هيئة تقويم التعليم
Education Evaluation Commission
المركز الوطني للتقويم والاعتماد الأكاديمي
National Center for Academic Accreditation and Evaluation

ATTACHMENT 5.

T6. COURSE SPECIFICATIONS (CS)

Course Title:	**Forensics and Incident Response**
Course Code:	NES 483 - **Forensics and Incident Response**
Program:	Bachelor of Network Engineering and Security
Department:	Computer Engineering
Institution:	Al Yamamah University Riyadh
Approval Date	16 March 2019

College of Engineering and Architecture

Al Yamamah University

Riyadh, KSA

هيئة تقويم التعليم
Education Evaluation Commission

Course Specifications

Institution: Al Yamamah University	Date: 16 March 2019
College/Department :College of Engineering and Architecture/ Computer Engineering	

A. Course Identification and General Information

1. Course title and code: NES 483- Forensics and Incident Response

2. Credit hours: 3+1 = 4

3. Program(s) in which the course is offered.
(If general elective available in many programs indicate this rather than list programs)

Bachelor of Network Engineering and Security

4. Name of faculty member responsible for the course: Dr. Abid Ali Minhas

5. Level/year at which this course is offered:
Fourth Year/ 8th semester

6. Pre-requisites for this course (if any)
NES 481 Security Policies and Procedures

7. Co-requisites for this course (if any)
(No Co-requisites course that is no course which is going be delivered at the same time)

8. Location if not on main campus
Main Campus

9. Mode of Instruction (mark all that apply)

a. traditional classroom	✓	What percentage?	100
b. blended (traditional and online)		What percentage?	
c. e-learning		What percentage?	
d. correspondence		What percentage?	
f. other		What percentage?	

Comments:

B Objectives

1. What is the main purpose for this course? The main purpose of this course is to describe the knowledge of Forensics and Incident Response by Investigating and analyzing misappropriation of the useful information and recover, categorize and analyze the data. It also demonstrates the legal issues of Computer Forensics.
2. Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field) • Use of LMS(Learning Management System) that increases the use of IT for students • Referring the students to related website

C. Course Description (Note: General description in the form used in Bulletin or handbook)

Course Description: This course provides an introduction to the topics of basic terminologies in law, computer forensics, computer crimes, response to security incidents, Cybercrime investigation and prosecution. Students will learn how to do digital forensics/ analysis. They will learn tools of imaging different type of electronic media and then analysis of these images to retrieve the evidences. They will also learn that how an organization can set up a security response team, prepare for Security incidents and manage these incidents.

1. Topics to be Covered			
List of Topics		**No. of Weeks**	**Contact hours**
Week No.			
1.	**Basics of Crimes** (Definition of Crime, Crime Categories and Sentencing Guidelines, Cybercrimes, Statutes Amended to Keep Pace with Cybercrimes, Civil vs. Criminal Charges) **Information Warfare, Electronic Attack, and Terrorism** (Information Warfare, Terrorism and Cyberterrorism, FBI's Computer Forensics Advisory Board)	1	3
2.	**Computer Forensics Evidence and Investigations** (Evidence: The Starting Point for Understanding What Happened, Evidence Investigative Skills, Cybertrails of Evidence, Artifact, Inculpatory, and Exculpatory Evidence, Admissible Evidence, Federal Rules of Evidence, Circumstantial Evidence, Hearsay Evidence and Expert Testimony, Material Evidence) **Electronic Evidence: Technology and Legal Issues** (Deleted, But Not Gone, E-Mail Evidence)	1	3
3.	**Computer Forensics: A Growing Field and Practice Area** **Discovery** (Federal Rules of Civil Procedure, Federal Rules of Discovery) **Electronic Discovery** (E-Discovery) (Discovery of E-Evidence, Landmark Case Involving E-Discovery, Increased Demand for E-Discovery)	1	3
4.	**The Role of E-Evidence in Solving Physical and Computer Crimes** (E-Evidence Trails, Finding Hidden Files on a Computer, Knowing What to Look For, Answering the 5 Ws Helps in Criminal Investigations) **Computer Forensics Science** (Admissibility of Evidence, Tradeoffs to Be Considered)	1	3
5.	**Digital Signatures and Profiling** (Digital Signature Left by Serial Killer, Digital Profiling of Crime Suspects)	1	3

