Course: **CJ 4750 Small Devices Forensics**

Credit Hours: **3 credit hours**

Instructor: **Joan Runs Through**

Office Phone: **(435) 879-4420**

Office Hours: **TBA**

PREREQUISITES: **CJ 2700 (CJ 3900 is highly recommended)**

REQUIRED TEXT:

Mobile Phone Examiner Training Manual

Various articles and white papers

as assigned by instructor

All students are expected to read and understand everything outlined in this syllabus. Enrollment and participation online is implied agreement with the terms of this syllabus. If there are questions or concerns about the syllabus, feel free to discuss them with me.

This is an online course, which requires verification of your identity through the use of proctored assignments and/or tests. The student will receive an F in the course if these proctored assignments are not completed and are not compatible with coursework submitted throughout the semester.

COURSE DESCRIPTION

Digital forensics through the exploration of various small scale digital devices such as personal digital assistants, cell phones, GPS devices, and MP3 players. Focuses on specific search and seizure issues with these devices, how forensic challenges differ from those present with personal computers, and the technical issues commonly encountered during examination.

There are no additional fees for this course, and this course does not hold GE status.

COURSE OBJECTIVES

This course is designed to provide students with an introduction to the examination of small devices including cell phones, GPS devices, and other small scale portable devices. On completion of this course students will be able to do the following:

1. Provide the steps for search and seizure of digital evidence on small portable devices
2. Understand how the 1st and 4th amendments apply to the search and seizure of small device digital evidence.
3. Be able to understand the difficulties faced by law enforcement when it comes to cell phone analysis.
4. Understand the basic difference in file systems between PCs and small digital devices.
5. Have a basic understanding of how GPS system work and how GPS data from small devices can be extracted and presented as evidence.
6. Be familiar with current small device extraction and interpretation technologies.

COURSE FOCUS

Unit I: Introduction to Personal Electronics — Week 1

In this unit, the student is introduced to the nature of cell phones, considerations for cell phones during search and seizure, applicable laws, and special considerations. Students will also be able to identify ten separate items of evidentiary interest that can be found a cell phone.

Unit II: Beginnings of Mobile Forensics and the Forensic Process — Week 2

Throughout this unit students will have the opportunity to increase understanding of the scientific method and how forensic science is applied to cell phone forensics. Emphasis is placed on the history and development of cell phone forensics, the differences between GSM and CDMA networks, and how the cellular network works. Students will apply the presentation phase of forensic using photography and note taking as a primary tool of early mobile forensics.

Unit III: Software Management — Week 3

In this unit students will have the opportunity to explore mobile device forensics through examining the use of mobile management software to create reports. Students will also explore the commercial tools that developed out of consumer management products to include SecureView and Oxygen forensic Suites.

Unit IV: Parsing Backups (Blackberry and iPhone Forensics) — Week 4

In this unit students will be tasked with examining backups rather than phones. Students will further develop presentation skills by compiling their findings into a examination report. Students will also explore how cloud storage effects the field of digital forensics.

Unit V: Commercial Tool Overview — Week 5

In this unit students have the opportunity to compare and contrast a variety of mobile forensic suites available on the market. Students will begin working with the AccessData product MPE+ with an overall goal of becoming certified in this software by the end of this course. Student will be able to define “push button forensics” as well as explain 2 pros and cons to this phenomenon.

Unit VI: File Systems 1: NAND and YAFFS2 Week 6

This unit introduces students to Android Architecture and the YAFFS2 file system. Student will be able to discuss issues caused by stacking bit, will be able to define Page, Block and Bits as well as explain how NAND Flash memory compensates for limited read/writes (mean time to failure). Students will be able to explain in layman's terms the YAFFS2 storage algorithm as wells as determine manual carving strategies for files stored on YAFFS2 systems.

Unit VII: File Systems 2: EXT, FAT and Brew Week 7

This unit compares the data storage algorithms for EXT, FAT and Brew and discusses how this affects data storage and carving techniques. Students will also be able to identify the timestamp formats used by each of these file systems .

Unit VIII: Parsing the Unstructured Data Dump Week 8

In this unit students will work with binary images of handheld devices and carve viable files from a hex dump. Students will work with XRY, Cellebrite Physical Pro as well as Scalpel, Strings, XXD, and Grep

Unit IX: Scripting and HTML Week 11

In this unit, students will be able to edit a script template and use the script to assemble acquired data into an appropriate presentation format. Students will also demonstrate an ability to create an HTML report to assemble acquired data into a report presentable to the courts.

Midterm and Practicum Week 9

SPRING BREAK Week 10

Unit X: Android ADB and Rooting Week 11

In this unit, students demonstrate installation of the Android SDK and its application toward forensic processes. The student will be able to identify and define a minimum of six adb commands. Students will also list two types of rooting process and explain in lay terms what rooting does for a mobile device. Students will be able to use ODIN to root a device and navigate the file system to remove a password or pattern lock.

