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

MASTER SYLLABUS

JUST365 / CYBR365 - Digital Forensic Analysis

Created by: Kambiz Ghazinour

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
FALL 2020

A. **TITLE**: Digital Forensic Analysis

B. **COURSE NUMBER:** JUST365/CYBR365

C. **CREDIT HOURS:** 3

- 3 hours of lecture per week

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

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

G. **COURSE DESCRIPTION:** This course is designed to cover: the need for computer forensics, best practices for general incidence response, legal aspects of forensics, tools and techniques to perform a full computer forensic investigation.

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. Identify and apply basic digital forensics principles.	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. Identify the uses of digital forensics and its challenges.	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
c. Identify and explain the technical concepts that are useful to digital 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
d. Describe the different types of labs and the tools that "they" use and apply them to a given scenario.	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
e. Explain how evidence is collected and processed.	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

f. Recognize and explain the purpose of Windows system artifacts.	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. Explain and apply anti-forensic techniques and their ability to disrupt investigations.	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. Identify and examine legal leverages and limitations in electronic evidence collection and analysis.	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
i. Describe and identify the basics and internals of the Internet.	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
j. Identify, analyze and apply the fundamentals of forensic network investigations.	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
k. Describe and explain how and why cell phones are used as evidence in investigations.	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
l. Research challenges and concerns of digital forensics in emerging technologies	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
m. Evaluate peer viewpoints and provide constructive critiques to further the discussion.	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	5

J. **APPLIED LEARNING COMPONENT:** **Yes**__X___ **No**_____

- Computer Lab Classroom

K. **TEXTS:** The Basics of Digital Forensics, 2nd Edition Author: John Sammons

- eBook ISBN: 9780128018927
- Paperback ISBN: 9780128016350

https://www.elsevier.com/books/the-basics-of-digital-forensics/sammons/978-0-12-801635-0

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

M. **EQUIPMENT:** Computer lab classroom

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

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Participation
- Discussions
- Assignments
- Tests

P. DETAILED COURSE OUTLINE:

- Introduction
  - What is forensic science?
  - What is digital forensics?
  - Uses of digital forensics
  - The digital forensics process
  - Locard's exchange principle
  - Scientific method
  - Organizations of note
  - Role of the forensic examiner in the judicial system
- Key technical concepts
  - Bits, bytes, and numbering schemes
  - File extensions and file signatures
  - Storage and memory
  - Computing environments
  - Data types
  - File systems
  - Allocated and unallocated space
  - How magnetic hard drives store data
- Labs and tools
  - Forensic laboratories
  - Policies and procedures
  - Quality assurance
  - Digital forensic tools
  - Accreditation
- Collecting evidence
  - Crime scenes and collecting evidence
  - Documenting the scene
  - Chain of custody
  - Cloning
  - Live system versus dead system
  - Hashing
  - Final report
- Windows system artifacts
  - Deleted data
  - Hibernation file (hiberfile.sys)
  - Registry
  - Print spooling
  - Recycle bin
  - Metadata
  - Thumbnail cache
  - Most recently used
  - Restore points and shadow copy
  - Prefetch
  - Link files
- Anti-forensics

    - Hiding data
    - Password attacks
    - Steganography
    - Data destruction
- Legal
    - The fourth amendment
    - Criminal law—searches without a warrant
    - Searching with a warrant
    - Electronic discovery
    - Expert testimony
- Internet and e-mail
    - Internet overview
    - Web browsers—Internet Explorer
    - E-mail
    - Social networking sites
- Network forensics
    - Network fundamentals
    - Network security tools
    - Network attacks
    - Incident response
    - Network evidence and investigations
- Mobile device forensics
    - Cellular networks
    - Operating systems
    - Cell phone evidence
    - Cell phone forensic tools
    - Global positioning systems
- Looking ahead: challenges and concerns
    - Standards and controls
    - Cloud forensics
    - Solid state drives
    - Speed of change
    - Additional resources

Q. LABORATORY OUTLINE: N/A