

## Adli Bilişim Mühendisliği Müfredatı ve Gereksinimleri

Erhan AKBAL<sup>1\*</sup>, Şengül DOĞAN<sup>1</sup>, Mustafa KAYA<sup>1</sup>

Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü, Elazığ  
\*erhanakbal@firat.edu.tr

(Geliş/Received: 13.06.2016; Kabul/Accepted: 13.07.2016)

### Özet

Son yıllarda bilişim teknolojisinde yaşanan hızlı değişimler bu alanda yeni suç işleme potansiyelleri oluşturarak insanların günlük hayatını olumsuz yönde etkilemektedir. İşlenen bu suçlarla etkin mücadele edebilmek için, hukuk ve bilişimin kesiştiği alanda insan kaynakları ve laboratuvar altyapılarının geliştirilmesi ve yeni tanımlamaların yapılması gerekmektedir. Ancak çoğu zaman bu yöndeki çalışmaların geciktiği ve güncel problemleri çözmede yetersiz kaldığı gözlenmektedir. Bilişim suçlarını tanımlama, algılama, engelleme, suç ispatı ve delillendirme süreçleriyle ilgili yeni bir bilim dalı tanım süreci bütün gelişmiş ülkelerde başlatılmış ve bunun için lisansüstü ve lisans müfredat çalışmaları yapılmaktadır. Digital Forensics olarak adlandırılan bu disiplinin müfredatının bilişim teknolojilerinin sürekli yenilenmesinden dolayı çok dinamik bir yapıda olması gerekmektedir. Bu çalışmada, dünyadaki benzer ön lisans, lisans, lisansüstü ve özel kurs programları incelenerek lisans düzeyinde bir müfredat geliştirilmiştir. Eğitimin sağlıklı yürütülebilmesi için gerekli laboratuvar koşulları ve öğretim sonrasında istihdam alanları da incelenmiştir.

**Anahtar Kelimeler:** Adli Bilişim Eğitimi, Adli Bilişim Mühendisliği, Müfredat Tasarımı

## Digital Forensics Engineering Curriculum and Requirements

### Abstract

Digital crimes in the World through the development of IT have increased and have had negative impact on the social life. We have to educate human resources, set up a new substructure, and develop new identifications on this area law come across with IT to struggle with them (digital crimes). Although, most of the time, the studies relevant to this issue are observed, which are delayed and insufficient. A new discipline has been defined relevant to the process of identification, detection, preventing, be considered as a crime, and recording of evidence for digital crimes in all the developed countries, and also researchers have studied to develop a curriculum for undergraduate and graduate programs. The curriculum of this discipline called digital forensics must be had also a very dynamic structure caused of state of the art information technologies. In this study, a new curriculum for digital forensics graduate program was developed for the Turkish Higher Education System, while similar undergraduate and graduate programs at the top educational institutions of the world and course programs are taken as reference. The employment area after this curriculum and laboratories needed have been researched for the education good can be implemented.

**Keywords:** Digital Forensic Education, Digital Forensics Curriculum, Curriculum Development

### 1. Giriş

Fırat Üniversitesi yaklaşık 40000 lisans, 5000 yüksek lisans ve doktora öğrencisiyle Türkiye’de hizmet veren bir devlet üniversitesidir. Üniversitede bulunan Teknoloji Fakültesi bünyesinde 10 farklı bölüm bulunmakta ve yaklaşık 5000 öğrenci ile öğretim yapılmaktadır. Adli bilişim mühendisliği bölümü teknoloji fakültesi bünyesinde açılarak 2014 yılında öğrenci alımı gerçekleştirilerek eğitim öğretime başlamıştır. Türkiye’de ilk kez bu

bölümün eğitime başlayacak olması, doğru bir müfredat seçilmesi açısından büyük öneme sahiptir. Bu çalışmanın amacı, pratik karşılığını bulacak şekilde, öğrencilere en iyi öğretim programını sunarak, bu alanda kariyerine devam etmek isteyen öğrencileri sektöre en iyi şekilde hazırlayacak müfredat ve gereksinimlerin neler olduğu bilgisini sunmaktır. Müfredat oluşturulmasında dünyadaki benzer örnekler ayrıntılı incelenmiş ve günümüz şartları da dikkate alınarak, bilimsel öğretim metodlarına göre dersler belirlenmiştir. Oluşturulan müfredat

ile ülkemizde ve dünyada adli bilişim alanında ihtiyaç duyulan insan gücü açığını kapatabilecek bilgi birikimine sahip mühendisler yetiştirmek amaçlanmıştır.