Unit XI: JTAG and Flashing Week 11

Student will be able to identify JTAG points on a phone, list common JTAG points, explain how what a flasher box is designed for and relay how it can be used for forensic purposes. Student will demonstrate ability to parse physical image obtained by JTAG and Flasher Boxes and put them in an appropriate presentation format.

Unit XII: Cell Phone Repair Week 11

In this unit, students experience hands-on disassembly and assembly of phones, cleaning corrosion and water damage as well as simple parts replacement. They learn the value of repair in the small device forensics process. They are able to identify the parts of the mobile PCB and they are able to identify the NAND flash memory chip on a PCB.

Unit XIII: Chip Off and Data Recovery Week 12

In this unit, students have hands on experience removing the NAND BGA chip from a PCB. Students repair a BGA chip in order to successfully acquire a binary image through a reader/programmer. . And students carve the binary image for data of an evidentiary nature.

Unit XIV: Small Device Research Week 11

Student will demonstrate understanding of the four forensic stages: Acquisition, Preservation, Analysis and Presentation and demonstrate and understanding of how research helps in all four stages.

Unit XV: Smart Card, SIM Card Structures, SD Cards Week 13

This unit provides students the opportunity to explore the structure of Smart Cards and SIM Cards. Students will be able to extract user data and deleted data from SIM cards. Students will also learn how magnetic cards can be used in fraud and other cases and how to search for and/or prevent this.

OBJECTIVES: During the course the student will demonstrate skills learned through assignments and exams.

The following table lists Course Competencies/Objectives and further describes this focus.

Modules	**Objectives**	**Activities**
Unit I Introduction to Personal Electronics and Information Contained on Cell Phones	**Performance Objective One:** Student will be able to identify three allowances made by the court for cell phone forensics (live searches, documented interaction, validation) **Performance Objective Two:** Student will be able to categorize cell phones by network (CDMA, GSM, iDen) **Performance Objective Three:** Student will be able to, in basic terminology, explain the cellular network **Performance Objective Four:** Student will be able to identify the type of paperwork needed for physical exams, historical records and live capture) **Performance Objective Five:** Student will be able to list four areas of concern when performing a search and seizure on a wireless device (isolate device from network, leave on or turn off, obtain password, obtain a warrant that specifies the device and what the device contains) **Performance Objective Six:** Student will be able to list 10 items of evidentiary value that may be recovered from a cell phone	• Course Policies and Syllabus Review • PPT: Introduction to Personal Electronics • Academic Module 4 & 9 • Reading Quiz
Unit II Beginnings of Mobile Forensics and the Forensic Process	**Performance Objective Seven:** Student will be able to outline the history of cell phones from the 1920s to the present. They will be able to connect the beginnings of frequency hopping from world	• PPT: Mobile Forensics History • Qualcomm

	war II to the cell towers of today. **Performance Objective Eight:** Student will be able to explain how the cell phone network works in terms that a jury will understand. **Performance Objective Nine:** Student will be able to define Half Duplex, Full Duplex, Analogue and Digital **Performance Objective Ten:** Student will be able to identify and compare and contrast Time Division Multiple Access (GSM) and Code Division Multiple Access (CDMA) networks. **Performance Objective Eleven:** Student will explore the origins of cell phone forensics through the use of camera documentation.	Reading • Academic Mod 2 & 5 • Unit II Reading Quiz • Lab: Project-a-Phone • Discussion Board
Unit III Software management	**Performance Objective Twelve:** Student will explore the development of small device forensics through the use of management software **Performance Objective Thirteen:** Student will examine the role of white papers and research in small device forensics. **Performance Objective Fourteen:** Student will demonstrate proficiency at using cell phone management software to extract data for inclusion in a forensic report. **Performance Objective Fifteen:** Student will demonstrate ability to recreate a documented research procedure.	• PPT • Reading: CDMA Clone Pape • Reading: Chapter 20 • Unit III Reading Quiz • Notice to Prepare Research Project • Lab: Bitpim • Discussion Board
Unit IV Parsing Backups Blackberry and iPhone Forensics	**Performance Objective Sixteen:** Student will demonstrate ability to use a phone simulation to explore backup content **Performance Objective Seventeen:** Student will demonstrate ability to parse iPhone/Blackberry backups for artifacts to include in a forensic report. **Performance Objective Eighteen:** Student will be able to identify methods for retrieving iPhone cloud backups	• PPT: Iphone & Blackberries • Reading: iPhone Paper • Unit IV Reading Quiz • Install VM and Santoku Howto • Lab: Backup Report
Unit V Commercial Tool Overview	**Performance Objective Nineteen:** Student will be able to identify 3 pros and cons for current small	• PPT: Tool Comparison • Reading: MPE

