GROSSMONT COLLEGE

Official Course Outline

ADMINISTRATION OF JUSTICE 155 – DIGITAL INVESTIGATIONS

1. Course Number Course Title Semester Units Semester Hours

AOJ 155 Digital Investigations 3 3 hours lecture:48-54 hours

96-108 outside-of-class hours

144-162 total hours

2. Prerequisites

None.

Corequisite

None.

Recommended Preparation

None.

3. Catalog Description

This course provides an introduction to the forensic analysis of digital devices (most commonly used cell phones, smart phones, tablets computers) and focuses on the procedures, policies, and technology utilized in digital evidence recovery. Emphasis is placed on the analysis of digital evidence for use during criminal or civil investigations from personal mobile devices. This course also prepares students with knowledge in investigative principles and applicable case law that is applicable to both civil and criminal investigations.

4. Course Objectives

The student will:

1. Define digital evidence as it pertains to mobile devices.
2. Explain how mobile devices work on cellular networks.

c. Describe the importance of collecting and preserving mobile device digital evidence.

d. Recognize how mobile devices are used as tools to commit crimes.

e. Identify and develop methods to recover mobile device digital evidence in a forensically sound manner.

f. Evaluate mobile device digital evidence policies and procedures.

g. Analyze data recovered from a mobile device.

h. Demonstrate the ability to accurately and thoroughly conduct and document a mobile device digital evidence investigation.

i. Create a report to document digital evidence analysis.

j. Discuss constitutional law related to searching and seizing of mobile devices and digital evidence.

k. Evaluate statutory and case law related to digital evidence.

l. Identify, analyze, and develop solutions to problems in digital evidence investigations.

m. Utilize computer technology and access information via the Internet as appropriate.

o. Conduct research appropriate to the discipline.

p. Evaluate personal and professional ethical standards.

5. Instructional Facilities

Standard classroom

ADMINISTRATION OF JUSTICE 155 –DIGITAL INVESTIGATIONS Page 2

6. Special Materials Required of Student

Electronic storage media.

7. Course Content

a. Introduction to computer science fundamentals.

b. Introduction to digital evidence.

c. Functions, duties, responsibilities of a digital evidence technician.

d. Digital evidence recovery, preservation, and analysis.

e. Legal aspects of digital evidence search and seizure.

f. Problems and solutions in digital evidence recovery.

8. Method of Instruction

1. Lecture, class discussion, and individual assignments and group projects as appropriate.

b. Links to additional internet resources for lecture enhancement and research

c. Qualified guest speakers may be invited to lecture on their respective fields of specialization.

d. Field trips to local public safety agencies and security organizations may be arranged.

9. Methods of Evaluating Student Performance

1. Discussion assignments
2. Written assignments.
3. Periodic examinations.
4. Research assignments such as researching previous cases and analyzing results.
5. Group projects such as investigating mock case(s) and extracting and analyzing “evidence” individually and in a group.
6. Oral presentations such as mock or real case analysis on mobile forensic evidence.
7. Written final examination.

10. Outside Class Assignments

a. Reading in required text.

b. Critical-thinking and problem solving exercises such as mock case analysis

c. Research paper or project such as researching previous cases and analyzing results.

d. Preparation for oral presentations for mock or real case analysis on mobile forensic evidence.

11. Texts

a. Required Text(s):

Brita, M.T. *Computer Forensics and Cyber Crime: An Introduction.* New York: New York, Pearson Publishers, 2013.

b. Supplementary texts and workbooks:

None.

Addendum: Student Learning Outcomes

Upon completion of this course, our students will be able to do the following:

1. Collect and preserve mobile device data using appropriate technology.
2. Properly analyze data recovered from a mobile device.
3. Describe constitutional law related to the search and seizure of mobile device digital evidence.

Date approved by the Governing Board: December 11, 2018