Günümüzde mevcut teknolojinin hızlı bir şekilde gelişmesi ile tüm dünyada bilişim alt yapısı kullanılarak işlenen suçların her geçen gün yeni bir boyut kazandığı görülmektedir. Mevcut teknoloji, insanların kâğıt üzerindeki belge, doküman gibi kişisel ve iş sektöründe kullandıkları verileri sayısal ortama aktararak günlük faaliyetlerini kolaylaştırırken aynı zamanda elektronik ortamda bulunan kişisel verilerinin güvenliğinin sağlanması konusundaki kaygılarını da artırmaktadır [1]. Dünyada ve ülkemizde bilişim sektöründe işlenen suçlarla mücadele edebilmek için gerekli olan yetişmiş personel sayısı ve teknik altyapı çalışmaları yetersiz kalmaktadır. Bu suçların oranında artma görülen ülkeler çeşitli hukuksal ve teknik düzenlemeler ile belirli önlemler almaya çalışmışlardır [2]. Ülkemizde ise bilişim suçları üzerine yapılan çalışmalar ve düzenlemeler, bilişim teknolojileri alt yapısının yaygın kullanılmasının sağlanması ve bilişim suçları kapsamı farkındalığının daha uzun bir süreçte gerçekleşmesi nedenleri ile daha geç olmuştur.

Bilişim alt yapısı kullanılarak işlenen suçlar 1960'lı tarihlere dayanmakla beraber yine aynı yıllarda bilimsel yayınlarda "bilgisayar suçu" kelimeleri telaffuz edilmeye başlanmıştır [2]. Ancak yaygın bir şekilde 1980'li yıllarda bilgisayarların, özellikle iş hayatımızda kullanılmaya başlanması ve sonrasında günlük hayatımızın bir parçası olması artık "bilgisayar suçu" terimini çok sık duyulan ve hukuksal açıdan önlem alınması gereken bir tabir haline getirmiştir [3]. O yıllardan günümüze kadar bilgisayar teknolojisindeki hızlı gelişmelere paralel olarak bilgisayar tabanlı işlenen suçlarda hızlı bir artış ve çeşitlilik görülmektedir [4]. Bilgisayar tabanlı işlenen bu suçların maddi kayıplar oluşturabilmesi yanında aynı zamanda elektronik ortamda bulunan mevcut verilerin güvenliğini sağlama gerekliliği göz önüne alındığında bu suçların farklı bir disiplin adı altında incelenmesi gerekliliği günümüzde zorunlu hale gelmiştir [5].

Bu çalışmanın ana katkıları aşağıdaki gibidir.

1. Çalışmada Adli bilişim mühendisliği eğitiminin dünyadaki örnekleri ortaya konulmuştur.

2. Günümüz teknolojileri ve gelecek teknolojilere göre güncel bir müfredat ve dersler belirlenmiştir.

3. Adli bilişim mühendisliği eğitiminin verilebilmesi için gerekli gereksinimler ortaya konmuştur.

4. Bu alanda yeni bölüm çalışmaları sürdürecektür kurumlara yol gösterilmiştir.

Bu çalışmada, ilgili çalışmalara bölüm 2'de yer verilmiştir. Bölüm 3'de mevcut programların analizi yapılmış, Bölüm 4'de ise programın amacından bahsedilmiştir. Adli Bilişim Mühendisliği Bölümü ders müfredatı ve ders içerikleri Bölüm 5'de verilmiştir. Bölüm 6'da, bölümden mezun olacak öğrencilerin çalışma olanaklarından bahsedilmiş ve sonuçlar Bölüm 7'de değerlendirilmiştir.