MPE+ and the FTK tie-in	device commercial tools. **Performance Objective Twenty**: Student will become certified in at least one commercial small device forensic tool. **Performance Object Twenty-One**: Student will be able to 4 identify tools within large device forensic suites that can be applied to small device forensics. **Performance Object Twenty-Two:** Student will be able to connect a supported device to the any of the top forensic suites and acquire a forensic extract.	Mod 4-7 • Lab: MPE+ report • Reading: AME Study Guide • Unit V Reading Quiz
Unit VI File Systems and research NAND YAFFS2,	**Performance Objective Twenty Three:** Student will demonstrate understanding of the role research plays in small device forensics by creating/recreating an investigative research project. **Performance Objective Twenty Four:** Student will be able to explain in layman's terms how data is stored on NAND flash memory as well as define Page, Block, Bits, and the issues of stacking bits **Performance Object Twenty-Five:** Student will be able to explain to members of a jury how the YAFFS2 file system assigns data storage.	• PPT: NAND and UAFFS2 • Reading: Yaffs2 • Unit VI Reading Quiz • Project Design Submission • Midterm Review
MIDTERM	**Practical: MPE+ Certification** **Written: Written Exam**	•
Unit VII File Systems II EXT, FAT, Brew	**Performance Objective Twenty-Six:** Student will be able to list three differences between the EXT, FAT, and BREW file systems including timestamp differences, files system metadata structures, and data storage algorithms.	• PPT: EXT, FAT, Brew • Reading: Brew • Unit VII Reading Quiz
Unit VIII Parsing the unstructured Data Dump	**Performance Objective Twenty-Seven:** When given a raw binary image student will be able to use Strings as a triage to evaluate for user data Performance Objective Twenty-Eight: When given a raw binary image, student will be able to configure Scalpel to extract phone numbers, sms, graphics and audio. Performance Objective Twenty-Nine: When given a raw binary image	• PPT: Strings, Scalpel, XXD, Grep • Lab: Carving
Spring Break		•
Unit IX	**Performance Objective Thirty:** After extraction of	• Scripting/Parsi

Scripting and HTML	artifacts student will be able to edit script template to assemble data into a csv Performance Objective Thirty-one: Student will be able to create an HTML report including assembled extracts.	ng Lab
Unit X Android ADB and Rooting	**Performance Objective Thirty-One:** Student will be able to download and install the Android SDK with the Platform Tool ADB **Performance Objective Thirty-Two:** Student will be able to identify six adb commands and identify their utility including adb devices, adb shell, adb push, adb pull, adb reboot, adb reboot-bootloader, fastboot devices, adb install	• PPT: Linux Basics/ADB • Santoku How To (ADB, AFLogical) • Lab: ADB
Unit XI JTAG and Flashing	**Performance Objective Thirty-Three:** Student will explore JTAG and Flashing and Identify 2 similarities and 2 differences between the processes. **Performance Objective Thirty-Four:** Student will be able to define the JTAG and the flashing process as it relates to digital forensics. **Performance Objective Thirty-Five:** Student will be able to identify how flashing technology is incorporated into commercial push button devices.	• PPT: JTAG and Flashing • Reading: JTAG and Flashing • Unit XI Reading Quiz
Unit XII Cell Phone Repair	**Performance Objective Thirty-six:** Student will identify the three basic physical types of cell phones and accurately predict where the screws and clips holding it together are located. **Performance Objective Thirty-seven:** Student will accurately identify the components on a cell phone PCB board. **Performance Objective Thirty-eight:** Student will identify and clean water damage and replace an lcd.	• PPT: Cell Phone Repair • Cell Phone Repair Project • Research Report • PowerPoint Presentation
Unit XIII Chip Off	**Performance Objective Thirty-nine:** Student will remove a BGA chip from PCB **Performance Objective Forty:** Student will successfully place BGA chip in reader and extract binary image	• Chip-Off PPT • Chip Off Reading • Unit XII Reading Quiz
Unit XIV Review	**Performance Objective Forty-One**: Student will demonstrate understanding of the four forensic stages: Acquisition, Preservation, Analysis and Presentation	• Research Project
Finals Week		•

Grade Breakdown

A 100-93% A- 92-90%
B+ 89-87% B 86-84% B- 83-80%
C+ 79-77% C 76-74% C-73-70%
D+ 69-67% D 66-64% D- 63-60%
F 59% or below

Dixie State College's Policies

The following link will allow you to view information on the following school policies, important dates, the final exam schedule, and helpful resources such as:

Disability Resource Center
Library Information
IT Help Desk
Online Writing Lab
Testing Center
Tutoring Center
Writing Center
Semester Schedule
Academic Dishonesty/Academic Integrity Policy
Disruptive Behavior Policy
Absences Related to College Functions
Reasonable Accommodation Policy

http://new.dixie.edu/reg/syllabus/