

CSIT 244: DIGITAL FORENSICS FUNDAMENTALS

1. Course Information

Subject

CSIT - Computer Science/ Information Technology

Course Number

244

School

Science, Technology, Engineering, Mathematics

Course Title

Digital Forensics Fundamentals

2. Hours

Semester Hours

3

Lecture

3

Lab

0

Practicum

0

3. Catalog Description

For display in the online catalog

This course introduces the methodology and procedures associated with digital forensic analysis. The objective of this class is to emphasize the fundamentals and importance of digital forensics. Students will learn different techniques and procedures that enable them to perform a digital investigation. This course focuses mainly on the analysis of physical storage media and volume analysis. It covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in hard disks and random-access memory.

4. Requisites

Prerequisites

CSIT 165 and CSIT 184

5. Course Type

Course Fee Code

3

Course Type for Perkins Reporting

vocational (approved for Perkins funding)

6. Justification

Describe the need for this course

This course provides the required training in Cybersecurity programs of study and helps students prepare for the fundamental of digital forensics.

7. General Education

Will the college submit this course to the statewide General Education Coordinating Committee for approval as a course, which satisfies a general education requirement?

No

If the course does not satisfy a general education requirement, which of the following does it satisfy:

Program-specific requirement

8. Consistency with the Vision and Mission Statements, the Academic Master Plan, and the strategic initiatives of the College

Please describe how this course is consistent with Ocean County College's current Vision Statement, Mission Statement, Academic Master Plan, and the strategic initiatives of the College:

Add item	
1	Demonstrating the college's commitment to offer comprehensive educational programs that develop intentional learners of all ages. (Mission Statement)
2	Seeking to ensure that students will thrive in an increasingly diverse and complex world. (Vision Statement)
3	Preparing students for successful transfer to other educational institutions and/or for entrance into the workforce. (Academic Master Plan)
4	Seeking to empower students through the mastery of intellectual and Practical Skills. (Academic Master Plan)
5	Challenging students to transfer information into knowledge and knowledge into action. (Academic Master Plan)

9. Related Courses at Other Institutions

Comparable Courses at NJ Community Colleges

Institution

County College of Morris

Course Title

Digital Forensic

Course Number

CMP 160

Number of Credits

3

Institution

Middlesex County College

Course Title

Computer Forensics

Course Number

CSC 258

Number of Credits

3

Institution

Brookdale CC

Course Title

Computer Forensics and Investigation

Course Number

NETW 236

Number of Credits

3

Institution

Camden County College

Course Title

Digital Forensics & Investigation

Course Number

CST 210

Number of Credits

3

Institution

Essex County College

Course Title

Computer & Internet Forensics

Course Number

CSC 230

Number of Credits

3

Institution

Passaic County CC

Course Title

Computer Forensics and Investigation

Course Number

CIS 289

Number of Credits

3

Institution

Raritan Valley CC

Course Title

Privacy, Ethics, & Computer Forensics

Course Number

NTWK 274

Number of Credits

3

Institution

Rowan College of South Jersey

Course Title

Computer Forensics

Course Number

CS 241

Number of Credits

3

Institution

Union County College

Course Title

Digital Forensics Essentials

Course Number

CST 170

Number of Credits

3

Transferability of Course**Georgian Court University**

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
EC Elective Credit, 3	Elective	

Kean University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
TECHX1003, 3	Technology Elective	

Monmouth University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
FE0001 100-level Free Elective 3	Elective	

Rowan University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CST 03252, Foundations of Computer Forensics, 3	Required	

Stockton University

Course Code, Title, and Credits	Transfer Category	If non-transferable; select status
CSISEC, Computer Science & Info Systems Elective, 3	Computer Science Elective	

10. Course Learning Outcomes**Learning Outcomes**

Students who successfully complete this course will be able to:	
CLO1	Discuss the fundamental concepts of computer forensics, digital evidence, forensic readiness, identify the roles and responsibilities of a forensic investigator and review legal compliance issues in computer forensics.
CLO2	Examine the computer forensic investigation process and its phases.
CLO3	Describe different disk drives, characteristics, and logical structure, understand Windows, Linux, and Mac boot processes, and examine various file systems and formats.
CLO4	Discuss data acquisition concepts, types, format, and methodology.
CLO5	Examine various anti-forensics techniques and identify countermeasures.
CLO6	Examine various volatile and non-volatile information gathering techniques for Windows, Linux, and Mac systems, including Windows memory and registry analysis, cache, cookie, history analysis, and metadata investigation.
CLO7	Explain network forensics fundamentals, event correlation, and perform network traffic investigation.
CLO8	Appraise web server logs and perform web application forensics to detect and investigate various attacks on web applications.
CLO9	Discuss malware forensics fundamentals, list and perform different types of malware analysis.