## 2. İlgili Çalışmalar

Bilişim alanında mevcut verilerin güvenliğinin sağlanması, takibi ve yazılım/donanım alanında gerekli yapının oluşturulması günümüzün en önemli araştırma alanlarının başında gelmektedir. Ülkelerin hukuksal boyutunu içerecek şekilde bilişim sistemlerinin güvenlik alt yapılarının oluşturulması ve devamının sağlanması için pek çok yeni yöntem ve yapı önerilmektedir. Garfinkel (2010) bilişim alanında ön plana çıkan bilişim sistemleri güvenliğinin sağlanması ve korunması için adli bilişim alanındaki verilerin analizi ve değerlendirilmesi sürecinde gelecek 10 yıl için bir araştırma planı sunmuştur. Bu plan; adli bilişim yazılımları ve donanımlarının geliştirilmesi için yeterli bütçenin ayrılması ve bu anlamda yetişmiş insan gücünden faydalanılarak sürecin ihtiyaçlar doğrultusunda iyileştirilmesinin sağlanmasını önermiştir [6]. Garfinkel et al. (2009) ise adli bilişim alanında yapılan araştırmalarda veri setlerinin belirli standartlara kavuşturularak sınırlılıkların kaldırılabilceğini ve böylelikle incelenen verilerin değerlendirilmesinde başarımın artırılabilceğini savunmuştur [7]. Carrier (2002) adli bilişim analiz araçlarını ve onların yasal kullanımını incelemiştir. Carrier yaptığı araştırmada delillerin güvenilirliğinin yasal boyutlarda değerlendirilebilmesi için ülkenin yasalarına uygun süreçte inceleme yapabilecek lisanslı ve açık kaynak kodlu yazılımların geliştirilmesi

gerektiğini belirtmiştir [8]. Bu araştırmalar göstermektedir ki bilişim sistemleri güvenliğinin sağlanmasında ülkelerin hukuksal boyutlarının bilinmesi ve bu bağlamda hareket edilmesi gerekmektedir. Adli bilişim sürecinin hem bilişim hem de hukuksal boyutunun ortak platformda değerlendirilebilmesi için belirli bir standarda erişmesi gerekmektedir. Bu yapının oluşturulması için günümüzde pek çok çalışma yapılmıştır. Reith et al. (2002) teknolojinin gelişmesi paralelinde dijital suçların sayısındaki artışı göz önüne alarak genel bir metodoloji oluşturulması gerektiğini savunmuştur. Geliştirilecek metodolojinin mevcut düzendeki suçların tespiti ve değerlendirilmesini sağlamanın yanı sıra hali hazırda gerçekleşmemiş suçları da kapsayacak nitelikte olması gerektiğini vurgulamıştır [9]. Gottschalk et al. (2005) Kuzey Amerika’da Adli Bilişim eğitimi veren lisans, yüksek lisans ve sertifika programlarını değerlendiren bir anket çalışması hazırlamışlardır. Bu anket çalışması ile öğrencilerin aldığı dersleri ve kredilerini de temel alarak eğitimin başarımı artırmak ve yeni açılacak programlar için müfredat tasarımı, öğretim üyelerinin niteliği, ayrılması gereken bütçe gibi etmenleri araştırmışlardır [10]. Logan et al. (2005) bilgisayar bilimleri alanında eğitim gören öğrencilerin çalışacakları birimlerde öncelikli görevlerinin yanı sıra veri güvenliğinin sağlanması alanında mesleki yeterliliğe sahip bireylerin yetiştirilmesi için bilgisayar bilimleri alanında eğitim alan öğrenciler için müfredatın güncellenmesi gerektiğini ve öğrencilerin bu alt yapıyı bilerek meslek hayatına başlamalarının gerekliliğini savundu [11].

