

Professor		
<p>Professor Josh Brunty Office: Weisberg Applied Engineering Complex (WAEC) 2001 Office Phone: 304-696-5602 (takes messages) Dept. Fax: 304-696-6533 Email: josh.brunty@marshall.edu Office Hours: MWF 8:00-9:00AM, TR 9:30AM-11:00AM Twitter: @joshbrunty @MuDigForensics Facebook: Marshall Digital Forensics & Information Assurance</p>		
Required Text(s)		
<p>Cellebrite UFED Student Lab Kit (F-UFD-04-008) ISBN: N/A. Available for sale from Marshall University Bookstore only: http://goo.gl/0ErXLu</p>		
Recommended Texts		
<p>**Additional reading/hardware materials will be provided by the instructor via handout/MUOnline</p>		
Resource Sites		
<p>http://www.cellebrite.com (Information on Cellebrite UFED Devices) https://www.cellebritelearningcenter.com (Cellebrite Learning Center Portal)</p>		
Course Description		
<p>This three (4) credit hour Mobile Device Forensics course (CRN #2624), 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.</p>		
Prerequisites		
<p>IST 261- Intro to Linux (Recommended) IST 264- Technology Foundations IST 449- Data Recovery & Analysis</p>		
Computer Requirements		
<p>Students will be required to complete assignments using Cellebrite UFED & Physical Analyzer, and other Linux command line utilities (i.e. Python).</p> <p>All students are responsible for knowing the University Computing Services’ Acceptable Use Policy available at http://goo.gl/W92DUa</p> <p>Students will receive emails via Marshall email (Please setup your Marshall account(s) if you have not done so). E-mail will be used to make any general announcements, last minute changes, etc. It is mandatory that you monitor both your email at least once a day. PLEASE ONLY USE MY MARSHALL EMAIL ADDRESS FOR QUICK CORRESPONDENCE. Messages left on MUOnline or any other social media may result in delayed responses.</p>		
Course Objectives/Outcomes		
<p>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.</p>		
<p>Upon completion of the Mobile Device Forensics course, students will be able to:</p>		
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 Laboratory Exercises, Midterm Exam, Final Exam
Utilize and gain proficiency of specialized mobile forensic tools	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module

such as Cellebrite, and other mobile forensic software tools.		Exercises, In-Class Laboratory Exercises, Midterm Exam, 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 Laboratory Exercises, Midterm Exam, 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 Laboratory Exercises, Midterm Exam, 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 Laboratory Exercises, Midterm Exam, Final Exam
Understand the underlying technologies and be able to extract data from various mobile operating systems and platforms such as Android, iOS, Blackberry, Nokia, Windows Mobile, and GPS Devices	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, 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, Midterm Exam, Final Exam
Students will obtain knowledge that will allow successful completion of field-recognized certifications (i.e. Cellebrite Certified Logical Operator-CCLO, and Cellebrite Certified Physical Analyst- CCPA)	In-class lecture & hands on laboratory exercises.	Classroom Discussion, End of Module Exercises, In-Class Laboratory Exercises, Midterm Exam, Final Exam
<p>This Mobile Device Forensics course will meet every MWF from 11:00am-11:50am and W from 12:12:50PM 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.</p> <p>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 semester.</p> <p>Students will sit for the both the Cellebrite Certified Logical Operator (CCLO) and Cellebrite Certified Physical Analyst Certification (CCPA) exams. The Cellebrite Certified Logical Operator (CCLO) Course is designed for the first responder and the basic to intermediate investigator / examiner. This portion of course exposes students to the fundamentals of mobile device investigations, logical extraction of user data, and analysis of mobile devices. Operation of the Cellebrite UFED product to perform a number of hands-on logical extractions on various mobile devices with a variety of operating systems is a key component of this class. Skill sets also include creating Safety SIMs and extracting evidentiary data from SIM cards. Participants also create reports on findings and are exposed to the free UFED Reader and</p>		