	Computer Forensics and the E-Evidence Collection Process (Unallocated Space and File Slack, Example of Standard Forensics Investigative Procedure) **Suppression, Probable Cause, and Search Warrants** (Withstanding Challenges to Evidence, Probable Cause and Search Warrants, Proper Procedure and Limitations Built into the Law, Conclusions and Lessons)		
6.	**Types of Motives and Cybercrimes** (Finding the Motive—The "Why" of the Crime, Computer Is the Crime Target, Computer Is the Crime Instrument, , Computer Is Incidental to Traditional Crimes, New Crimes Generated by the Prevalence of Computers) **Forensics Rules and Evidence Issues** (Chain of Custody Procedures, Report Procedures) **Computer Forensics Investigator's Responsibilities**	1	3
7.	**Managing the Life-Cycle of a Case** (Maintaining a Defensible Approach, Selecting the Right Tools for a Case) **Acquiring and Authenticating the E-Evidence** (Document and Collect the Data, Power Down or Unplug?, Create a Drive Image or Bit-Stream Image, Use a Forensically Clean Hard Drive for Copying, Verify the Accuracy of the Copy) **Searching and Analyzing the Data** (Effective Data Searches, Identify Data Types)	1	3
8.	**Investigative Environments and Analysis Modes** (Trusted Environments, Untrusted Environments) **Forensic Tools and Toolkits** (EnCase Forensic Version 5, EnCase Cybercrime Arsenal, Forensic Toolkit and Ultimate Toolkit, WinHex, Autopsy, Sleuth Kit, and dtSearch, Macintosh Forensic Software: BlackBag and MacQuisition, PDA Seizure) **Forensics Equipment** (Password Crackers, Portable Hard Disk Duplicators) **Certification and Training Programs**	1	3
9.	**Reasons for Policies and Procedures** (Personnel Hiring Issues, Personnel Training, Structure of a Forensics Unit)	1	3

	Pre-Case Preparations (Deciding to Take a Case, General Case Intake Form, Documenting the First Steps in the Case, Equipment in a Basic Forensics Kit) **Steps in the Forensic Examination** (Verify Legal Authority, Collect Preliminary Data, Determining the Environment for the Investigation, Securing and Transporting Evidence, Acquisition of Evidence Procedures)		
10.	**Examining the Evidence** (Physical Extraction or Examination, Logical Extraction or Examination, Bottom-Layer Examinations, Second-Layer Examinations, Third-Layer Examinations, Fourth-Layer Examinations, Fifth-Layer Examinations) **The Art of Forensics: Analyzing the Data** (File Analysis, Data Hiding Analysis, Time Frame Analysis) **Reporting on the Investigation** (Ongoing Documentation, Creating a Detailed Report)	1	3
11.	**Data, PDA, and cell phone forensics** Basic Hard Drive Technology, Other Storage Technologies, Personal Digital Assistant Devices (PDAs), Cellular Phones, Drive and Media Analysis, PDA Analysis, Cellular Phone Analysis, Disk Image , Forensic Tools, PDA/Cellular Phone Forensic Software	1	3
12.	**Mobile Forensics** Cellular networks, Retrieve Evidence from a Smartphone, Analyze Cell Phone Operating Systems, Understand How to Document a Cell Phone Investigation,	1	3
13.	**Incident Response** Types of incident response, Actions taken to deal with an incident, Rationale for Incident Response, Risk Analysis, Methodology of Incident Response, Forming and Managing an IR-Team, Basic Requirements of IR, Success Metrics, Organization of IR Team, Role of Computer Forensics	1	3
14.	**Investigating Windows_Linux and Graphics Files** Investigating Windows Systems, Finding User Data and Profiles in Windows Folders, Investigating System Artifacts, Investigating Linux Systems, Graphic File Forensics	1	3

15.	**E-Mail and Webmail Forensics** Importance of E-Mail as Evidence, Working with E-Mail, Working with Webmail, Working with Mail Servers, Examining E-Mails for Evidence, Working with Instant Messaging	1	3
	Total:	15	45

2. Course components (total contact hours and credits per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other:	Total
Contact Hours	Planed	45					45
	Actual	45					45
Credit	Planed	3					3
	Actual	3					3

