chains)	
11/29	W	CCPA Module 8 (Plug-in Chains)	
12/1	F	CCPA Module 8 (Plug-in Chains)	✓ All CCPA Labs DUE via 12/1 @ 11:59PM via MUOnline
12/4	M	**No Class- Instructor Travel**	
12/6	W	CCPA Module 9 (Reporting)	
12/8	F	Final Exam (CCO) Review Session	
12/12	T	**Final CCO Exam (10:15AM-12:15PM)**	