how to use that to multiply investigative efforts. The score obtained in this examination will count towards your midterm exam grade (Exam #1). You must earn an 80% or better to earn the CCLO credentials. You will have one (1) attempt to pass the exam. The Cellebrite Certified Physical Analyst (CCPA) Course is designed for the intermediate and advanced investigator / digital forensic examiner. This portion of the course focuses on the use of Cellebrite's UFED to perform file system extractions, physical extractions, password bypasses and the advanced analysis of evidentiary items using the UFED Physical Analyzer software. The score obtained in this examination will count towards your final exam grade (Exam #2). You must obtain an 80% or better on the exam to earn CCPA credentials. You will have one (1) attempt to pass the exam.

Lectures and course materials will be available from MUOnline as they become available. You can log into the course website using your MU student ID at the following address: www.marshall.edu/muonline

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/?page_id=802

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

Professionalism/Attendance Policy

Attendance is REQUIRED for this course. Students must attend 90% of class sessions in the CCLO and CCPA portion of the course to be allowed to sit for the 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 result in lost points (5 points per class), 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.

Instructor Contact & Social Media Policy

You are welcome to follow me on Twitter (@joshbrunty) and/or join my network on LinkedIn. You can also follow our department through our MU Digital Forensics or MU Forensics Facebook group pages. For class-related questions, however, please email me (no DM's, Snaps, etc.). You are also encouraged to stop by my office. Please note, however, that I rarely answer or walk you through lab-related questions via email. In these circumstances, you are encouraged to stop by my office during posted office hours and/or make an appointment.

Inclement Weather Policy

Students can find information concerning Marshall's policy regarding inclement weather regarding inclement weather online via <http://www.marshall.edu/ucomm/weather.html>. Please note that a two-hour delay means that classes that begin at 10:00 a.m. begin on time. Classes that begin at 8:30 a.m. meet at 10:00 a.m. and continue for the remaining period of that class.

Project Submission Guidelines

The course includes a number of laboratory projects. All laboratory projects 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. These assignments will usually be distributed and due on Thursdays (lab days). Please see the instructor if extenuating circumstances exist that may merit an extension or modification of the assignment. 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.

All electronic submissions MUST follow this file naming convention:

IST467_LastName_FirstInitial_Assignment Name.doc ("IST467_brunty_j_project1.doc")

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.

Assignments & projects must convey information in a clear, concise, and technical matter; hence obvious grammatical mistakes will be deducted. Projects will be available for download & submitted via MUOnline unless otherwise noted by the instructor.

All course assignments will:

- 1) Be completed on time
- 2) Meet guidelines and scoring rubrics for the assignment

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. GREP Quiz, 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.

Final letter grades will be based on the following scale:

90-100	A
80-89	B
70-79	C
60-69	D
0-59	F

Percentage of grades will be distributed as follows:

Attendance/In-Class Labs	20%
End-of-Module Exercises	20%
Exam #1- CCLO	30%
Exam #2- CCPA	30%

Example:

Attendance/In-Class Labs (86%)	x .20 = 17.2
End-of-Module Exercises (86%)	x .20 = 17.2
Exam #1- CCLO (91%)	x .30 = 27.3
Exam #2- CCPA (84%)	x .30 = 25.2

	86.9 (87% B)

Attendance/In-Class Labs (20%)

Students must attend 90% of class sessions in the CCLO and CCPA portion of the course to be allowed to sit for the examination. Each class is worth five (5) points and will be totaled twice; once before the CCLO examination and once before the CCPA examination. We will also be working through various instructor-led labs throughout each module of the course. Lack of participation (i.e. cutting out early, being disruptive/disrespectful, or not working on labs) will result in a loss of points. These points can be given and taken away at the discretion of the professor. Merely showing up to class does not guarantee points for a given class session.

End-of-Module Exercises (20%)

Each CCLO and CCPA module includes end-of-module questions and discussion. These can generally be completed out-of-class with the respectable modules (CCLO & CCPA) due the week of each exam. Exact dates can be found in both the course schedule below and MUOnline. No late submissions will be accepted.