3. Additional private study/learning hours expected for students per week. 6

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategy

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and intended learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy ought to reasonably fit and flow together as an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge** *After successful completion of the course students will be able to*		
1.1	*Describe* basic terminologies of FIR and describe how to perform computer crime investigations, the recovery and analysis of digital evidence, addressing legal and technical issues.	• Lectures, • Group discussions	• Written exams (quizzes, mid-term, and final exams) • Oral presentations Participation in class • Assignments/ Homework
1.2	*Outline* forensic examination techniques of Windows and Unix systems.	• Lectures, • Group discussions	• Written exams (quizzes, mid-term, and final exams) • Oral presentations Participation in class • Assignments/ Homework
2.0	**Cognitive Skills** *After successful completion of the course students will be able to*		
2.1	*justify* how an organization can set up a security response team, prepare for Security incidents and manage these incidents	• Lectures • Case studies • Presentation • Literature survey	• Written exams (quizzes, mid-term, and final exams) • Case studies • Oral presentations • Assignments/ Homework/ Reports • Literature survey
2.2	*analyze* the forensics incidents	• Lectures • Case studies • Presentation • Literature survey	• Written exams (quizzes, mid-term, and final exams) • Case studies • Oral presentations

			• Assignments/ Homework/ Reports • Literature survey
3.0	**Interpersonal Skills & Responsibility** *After successful completion of the course students will be able to*		
3.1	demonstrate their effective working in groups and exercise leadership when required	• Lectures • Case studies • Presentation • Literature survey	• Monitoring and grading students' performance on the mentioned teaching strategies.
4.0	**Communication, Information Technology, Numerical** *After successful completion of the course students will be able to*		
4.1			•
5.0	**Psychomotor**		
5.1	Not applicable		
5.2	Not applicable		

Levels: I = Introduction P = Proficient A = Advanced, X= Not applicable (NA) or (-)

5. Map course LOs with the program LOs. (Place course LO #s in the left column and program LO #s across the top.)

Course LOs #	**Program Learning Outcomes (Use Program LO Code #s provided in the Program Specifications)**									
	1.1	**1.2**	**1.3**	**2.1**	**2.2**	**3.1**	**3.2**	**3.3**	**4.1**	**4.2**
1.1	**P**	-	-	-	-	-	-	-	-	-
1.2	-	**P**	-	-	-	-	-	-	-	-
2.1	-	-	-	**P**	-	-	-	-	-	-
2.2	-	-	-	-	**P**	-	-	-	-	-
3.1	-	-	-	-	-	**P**	-	-	-	-
4.1	-	-	-	-	-	-	-	-	-	-

5. Schedule of Assessment Tasks for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Quizzes	All along	10%
2	Assignments/ Literature Survey/ Presentations/Projects/ Reports on Forensic Tools	All along	30%
3	Mid Exam	Week 8	20%
4	Final Exam	Week 16	40%
5			

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week) In addition to class lectures time, teacher is supposed to display his/ her advisory ten hours (10 hours per week) for the students outside his/ her office in order to have individual student consultations and academic advice.

E. Learning Resources

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) One lab with 24 PCs and Internet connection. An over-head projector is normally installed in every class and lab throughout the university campuses.
2. Computing resources (AV, data show, Smart Board, software, etc.) Data show projector, Can use a forensics online applications.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list) None.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) One lab with 24 PCs and Internet connection. An over-head projector is normally installed in every class and lab throughout the university campuses.
2. Computing resources (AV, data show, Smart Board, software, etc.) Data show projector, Can use a forensics online applications.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list) None.

G Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching At the end of the course, students receive feedback survey forms designed as per guidelines of NCAAA that are used to see the effectiveness of teaching.
2 Other Strategies for Evaluation of Teaching by the Program/Department Instructor Peer review visits are normally conducted among faculties wherever possible during academic year. During the lecture time Chair (Head)/ Dean of the department visits the classroom. At the end of each visit, faculties are usually set together to discuss related issues.
3 Processes for Improvement of Teaching • Feedbacks from students using different types of survey including Student Experience Survey (SES), Program Evaluation Survey (PES), and Alumni Survey (AS) are shown and discussed with faculty members to improve the teaching. • Specialized workshops and seminars are conducted throughout academic year to address specific teaching strategies and improvements.
4. Processes for Verifying Standards of Student Achievement (e.g. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution) Peer review and discussion with course coordinator. There should be a strong liaison with teacher from some external university/institute in order to exchange ideas related to marking/ evaluating quizzes and assignments.

5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.

At the end of each semester, Curriculum committee conducts a meeting with all faculty members in which surveys filled by the students and other feedbacks from faculty members are discussed. Effectiveness of the courses, mistakes done and weaknesses are discussed. These points are made basis for the planning for improvements for next semester/ year.

Name of Course Instructor: Dr.Abid Ali Minhas

Signature: _____ Date Specification Completed: 16 March 2019

Program Coordinator: _____

Signature: _____ Date Received: _____