### 3. Mevcut Programların Analizi

Adli bilişim mühendisliği bölümü farklı disiplinlerin bir araya gelmesiyle oluşan bir disiplindir. Bunlar ceza hukuku, muhasebe ve yönetim, bilgisayar bilimleri ile ilgili bilgisayar, bilgi ve bilişim sistemleri, sistem mühendisliği, enformatik, siber güvenlik gibi disiplinlerdir. Bu çalışmada özellikle adli bilişim mühendisliği alanına odaklanılmış ve buna uygun bir müfredat çalışması gerçekleştirilmiştir. Dünya da Adli bilimlerle ilgili birçok üniversite eğitim vermektedir. Fakat verilen eğitimlerin az sayıda olanı doğrudan adli bilişime odaklanmaktadır.

Ayrıca lisans derecesinde eğitim veren kurum sayısı sınırlı sayıdadır.

Çalışmada dünyada adli bilişim mühendisliği alanında lisans, lisansüstü ve kurs programı olarak eğitim veren kurumlar incelenmiştir. Bu alanda eğitim veren ve incelenen kurumlar Tablo 1’de verilmiştir [12-26].

**Tablo 1.** Adli bilişim mühendisliğinde eğitim veren ve incelenen kurumlar

Üniversite	Program	Lisans	Lisans Üstü	Kurs/ Sertifika
Abertay Üniversitesi, 2015	Digital Forensic Programı	+	+	
Sam Houston State Üniversitesi, 2015	Digital Forensics Programı	+	+	
Marshall Üniversitesi, 2015	Marshall Forensic Science Programı			
Birmingham Alabama Üniversitesi, 2015	Computer Forensic Programı			+
Rhode Islanda Üniversitesi, 2015	Digital Forensic Programı			+
Bloomsburg Üniversitesi, 2015	Digital Forensics Programı	+		
Ball State Üniversitesi, 2015	Criminal Justice and Criminology Fakültesi Digital Forensic Programı			+
Westminster Üniversitesi, 2015	Computer Forensics Programı		+	
Liverpool John Moores Üniversitesi, 2015	Computer Forensics Programı	+		
South Wales Üniversitesi, 2014	Computer Forensics Programı		+	
Birmingham City Üniversitesi, 2015	Forensic Computing Programı	+		
George Mason Üniversitesi, 2015	Computer Forensics Programı			+
Teesside Üniversitesi, 2015	Computer and Digital Forensics Programı	+		
Portsmouth Üniversitesi, 2015	Forensic Computing Programı	+		
Sunderland Üniversitesi, 2015	Computer Forensics Programı	+		
De Montfort Üniversitesi, 2015	Forensic Computing Programı	+		

Programlar incelendiğinde Adli bilişim mühendisliği eğitiminin adli bilimlerin üç temel konusunu kapsadığı görülmektedir. Bunlar bilim, delil ve hukuktur [27]. Ayrıca tam bir adli bilişim mühendisliği eğitimi için 4 yıllık eğitime ihtiyaç duyulduğu da görülmektedir [28].

Genel olarak adli bilişim mühendisliğinin temel ilgi alanları Tablo 2’de verilmiştir. Müfredat oluşturulurken belirtilen ilgi alanları göz önünde bulundurulmuştur.

**Tablo 2.** Adli bilişim programının temel ilgi alanları

Bilgisayar Bilimleri	Kriptolama ve Güvenlik
	Ağ İletişimi
	Sistem ve Analiz
Prosedürler, Metotlar ve Politikalar	Adli Bilimler / Kriminoloji
	Olay Soruşturma
	Devlet Kuralları
Yasal Sistem ve Kanunlar	Yasal Prosedürler / Etik
	Bilgisayar / İş Kanunları
	Anayasal Kanunlar
Adli Bilişim	Veriye el koyma ve Koruma
	Dijital Delil Analizi
	Dokümantasyon ve Sunum
	Siber Suçlar ve Mücadele

#### 4. Programın Amacı

Bilişim teknolojilerinde yaşanan hızlı değişim ve gelişim günlük hayatımızı pek çok alanda olumlu yönde etkilerken aynı zamanda kontrol edilmesi güç sorunları da beraberinde getirmektedir. Bu sorunların başında bilişim alt yapısı kullanılarak işlenen suçlar için alınması gereken tedbirler, tespit ve ispat için gerekli süreçler ve hukuksal boyutların değerlendirilmesi gelmektedir. Ancak bilişim alt yapısı kullanılarak işlenen suçlar insanların suç işleme eğilimleri ve yetenekleri paralelinde her geçen gün farklı boyutlara taşınmaktadır [29]. Böylelikle bilişim teknolojilerinin sunmuş olduğu imkânlarla daha önce belli bir bölge ile sınırlı olan bu suçlar mevcut yapıyı aşarak küresel hale gelmektedir [30].

