FORENSIC SCIENCE

COURSE SYLLABUS
FSC 634- Comp Search & Seizure
CRN: 3273-3 CR HRS.
Spring 2023

Instructor:	Dr. Josh Brunty GASF, MCFE, CCME	**Class Meets:**	M 2:30PM-5:30PM
TA:	Christopher Vance MCFE		
Office:	Forensic Science Ctr. W200G	**Classroom:**	WAEC 2237
Phone:	304-691-8962	**Office Hours:**	M- 1:00-2:00PM WF- 10:00-11:00AM T & TR 9:30-11AM
Email	josh.brunty@marshall.edu Vance117@marshall.edu		Book a Meeting with Me

Course Description (from catalog):

Topics covered in this course will expand upon material covered in FSC 632. Additional areas include affidavits and warrants, national information security concepts, evidence collection, transport and preservation, computer networks, e-mail traces, imaging of original evidence, introduction to forensic tools, Window registry, malware and spyware, virtualization and handheld devices. Classes are presented in a lecture format and culminates with a mock, digital crime scene exercise.

Course Description (additional information):

This three (3) credit hour Computer Search & Seizure course (CRN #3273), 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.

Course Format:

This course will meet every Monday from 2:30-5:20PM in the Weisberg Applied Engineering Complex (WAEC) Room 2237 (Advanced Cyber Forensics & Security 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 techniques and methodologies. Additionally, students will also complete multiple practical assessments and a written assessment throughout the course of the semester.

Required Texts, Additional Reading, & Other Materials:

- Required Text:
  - None
- Recommended Texts:
  - Bair, J. *Seeking the Truth From Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations. 1st Ed*. November 13, 2017. Paperback ISBN: 9780128110560. eBook ISBN: 9780128110577 [Link].

- 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., slides, handouts, reading assignments, lab exercises/submissions, etc.) will be posted to Teams/OneDrive/Class Notebook. A course OneDrive link has also been setup at: http://bit.ly/mobile-device-forensics-onedrive This OneDrive link contains course-related software & files.

- Specialized forensic software & equipment will be available only on the machines in WAEC 2237 (Advanced Cyber Forensics & Security Laboratory).

- Each student will also be supplied with a mobile forensic hardware & equipment kit with materials necessary to complete the course. This kit is to stay in laboratory at ALL TIMES and cannot be checked out, although you will have access to the kit outside of normal class times.

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. To accomplish this, the course is broken down into 3 separate parts: *Part I- Foundational Concepts, Part II- Intermediate Concepts, and Part III- Advanced Concepts.*

Course Student Learning Outcome	How Practiced in This Class	How Assessed in This Course
Fundamental Concepts (CO1) Students will understand and explain the underlying fundamental concepts & technologies of mobile device forensics and how they are utilized in digital forensics.	In-class lecture, classroom discussion, & hands on laboratory exercises.	• In-class Lab & Exercises
Intermediate Concepts (CO2)	In-class lecture, classroom discussion, &	• iOS & Android Practical

Students will analyze and apply intermediate concepts knowledge and how they relate to mobile forensics examinations. Students will understand various encoding techniques found within mobile devices and how to decode them, in addition to decoding application data, and how to conduct and testify on advanced validation.	hands on laboratory exercises.	
Advanced Concepts (CO3) Students will understand how to perform advanced-level application analysis, as it applies to both iOS and Android devices	In-class lecture, classroom discussion, & hands on laboratory exercises.	• Final Project- Application Analysis • Final Project Presentation

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:

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. Attendance and discussion questions will be given prior to every class period utilizing PollEverywhere. Being present and on time for all class meetings is expected. Period. Excused absences include: 1) University-sponsored academic activities (performing arts, debate and individual events, honors classes, ROTC); official athletic events; other university activities (student government). 2) 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. 3) Short-Term Military Obligation. 4) Jury Duty or Subpoena for Court Appearance and 5) Religious Holidays. It is the student's responsibility to provide appropriate documentation to Dean of Student Affairs or the instruction for excused absence. Learn how the process works here: http://www.marshall.edu/student-affairs/excused-absence-form/ The student should also 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.

It is the student's responsibility to complete a Marshall University Forensic Science Program Excused Absence Form if an absence is incurred (or anticipated). Because this course is an interactive class, students who miss class due to University-excused activities will be provided with an alternative assignment that connects to the activities in the missed class session.