Exam #1- CCLO (30%)

This exam will cover the proficiency gained from the Cellebrite Certified Logical Operator (CCLO) portion of the course. A score of 80% or better is required to obtain the CCLO credential, however you will be graded on your raw score on this exam. You will only have one (1) attempt at this exam. The date of the CCLO can be found in the course schedule below (*cont. on next page*)

Exam #1- CCPA (30%)

This exam will cover the proficiency gained from the Cellebrite Certified Physical Analyst (CCPA) portion of the course. A score of 80% or better is required to obtain the CCPA credential, however you will be graded on your raw score on this exam. You will only have one (1) attempt at this exam. The date of the CCPA can be found in the course schedule below. NOTE: This exam will be taken during finals week.

CLASS SCHEDULE	Marshall University Dates/ Important Dates/Notes	WEEK CLASS DATE
NOTE: When projects are assigned for a week, the due date will be reflected within the posted assignment via MUOnline. It is expected of the student to submit the project to MUOnline prior to the due date/cutoff time (which is usually the beginning of class). Failure to do so will result in a zero for the project. Please see the instructor if extenuating circumstances exist that may merit an extension or modification of the assignment. Late, incomplete or poorly organized assignments will result in point deductions. The following outline delineates the tentative class schedule with topics to be addressed during the course. Please note this is a tentative schedule and it may change upon class progress:		
Week 1 Module 0 & 1: Introduction to Mobile Device Forensics & CCLO		Aug 22-26
Week 2 CCLO - Module 2: Mobile Device Tech Overview		Aug 29-Sept 2
Week 3 CCLO - Module 3 Mobile Device Trends	✓ September 5 (Monday)- Labor Day- No Class	Sept 5-9
Week 4 CCLO - Module 4 Forensic Handling of Mobile Devices		Sept 12-16
Week 5 CCLO - Module 5 UFED Tech Overview		Sept 19-23
Week 6 CCLO - Module 5 UFED Tech Overview (Cont.)		Sept 26-30
Week 7 CCLO - Module 6 Logical Analyzer and Bookmarking		Oct 3-7
Week 8 CCLO Review Exam #1 (CCLO) CCPA - Module 1 Media System Files and Encoding	<ul style="list-style-type: none"> ✓ Monday October 10- CCLO Review ✓ Wednesday October 12 @ 11AM-Exam #1 (CCLO) ✓ Friday October 14 @ 11:59PM- CCLO Modules Due via MUOnline 	Oct 10-14
Week 9 CCPA - Module 1 Media System Files and Encoding (Cont.)		Oct 17-21
Week 10 CCPA - Module 2 UFED Overview	✓ Oct 28 (Friday)- Last day to drop a full semester individual course	Oct 24-28

Week 11 CCPA - Module 3 Physical Analyzer Overview		Oct 31-Nov 4
Week 12 CCPA - Module 4 Advanced Search Techniques		Nov 7-11
Week 13 CCPA - Module 5 Verification and Validation	✓ SecureWV/HackerCon (Nov 18-20)	Nov 14-18
Week 14 No Class	✓ Thanksgiving/Fall Break- 11/21-11/25	Nov 21-25
Week 15 CCPA - Module 6 Plug-in Chain Manager CCPA - Module 7 Reporting on Technical Findings		Nov 28-Dec 2
Week 16 CCPA - Module 8 UFED Reader	✓ Dead Week ✓ Friday December 9- CCPA Review ✓ Friday December 9 @ 11:59PM- CCPA Modules DUE via MUOnline	Dec 5-9
Week 17 Exam #2 (CCPA)	✓ Exam #2 (CCPA)- Tuesday December 13, 10:15AM- 12:15PM	Dec 12-16



cellebrite
 delivering mobile expertise



**Syllabus meets requirements set forth by MUBOG Policy AA-14*