Bilişim suçları için yapılacak araştırmada suç mahallinin incelemesi işlemi bu alanda eğitim almış uzman kişiler tarafından yapılmalıdır. Ancak günümüzde delillere el koyma ve inceleme aşamasında görevlendirilebilecek yetişmiş uzman personel sayısında yeterli seviyeye ulaşılamamıştır. Kurumların birçoğu bu eksikliği ülke içi veya dışından özel eğitim kuruluşları, kurslar veya bu alanda faaliyet gösteren ticari kuruluşlardan kısa süreli eğitimler vasıtasıyla tedarik etmeye çalışmaktadırlar. Dolayısıyla bu durum, ilgili kurumların bilişim suçlarını algılama, takip edebilme, delillendirme ve sonuçlandırma süreçlerini olumsuz etkilemektedir. Suç mahalli incelemesi sırasında

pek çok delil, doğru şekilde delilin olay yerinden alınmaması sonucu geri dönülmeyecek şekilde zarar görebilmektedir. Bu nedenle dijital delilerin elde edilmesinden incelenip sonuçlandırılacağı sürecin bütünü bu alanda eğitim görmüş kişilerin yapması büyük önem taşımaktadır [31]. Adli bilişim mühendisliği, alana özgü dersler ve uygulamalar ile kişilerin bu alanlarda uzmanlaşmasını sağlamakla beraber aynı zamanda temel mühendislik eğitimi ile öğrencilerde ortak kazanımların oluşturulması amaçlanmaktadır. Adli bilişim mühendisliği eğitimin temelinde üç amacı bulunmaktadır. Bunlar:

- Siber Güvenlik: Suç oluşmadan önce gerekli önlemlerin alınması ile kişi, kurum ve kuruluşların zarar görmesini engellemektir. Bunun için amaca uygun şekilde bilişim sistemlerinin seçilmesi, planlanması, yapılandırılması ve gerekli güvenlik önlemlerinin oluşturularak yapının korunaklı hale getirilmesi bilgilerinin sağlanması gerekmektedir.
- Dijital Deliller: Bilişim alt yapısı üzerinden işlenen suçlarla ilgili verileri doğru almak, analiz etmek ve hukuksal yapıya uygun olarak raporlandırmaktır.
- Yasalar: Hem eğitimin verildiği ülkede hem de diğer örnekleri dikkate alınarak dijital suçlarla ilgili yasal düzenlemelerde etkin bilgiye sahip olmaktır. Bu nedenle müfredat içerisinde mutlaka eğitimin verildiği ülkeye ait yasal mevzuatlar ve yapı ile ilgili bilgi kazandırılmalıdır. Böylelikle bu üç temel amacın sağlanabilmesi için gerekli olan uygulamalı ve teorik derslerin belirlenerek, mezun olduktan sonra öğrencilerin yeterli bilgiye sahip olabilmeleri amaçlanmıştır.

#### 4.1. Öğrenci kazanımları

Adli bilişim mühendisliği bölümü lisans eğitimi, 4 yıllık eğitim öğretim sürecinde 120 teori ve 66 uygulama dersi olmak üzere toplamda 186 ders saatinden oluşmaktadır. Teori derslerinin oranı %64 iken uygulama derslerinin oranı %36'dır. Bu derslerin 107 saati bölümle ilgili teknik dersleri, 14 saati hukuksal içeriği, 29 saati

temel mühendislik derslerini ve 30 saati ise staj ve işyeri eğitimini içermektedir.

Oluşturulan müfredat ile her bir öğrenci için aşağıda belirtilen kazanımların sağlanması amaçlanmıştır.