Assignment Submission & Late Policy:

This course includes a number of projects and assignments. All assignments are due on their due date and must be submitted through via Teams (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 Teams 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 out-of-class laboratory projects and practical assessments are due on Fridays @ 11:59PM

All electronic submissions MUST follow this file naming convention:
FSC634_LastName_FirstInitial_Assignment Name.extension. ("FSC634_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 Teams. Should you wish to appeal a grade, test question, etc, you need to follow this procedure. You should send an email to 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 Teams, 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 Labs Quizzes (40%)- Attendance will be each class period. It is the student's responsibility to make sure that they enter the appropriate attendance code. The student will also complete multiple in-class, instructor led labs and exercises throughout the course of the semester. Attendance & in-class quizzes and labs/exercises are calculated as total points and converted to "out of 100" a score at the end of the semester.

Out of Class Lab Exercises/Assessments (30%) – During the course of the semester you will complete five (5) assessments, 4 practical and 1 written, that will assess the various techniques you learn throughout the course. These will involve the proper triage, extraction, and forensic examination of iOS and Android devices.

Final Project (40%)- Each student will choose an application to perform a full forensic analysis and application deconstruction upon. In addition to performing a write-up report on the chosen application, the student will also present such findings to the class. The schedule and due dates of this final project can be found in the course schedule below.

The above categories will be graded as follows:

Attendance/In-Class Labs	40%
Out of Class Lab Exercises/Assessments	30%
Final Project	30%
Total	**100%**

Evaluation Category	**Your Score (Total Score)**	**Weight**	**Contribution to Final Grade**
Attendance/In-Class Labs & Quizzes		X .40 =	
Out of Class Labs/Assessments		X .30 =	
Final Project		X .30 =	
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)**	

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.

There will be a number of out-of-class labs and hands-on assignments as part of this course. As such, you will be given 24/7 access privileges 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. You can also visit the ID office to enable RFID access on a companion mobile device (i.e. Apple Watch or iPhone) if compatible. 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 https://netapps.marshall.edu/cosweb/agreements/?a=cositconduct. Usage of the computers and course files will not be permitted until the online form is completed.

Communication:

I will post course content to the course Blackboard and the course OneDrive (e.g., syllabus, assignments, readings, lectures, 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 the course Teams page 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). You will also have the ability to chat with other classmates, setup meetings, etc. via the course Teams page as well.

If you need to schedule an office-hours appointment with me (career guidance, help with lab projects, etc.) you can stop by during my office hours or you can schedule an appointment with me anytime by visiting my Bookings page HERE.

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 and/or classes are cancelled. Lab Projects, etc. are listed in the notes section. The official MU Academic Calendar can be found at: https://www.marshall.edu/academic-calendar/

Week/Date	Readings/Activities/Assignments
Week 1 **1/8** **Introduction to Mobile Forensics & Evidence Handling**	**Readings** • Bair Ch. 1-Defining Cell Phone Forensics & Standards (pp. 3-13) • Bair Ch. 2- Evidence Contamination & Faraday Methods • SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition • NIST 800-101 R1- Guidelines on Mobile Device Forensics • Validation of Forensic Tools, Software, & Methods- A Primer for the Digital Forensics Examiner

	Activities • Distribute Mobile Device Lab Kits • Reset/Populate Mobile Devices • Complete Lab Safety & COS IT conduct forms
Week 2 **1/15** **No Class- MLK Day**	
Week 3 **1/22** **Intro to Cellular Networks, Mobile Device Identification, Triaging, & Logical Extraction**	**Readings** • Bair Ch. 5- The Cellular Network (pp. 55-70) • Bair Ch. 7- Device Identification (pp. 87-101) • Bair Ch. 8- Triaging Evidence (pp. 103-117) • Bair Ch. 9- The Logical Examination (pp. 119-139) • Bair Ch. 10- Troubleshooting Logical Examinations- (pp. 141-153) • Bair Ch. 11- Manual Examinations (pp. 155-166) **Activities** • Introduction to Cellebrite UFED / Magnet AXIOM • Logical & Filesystem Extraction- Feature Phone & Smartphone (in-class)
Week 4 **1/29** **Subscriber Identity Module (SIM) Forensics & Forensic Report Writing**	**Readings** • Bair Ch. 6- Subscriber Identity Module (pp. 71-85) • Bair Ch. 12- Report Writing (pp. 167-183) • Writing DFIR Reports: A Primer **Activities** • SIM Extraction Lab (in-class) • SD Card Extraction (in-class)
Week 5 **2/5** **Understanding the Mobile Landscape & Mobile Device Encryption**	**Readings** • None **Activities** • Understanding The Mobile Landscape (in-class) • Exploring Mobile Device Encryption (in-class) Assignments • None

