

Course title	Code	semester	T+U	credit	ECTS
Forensic Informatics		7	2 + 0	2	2
<b>Prerequisite Courses</b>	None				
<b>Language of the Course</b>	English				
<b>Course Level</b>	Undergraduate				
<b>Type of Course</b>	Optional				
<b>Course Coordinator</b>					
<b>Instructors</b>					
<b>Course Assistants</b>					
<b>The aim of lesson</b>	Information about cyber crimes and the characteristics of these crimes is provided. In-depth knowledge of the elements of cyber crimes, which are frequently encountered in practice, is obtained. It is aimed to learn the characteristics of the protection measures that can be applied against cyber crimes and the decision and implementation mechanisms of these protection measures.				
<b>Course Content</b>	Within the scope of this course, first of all, general information about cyber crimes will be emphasized, then cyber crimes, which are frequently encountered in practice, will be examined in detail in accordance with the crime investigation technique, by evaluating court decisions, and the protection measures that can be applied to clarify cyber crimes and the conditions of these measures will be evaluated.				
<b>Course Learning Outcomes</b>	<p>Students who successfully complete this course;</p> <ol style="list-style-type: none"> <li>1. Knows the concept of cybercrime and the characteristics of these crimes.</li> <li>2. Evaluate the cyber crimes, which are frequently encountered in practice, according to the classical crime investigation method, taking into account the decisions of the Supreme Court.</li> <li>3. It determines which protection measures can be applied against cyber crimes, the conditions of these protection measures and the authorities that can decide on the protection measures.</li> </ol>				
<b>Weeks</b>	<b>Topics</b>				
one	Introduction and Introduction of Course Content				
2	The Concept of Cybercrime and Characteristics of Cybercrime				
3	Violation of the Confidentiality of Communications				
4	Listening and Recording Conversations Between People				
5	Violation of the Privacy of Private Life				
6	Recording Personal Data, Unlawful Giving and Capturing Data, Not Destroying Data				
7	Entering the Information System				
8	Entering the Information System				
9	Blocking, Corrupting, Destroying or Modifying the System				
10	Misuse of Debit or Credit Cards				
11th	Searching, Copying, and Confiscation of Computers, Computer Programs, and Logs				
12	Supervision of Communication via Telecommunication				
13	Monitoring with Technical Tools				
14	Expert examination				
15	Expert examination				
<b>General Competencies</b>					
Information about cyber crimes and the characteristics of these crimes is provided.					
<b>resources</b>					
<p>R. Doğan, “Information Crimes in the Turkish Penal Code No. 5237”, Adalet Publishing House, 2014.  A. Karagülmez, “Computer Crimes and Investigation-Prosecution Phases”, Seçkin Publishing, 5th Edition, 2014, ISBN: 9789750229336</p>					

H. Akarslan, IT Crimes, Seçkin Publishing, 2012, ISBN :9789750233166

### Evaluation System

The dates, days and hours of the Midterm Exam, Quiz, Final Exam and Evaluations will be announced later, according to the decision of the Faculty Administrative Board.

WITH PROGRAM LEARNING OUTCOMES COURSE LEARNING OUTCOMES RELATIONSHIP TABLE											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
LO1	3	3	3	3	3	3	3	3	5	3	4
LO2	3	3	3	3	3	3	3	3	5	3	4
LO3	3	3	3	3	3	3	3	3	5	3	4
LO: Learning Outcomes OP: Program Outcomes											
Contribution Level	1 Very Low		2 Low		3 Medium		4 High		5 Very High		

### Relation of Program Outcomes and Related Course

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
Forensic Informatics	3	3	3	3	3	3	3	3	5	3	4