1. Temel mühendislik olgusunun kazandırılması

2. İyi derecede bilgisayar ve ağ bilgisinin oluşturulması

3. Adli bilişim incelemelerinde kullanılan yazılım, donanım ve yöntemlerin uygulamalı olarak öğrenilmesi

4. Ceza hukuku, yasal sorumluluklar ve kişisel veriler ile ilgili yasal düzenlemelerin öğrenilmesi

5. Takım çalışmasına uyum sağlama ve sosyal becerilere sahip olabilmek

7. Alanında iyi derecede uygulama becerisine sahip olarak iş yaşantısına kolay adapte olabilmek

Adli bilişim mühendisliği Türkiye’de ilk kez eğitim öğretime başladığı için müfredatın seçiminde güncel durum ve gelecekteki ihtiyaçlarda analiz edilmiştir.

## 4.2. Gereksinimler

Adli bilişim mühendisliği eğitimi verilebilmesi için öncelikle alanında uzmanlaşmış bir akademik kadroya ihtiyaç duyulmaktadır. Bilgisayar bilimleri alanında bilişim suçları üzerinde çalışmalar yapmış akademisyenler ile Hukuk alanında bilişim hukuku üzerine uzmanlaşmış akademisyenlerin bir araya gelmesi gerekmektedir. Ayrıca derslerin işleneceği altyapının doğru bir biçimde oluşturulması gerekmektedir. Öğrencilerin derslerde almış oldukları teorik bilgileri uygulamalı olarak kavrayabilmesi ve derslerin uygulama saatlerinin değerlendirilmesi oluşturulacak altyapıyla doğrudan ilgilidir.

Temel olarak 5 farklı eğitim ortamı ve araçlarına ihtiyaç duyulmaktadır. Bunlar;

- Veri inceleme Laboratuvarı ve Araçları,
- Görüntü İnceleme Laboratuvarı ve Araçları
- Ses İnceleme Laboratuvarı ve Araçları
- Ağ uygulamaları Laboratuvarı
- Bilgisayar Laboratuvarı

Veri inceleme ve Kurtarma Laboratuvarı ve Araçları, dijital delillerin incelenerek sınıflara ayrılması süreçlerinin kavranması için gereklidir. Veri incelemede literatürde kullanılan birçok

yazılım ve donanım bulunmaktadır [32]. Bunların temin edilerek öğrencilerin ders uygulamalarında ve diğer zamanlarda kullanabilmesinde imkân tanımak gerekmektedir. Ayrıca donanımsal veri kurtarma araçlarının da bulunması gerekmektedir.

Görüntü inceleme Laboratuvarı ve Araçları; dijital delillerin veri inceleme araçlarıyla incelenmesinin ardından suça konu olan delillerde görüntüyle ilgili inceleme yapılması durumunda farklı yazılım ve donanım araçlarıyla incelenmesi gereklidir. Bu nedenle görüntü incelemede kullanılan araçların içinde bulunduğu bir laboratuvar ortamına ihtiyaç duyulmaktadır. Özellikle görüntü iyileştirme, görüntü manipülasyonu, görüntü içerisindeki bilgilerin çıkarımı gibi süreçlerin öğrenciler tarafından kavranması gerekmektedir.

Ses inceleme Laboratuvarı ve Araçları; ses kayıtları ile ilgili verilerin incelenmesiyle, kayıtlın ilgili kişilere aidiyetinin belirlenmesi, kimliklendirme ve tanıma süreçleri, kayıt üzerindeki gürültülerin giderilerek anlaşılabilir hale getirilmesi, kayıtlardaki değişikliklerin tespit edilmesi, kayıtlın orijinalliğinin belirlenmesi, kayıttaki seslerin kalitesinin artırılması ve yazılı hale getirilmesi sağlanmaktadır. Bu kapsamda kullanılan yazılımsal ve donanımsal araçların içerisinde bulunduğu bir uygulama ortamına ihtiyaç duyulmaktadır.