11. Topical Outline

(include as many themes/skills as needed)

	Major Themes/ Skills	Assignments (Recommended but not limited to)	Assessments (Recommended but not limited to)	Course Learning Outcome(s)
T01	1. Fundamentals of Computer Forensics 2. Digital Evidence 3. Forensic Readiness 4. Roles and Responsibilities of a Forensic Investigator 5. Legal Compliance in Computer Forensics	Reading, Class discussion	Quiz/ Exam	CLO1, CLO2
T02	1. Forensic Investigation Process and its Importance 2. Forensic Investigation Process - Pre-investigation Phase 3. Forensic Investigation Process - Investigation Phase 4. Forensic Investigation Process - Post-investigation Phase	Reading, Class discussion	Quiz/ Exam	CLO3
T03	1. Different Types of Disk Drives and their Characteristics 2. Logical Structure of a Disk 3. Booting Process of Windows, Linux, and Mac Operating Systems 4. File Systems of Windows, Linux, and Mac Operating Systems 5. File System Examination	Reading, Class discussion	Quiz/ Exam	CLO2, CLO3
T04	1. Data Acquisition Fundamentals 2. Types of Data Acquisition 3. Data Acquisition Format 4. Data Acquisition Methodology 5. Anti-forensics and its Techniques 6. Anti-forensics Countermeasures	Reading, Class discussion	Quiz/ Exam	CLO4, CLO5
T05	1. Volatile and Non-Volatile Information 2. Windows Memory and Registry Analysis 3. Cache, Cookie, and History Recorded in Web Browsers 4. Windows Files and Metadata 5. Volatile and Non-Volatile Data in Linux 6. Memory Forensics 7. Mac Forensics	Reading, Class discussion	Quiz/ Exam	CLO4, CLO5

T06	1. Network Forensics Fundamentals 2. Event Correlation Concepts and Types 3. Identify Indicators of Compromise (IoCs) from Network Logs 4. Investigate Network Traffic 5. Web Application Forensics 6. IIS and Apache Web Server Logs	Reading, Class discussion	Quiz/ Exam	CLO5, CLO6
T07	1. Investigating Web Attacks on Windows-based Servers 2. Detect and Investigate Attacks on Web Applications 3. Dark Web 4. Dark Web Forensics 5. Tor Browser Forensic	Reading, Class discussion	Quiz/ Exam	CLO6, CLO7
T08	1. Email Basics 2. Email Crime Investigation and its Steps 3. Malware, its Components and Distribution Methods 4. Malware Forensics Fundamentals 5. PowerShell Scripts	Reading, Class discussion	Quiz/ Exam	CLO7, CLO8, CLO6
T09	1. Recognize Types of Malware Analysis 2. Static Malware Analysis 3. Analyze Suspicious Word Documents 4. Dynamic Malware Analysis 5. System Behavior Analysis 6. Network Behavior Analysis 7. Communication	Reading, Class discussion	Quiz/ Exam	CLO8, CLO9

12. Methods of Instruction

In the structuring of this course, what major methods of instruction will be utilized?

Class lecture, presentations, discussions, lab assignments/exercises, case studies and projects.

13. General Education Goals Addressed by this Course (this section is to fulfill state requirements)

Information

Communication-Written and Oral

Yes

Related Course Learning Outcome

CLO1-CLO9

Related Outline Component

T01-T09

Assessment of General Education Goal (Recommended but not limited to)

N/A

Technological Competency

Yes

Related Course Learning Outcome

CLO1-CLO9

Related Outline Component

T01-T09

Assessment of General Education Goal (Recommended but not limited to)

N/A

Information Literacy

Yes

Related Course Learning Outcome

CLO1-CLO9

Related Outline Component

T01-T09

Assessment of General Education Goal (Recommended but not limited to)

N/A

14. Needs**Instructional Materials (text etc.):**

Text: Appropriate textbook(s) will be selected. Please contact the department for current adoptions.

Technology Needs:

N/A

Human Resource Needs (Presently Employed vs. New Faculty):

N/A

Facility Needs:

N/A

Library needs:

N/A

15. Grade Determinants

The final grade in the course will be the cumulative grade based on the following letter grades or their numerical equivalents for the course assignments and examinations

A: Excellent

B+: Very Good

B: Good

C+: Above Average

C: Average

D: Below Average

F: Failure

I: Incomplete

R: Audit

For more detailed information on the Ocean County College grading system, please see Policy #5154.

16. Board Approval

History of Board approval dates

Board of Trustees Approval Date: March 17, 2023