CS5291: CYBERSECURITY FORENSICS AND INCIDENT RESPONSE

New Syllabus Proposal

Effective Term
Semester A 2026/27

Part I Course Overview

Course Title
Cybersecurity Forensics and Incident Response

Subject Code
CS - Computer Science
Course Number
5291

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
Nil

Equivalent Courses
NIl

Exclusive Courses
Nil

Part II Course Details

Abstract

This course provides students with an integrated skill set in Digital Forensics and Incident Response (DFIR). Upon completion, students will gain a comprehensive understanding of computer forensics principles, including evidence identification, acquisition, preservation, analysis, and the incident response lifecycle, which encompasses preparation, detection, containment, eradication, recovery, and post-incident recovery. Additionally, students will acquire the ability to conduct investigations utilizing industry-standard tools, analyze case studies, identify potential threat actors or root causes, adhere to legal and ethical standards, and generate comprehensive reports that guide DFIR efforts effectively.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understand the incident response lifecycle phases to manage security breaches.	25%	x	x	x
2	Apply digital forensics procedures to identify, acquire, preserve, and analyze evidence during cybersecurity investigations using available tools.	20%	x	x	
3	Analyze forensic case studies in cybersecurity attacks to identify root causes and threat actors.	25%	x	x	x
4	Develop comprehensive cybersecurity incident and forensic reports for complex environments.	30%	x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Students will learn the integrated methodology of digital forensics and incident response, focusing on the cybersecurity incident response lifecycle and essential forensic procedures. Investigative techniques and necessary tools for responding to security breaches, analyzing digital artifacts, and identifying threat actors and root causes will be covered. Realistic incident response for cybersecurity will also be introduced to facilitate understanding.	1, 2, 3, 4	2 hours/week
2	Tutorials	Students will use selected tools for evidence acquisition, forensic analysis (disk, memory, network), and incident response. Practical exercises will simulate security breaches, requiring students to perform incident triage, collect evidence from various sources (servers, endpoints, logs), and conduct timeline reconstruction, root cause analysis, and containment actions. They will develop comprehensive incident reports and forensic documentation, following chain of custody and legal/ethical standards. These activities will enhance their proficiency in investigating real-world cybersecurity incidents, enabling them to analyze digital evidence, trace attacker activities, determine root causes, and formulate effective recovery strategies.	1, 2, 3, 4	1 hour/week

3	Project	Students will investigate a real-world or simulated security breach scenario. They will practically apply forensic tools to securely collect digital evidence (disk images, memory dumps, network captures, server/endpoint logs). Following this, they will analyze the evidence, formulate containment/ eradication actions and synthesize their findings into a comprehensive, legally sound incident response report. This project integrates all core skills: tool proficiency, evidence handling, analysis, root cause identification, response strategy, and professional reporting.	1, 2, 3, 4	2 hours/week for 4 weeks

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignment 1	1, 2	13	-	No
2	Assignment 2	3, 4	13	-	No
3	Project	1, 2, 3, 4	24	-	No

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Assignments 1 and 2

Criterion

Ability to analyze and answer fundamental cybersecurity incident response lifecycle and essential forensic procedures.

Excellent
(A+, A, A-): High

Good
(B+, B, B-): Significant

Fair
(C+, C, C-): Moderate

Marginal
(D): Basic

Failure
(F): Below Marginal

Assessment Task
Project

Criterion
Ability to conduct a substantial case study in simulated or real-world scenarios.

Excellent
(A+, A, A-): High

Good
(B+, B, B-): Significant

Fair
(C+, C, C-): Moderate

Marginal
(D): Basic

Failure
(F): Below Marginal

Assessment Task
Examination

Criterion
Ability to explain the fundamentals of cybersecurity incident response and forensic procedures and apply relevant techniques in given scenarios.

Excellent
(A+, A, A-) High

Good
(B+, B, B-): Significant

Fair
(C+, C, C-): Moderate

Marginal
(D): Basic

Failure
(F): Below Marginal

Part III Other Information

Keyword Syllabus

1) **Incident Response Framework**: Incident Response Lifecycle (Preparation, Detection, Containment, Eradication, Recovery, Post-Incident), Incident Triage, Threat Hunting, Kill Chain Analysis, Crisis Management, Tabletop Exercises. 2) **Digital Forensics Core**: Digital Evidence Identification & Acquisition, Evidence Preservation & Chain of Custody, Forensic Imaging & Hashing, Timeline Analysis, Artifact Analysis, Network Forensics. 3) **Cybercrime Investigation & Analysis**: Malware Analysis, Root Cause Determination, Threat Actor Attribution, Attack Vector Analysis, Anti-Forensics Techniques, Legal Admissibility & Ethical Guidelines. 4) **Digital Forensics and Incident Response Tools & Operations**: Industry-Standard Forensic Suites, Memory Analysis Tools, Network Analysis Tools, Incident Response Platforms & Automation, Reporting & Documentation Best Practices. 5) **Other Emerging Areas**: Cloud Forensics & Incident Response, IoT Device Forensics, Threat Intelligence Integration, Advanced Persistent Threat (APT) Investigations, Ransomware Response, Countermeasure Evaluation & Implementation.

Reading List

Additional Readings

	Title
1	Jason T. Luttgens, Matthew Pepe, Kevin Mandia. Incident Response & Computer Forensics, Third Edition. McGraw Hill (2014)
2	Gerard Johansen. Digital Forensics and Incident Response: Incident Response Techniques and Procedures. Packt Publishing (2020)
3	Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press (2013)
4	Don Murdoch. Blue Team Handbook: Incident Response Edition. (2014)