STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

JUST365 / CITA365 - Digital Forensic Analysis

Created by: Robert Edwards / William Mein / Robert House / Christopher Sweeney
Updated by: Minhua Wang

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
and
CANINO SCHOOL OF ENGINEERING TECHNOLOGY
FALL 2018

A. **TITLE**: Digital Forensic Analysis

B. **COURSE NUMBER:** JUST365/CITA365

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

 # Credit Hours: 3
 # Lecture Hours: 2 **per week**
 # Lab Hours: 2 **per week**
Other: **per week**

Course Length: 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Spring

G. **COURSE DESCRIPTION:** This course is designed to prepare the student to complete forensic analysis of digital media and to understand the process and technical challenges of internet investigations. The course looks specifically at how to obtain evidence from digital media, how to process network messages and logs while preserving the evidentiary chain, and how to adhere to the legal requirements of the search and seizure of digital media and related equipment and information.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): Junior Level Status in Cybersecurity, Information Technology, or any Baccalaureate Criminal Justice Program
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	***PSLO***	***ISLO***
a. Describe the role of computer forensics.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5
b. Demonstrate an ability to apply computer forensics to investigations.	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
c. Demonstrate the ability to perform a computer forensic analysis using computer and network-based tools.	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5

d. Analyze case studies involving collaborative investigation techniques.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA] 5
e. Describe the concepts of how data are stored on digital devices.	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
f. Describe the process of computer forensic analysis.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5
g. Apply current knowledge and techniques to the analysis of digital devices.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	5
h. Construct a comprehensive report of forensic analysis.	1. Communicate clearly, concisely, and correctly in the written, spoken, visual, and electronic form that fulfills the purpose and meets the needs of audiences 2. Interpret, produce, and present work-related documents and information effectively and accurately	1[W] 4[ER] 5

J. **APPLIED LEARNING COMPONENT:** **Yes** X **No**

- Classroom/Lab

K. **TEXTS:** None

L. **REFERENCES:** Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database

M. **EQUIPMENT:** Computer lab classroom

N. **GRADING METHOD:** A-F

O. **SUGGESTED MEASUREMENT CRITERIA/METHODS:**

- Participation
- Reports
- Lab Assignments
- Tests

P. **DETAILED COURSE OUTLINE:**

I. The System Forensics Landscape
   A. System Forensics Fundamentals
   B. Overview of Computer Crime
   C. Challenges of System Forensics
   D. Forensics Methods and Labs

II. Technical Overview: System Forensics Tools, Techniques, and Methods
A. System Forensics Technologies
B. Controlling a Forensic Investigation
C. Collecting, Seizing, and Protecting Evidence
D. Investigating Information-Hiding Techniques
E. Recovering Data
F. Investigating and Scrutinizing E-mail
G. Performing Network and Internet Analysis
H. Searching Memory in Real Time with Live Systems Forensics

III. Emerging Technologies, Future Direction, and Resources
A. Incident/Intrusion Response
B. Future Directions

A.

Q. <u>LABORATORY OUTLINE</u>:

Lab assignments using the *JBL Virtual Security Cloud Labs* which provides a "virtual sandbox" for students to practice coursework on an actual IT infrastructure.

I. Perform a Byte-Level Computer Audit
II. Apply the Daubert Standard on the Workstation Domain
III. Create a Forensic System Case File for Analyzing Forensic Evidence
IV. Uncover New Digital Evidence Using Bootable Utilities
V. Automate Digital Evidence Discovery Using Paraben's P2 Commander
VI.
VII. Apply Steganography to Uncover Modifications to an Image File
VIII. Decode an FTP Protocol Session and Perform Forensic Analysis
IX. Automate Image Evaluations and Identify Suspicious or Modified Files
X.
XI. Craft an Evidentiary Report for a Digital Forensic Case
XII. Perform an Incident Response Investigation for a Suspicious Logon