LAGUARDIA COMMUNITY COLLEGE
CITY UNIVERSITY OF NEW YORK
MAC257: Digital Forensics
3 Credits, 4 hours (Lecture – 2 hours, Lab – 2hours)

Course Description

Digital Forensics course introduces the methods and technologies relevant to conducting a computer forensic investigation. Topics include: collecting, analyzing, recovering, preserving and reporting a forensic evidence. This course will also introduce how to retrieve data that resides on a computer and recover deleted, encrypted or damaged files. Students will learn about legal considerations and ethics as well. Various operating systems will be considered including Windows, Macintosh, and Linux.

Prerequisites – MAC246, MAC237

Pre/ Corequisite: MAC254

Textbooks

- "System Forensics, Investigation, and Response" by Chuck Easttom. Publisher: Jones & Bartlett Learning, 2nd edition. ISBN: 1284031055
- "Laboratory Manual to Accompany System Forensics, Investigation And Response" by vLab Solutions. Publisher: Jones & Bartlett Learning, Lab Manual Edition. ISBN: 144963852X

Instructional Objectives

1. Introduce principles of computer forensics.
2. Introduce important laws and ethics affecting digital forensics.
3. Familiarize students with various computer crimes.
4. Familiarize students with forensic methods and labs.
5. Familiarize students with the proper procedure for collecting, seizing, and protecting evidence.
6. Familiarize students of methods to recover encrypted, hidden, damaged or deleted data.
7. Introduce E-mail forensics and laws regarding privacy.
8. Introduce tools to perform network analysis and to collect data from network elements.
9. Introduce incident and intrusion response.
10. Familiarize students with global issues in digital forensics.

Performance Objectives

Upon completion of this course students should:

1. Identify the basic principles of Computer Forensics.

2. Summarize different laws and ethics pertaining to computer forensics.

3. Describe common computer crimes.

4. Employ digital forensic methodologies and be able to set up a forensic lab.

5. Outline the proper approach to collecting seizing and protecting evidence

6. Be able to recover data on a Windows, Mac or Linux system.

7. Understand how e-mail works and how to get the header from different e-mail systems and demonstrate knowledge of laws regarding privacy.

8. Be able to perform network analysis, to collect data from a router or a firewall.

9. Describe incident and intrusion response.

10. Write an essay on global issues in digital forensics

Grading Guidelines

A-, A	90-100
B-, B, B+	80-89
C-, C, C+	70 – 79
D-, D, D+	60 – 69
F	Below 60
WU	Unofficial Withdrawal (Students who have stopped attending at any time before the final exam week, and did not officially withdraw will receive this grade)

Grading Standards

CATEGORY	PERCENTAGE
Assignments (5 @ 3% each)	15%
Labs (10@3% each)	30%

Midterm Exam	20%
Project	15%
Final Exam	25%
Total	**100%**

ACADEMIC INTEGRITY

This class will be conducted in compliance with LaGuardia Community College's academic integrity policy.

ATTENDANCE

The maximum number of unexcused absences allowed is 15% of the total class meetings (about 7 hours). Unexcused absences beyond this maximum will result in a grade of WU or F.

COMMENTS

The grading standards listed above, and the suggested homework problems listed in the course outline are both subject to modification by the instructor.

For more details about the academic requirements and grading policy, see the following link: https://www.laguardia.edu/uploadedFiles/Main_Site/Content/Academics/Catalog/PDFs/AcademicRequirementsAndPolicies.pdf

Weekly Topics

Week	Lecture Topics	Labs
1	Introduction to Forensics. Overview of Computer Crime	Lab 1: Documenting a Workstation. Configuration Using Common Forensic Tools.
2	Forensic Methods and Labs	Assignment 1: Cybercrime, digital forensics firms and Certifications in digital forensics. Lab 2: Creating a Forensic System Case File for Analyzing Forensic Evidence. Project Discussion: Global Issues in Digital forensics.

3	Collecting, Seizing, and Protecting Evidence. Understanding Techniques for Hiding and Scrambling Information.	Lab 3: Uncover New Digital Evidence Using Bootable Utilities.
4	Recovering Data	Assignment 2: Denial of Service Tools, Digital Forensic software Lab 4: Automate Image Evaluations and Identify Suspicious or Modified Files
5	E-mail Forensics	Lab 5: Craft an Evidentiary Report for a Digital Forensic Case
6	Windows Forensics	Assignment 3: E-mail Law, Tools for Monitoring Changes to Files and Memory. Lab 6: Automate Digital Evidence Discovery Using Paraben's P2 Commander.
7	Linux Forensics	Midterm Exam
8	Macintosh Forensics Mobile Forensics	Assignment 4: Best Practices in Collecting Digital Evidence, Proper Methods for Capturing Data. Lab 7: Craft an Evidentiary Report for a Digital Forensic Case
9	Performing Network Analysis	Lab 8: Apply Steganography to Uncover Modifications to an Image File.
10	Incident and Intrusion Response	Assignment 5: Network Traffic Analysis Tools. Lab 9: Decode an FTP Protocol Session and Perform Forensic Analysis.
11	Trends and Future Directions	Lab 10: Perform an Incident Response Investigation for a Suspicious Logon Project due.
12	System Forensics Resources	Review
13	Final Exam	