Week 5 **2/12** **iOS Forensics Part 1**	**Readings** • iOS Forensics Slides (OneDrive) • iOS Cheatsheet (OneDrive) **Activities** • iOS Logical Extraction (in-class) • Using Open Source Tools (in-class) • iOS SysDiagnose Extractions (in-class) • iOS iCloud Overview & Exploration (in-class) • iOS iTunes/iCloud Backup Ingest/Process (in-class)
Week 6 **2/19** **No Class- AAFS Conference**	
Week 7 **2/26** **iOS Forensics Part 2**	**Readings** • iOS Forensics Slides (OneDrive) • iOS Cheatsheet (OneDrive) **Activities** • iOS File System Extractions (in-class) • iOS File System Walkthroughs and Comparison (in-class) **Assignments** • Exploring iOS Filesystems (lab)
Week 7 **3/4** **iOS Forensics Part 3**	**Readings** • iOS Forensics Slides (OneDrive) • iOS Cheatsheet (OneDrive) **Activities** • iOS Artifact Exploration (in-class) • Understanding 3rd Party Storage (in-class) • Advanced Artifacts (in-class) **Assignments** • Exploring iOS Artifacts (lab)
Week 8 **3/11** **Android Forensics Part 1**	**Readings** • Android Forensics Slides (OneDrive) • Android Cheatsheet (OneDrive) **Activities** • Android Targeted Extractions (in-class) • Android Extraction Explorations (in-class)

	• Android Backup Explorations (in-class) • Android Cloud Explorations (in-class) **Assignments** • Performing Targeted Extractions of Androids (lab)

Week 9 **3/18** **No Class- Spring Break**	
Week 10 **3/25** **Android Forensics Part 2**	**Readings** • Android Forensics Slides (OneDrive) • Android Cheatsheet (OneDrive) **Activities** • Android Physical Examinations (in-class) • Android File System Examinations (in-class) **Assignments** • Performing File System Extractions of Android Devices (lab)
Week 10 **4/1** **Android Forensics Part 3**	**Readings** • Android Forensics Slides (OneDrive) • Android Cheatsheet (OneDrive) **Activities** • Android Artifact Exploration (in-class) • Understanding 3rd Party Storage (in-class) • Advanced Artifacts for Android (in-class) **Assignments** • Exploring Android Artifacts (lab)
Week 11 **4/8** **Physical Memory Encoding/Decoding, Date/Timestamps**	**Readings** • Bair Ch. 14- Physical Memory & Encoding (pp. 201-214) • Bair Ch. 15- Date & Timestamps (pp. 215-232) **Activities** • Encoding/Decoding Practical Lab (in-class) • Date & Timestamp Practical Lab (in-class) • Decoding Advanced Storage Lab **(in-class)**

Week 12 **4/15** **SQLite Forensics & Final Project Preparation**	**Readings** • Bair Ch. 17- Application Data (pp. 247-265) • SQLite Forensic Slides (OneDrive) • SQLite Cheatsheet (OneDrive) **Activities** • Writing SQlite Queries Lab (in-class) • Selecting Final Project Application • Open Lab & Instructor Assistance – Final Project **Assignments** • SQLite Assignment – Parsing App Data
Week 13 **4/22** **Final Project & Presentations**	**Final Project Presentations** • Students will present their project findings in a 5-7 minute presentation • Final Project Written Turn-In • Final Presentation Date: Monday 4/22 @ 2:30PM

About Your Professor:

I am an Associate Professor in the School of Forensic & Criminal Justice Sciences at Marshall University and have been since 2012. My teaching & research expertise is in digital forensics, mobile device forensics, network forensics, and multimedia forensics. I am a Fellow of the American Academy of Forensic Sciences (AAFS), an appointed member & Executive Secretary of the NIST Organization of Scientific Area Committee (OSAC) on Digital Evidence, Commissioner of FEPAC & a member of ASTM E30 Committee on Forensic Sciences. I am also an Editorial Board Member of the Journal of Forensic Sciences Prior to entering academia, I managed digital forensic casework & research laboratories at the Marshall University Forensic Science Center and also worked as an examiner with the West Virginia State Police's Digital Forensic Unit. I also worked as a Technical Assessor for the ANAB assessing digital forensics laboratories throughout the US seeking ISO accreditation. I am graduate of the FLETC Seized Computer Evidence Recovery Specialist (SCERS) program, a certified Computer Hacking Forensic Investigator (CHFI), a Magnet Certified Forensics Examiner (MCFE), a LEVA Certified Forensic Video Technician (CFVT), a Cellebrite Certified Mobile Examiner (CCME), & GIAC Advanced Smartphone Forensics (GASF) certified.

A more detailed background, including my past work & research, can be found at: http://science.marshall.edu/brunty11 or https://solo.to/joshbrunty

You can also follow me on Twitter @joshbrunty