Ağ Uygulama Laboratuvarı; Adli bilişim mühendisliği eğitiminin amaçlarından ilki olan suç oluşmadan önceki önlemlerin alınmasının sağlanabilmesi için öğrencilerin ağ ortamını benzetimini yapabileceği ve içerisinde çeşitli ağ donanımlarının bulunduğu bir laboratuvara ihtiyaç duyulmaktadır. Siber saldırılarla ilgili davranışların analiz edilmesi sağlanarak bu alandaki uygulama kapasitesi artırılmış olacaktır. Bilgisayar Laboratuvarı; genel olarak çeşitli araştırmaların yapılabilmesi, öğrencilerin internet teknolojilerini ve yazılımsal çalışmalarını üzerinde yapabileceği, içerisinde performansı yüksek bilgisayarların bulunduğu bir laboratuvar oluşturulması gerekmektedir.

## 5. Müfredat

Adli bilişim mühendisliği lisans eğitim 4 yıl süre ile 8 yarıyıldan oluşmaktadır. Ayrıca 20+20 gün yaz stajı bulunmaktadır. 7. Yarıyıl da öğrencilerin uygulamalı olarak alanıyla ilgili bir

kurumda işyeri stajı yapması gerekmektedir. Müfredatta bulunan derslerin belirlenmesinde bölümün ihtiyaçları ve adli bilişim kavramının içindeki konular dikkate alınmıştır. Tablolarda derslerin teorik ve uygulamalı ders saatleri ve kredileri gösterilmiştir. Ayrıca derslerin AKTS (Avrupa Kredi Toplama ve Transfer Sistemi) kredilerinin ne olması gerektiği de belirlenerek müfredata eklenmiştir. Böylece eğitimin ülkemizin de içerisinde bulunduğu Avrupa ülkelerinde geçerliliği de sağlanmıştır. Tablolarda T teorik ders saatini, U uygulamalı ders saatini, K krediyi göstermektedir.

### 5.1. I. yıl müfredatı

Birinci yıl müfredatı dersleri Tablo 3’de gösterilmiştir. Öğrencilerin temel mühendislik becerilerini kazanabilmesi için Fizik, Matematik vb. dersleri bulunmaktadır. Bilişim alanında temelin oluşması için alanla ilgili dersler müfredata konulmuştur.

**Tablo 3. I. yıl müfredatı**

Birinci Yıl					
I. Yarıyıl			II. Yarıyıl		
Dersin adı	K	AKTS	Dersin adı	K	AKTS
Algoritma ve Programlama	4	7	Programlama Dilleri	4	7
Adli Bilişim Müh. Temelleri	4	7	Bilgisayar Sistemleri	4	7

#### 5.1.1. I. yıl müfredatı ders içerikleri

Algoritma ve programlama ve Programlama dilleri dersi ile temel programlama mantığının kavranarak programlama dillerinin tanıtılması ve uygulamalı olarak dillerin kullanılması amaçlanmıştır.

Adli bilişim mühendisliğinin temelleri dersi ile Adli bilişim kapsamına giren temel kavramların kavranması amaçlanmıştır. Bilgisayar sistemleri dersi bilgisayar sistemlerinin yapılandırılmasını, kullanılan teknolojileri ve yöntemleri kapsamaktadır.

### 5.2. II. yıl müfredatı

İkinci yılda verilen dersler Tablo 4’de verilmiştir.

**Tablo 4. II. yıl müfredatı**

İkinci Yıl					
III. Yarıyıl			IV. Yarıyıl		
Dersin adı	K	AKTS	Dersin adı	K	AKTS
Bilgisayar Ağları	3	6	Ağ ve Sistem Güvenliği	3	5
Bilişim Suçu Donanımları	3	5	İnternet ve E-Ticaret Güvenliği	4	6
Bilgi Güvenliği ve Şifreleme Teknikleri	4	6	İstatistik ve Olasılık	2	2
Adli Bilişim Kanunları	4	5	Mesleki İngilizce	3	3
Mühendislik Matematiği	3	4	Çoklu Ortam Bilgi Sistemleri	4	6
Sosyal Seçmeli Ders	2	2	Lineer Cebir	2	3
			Sosyal Seçmeli Ders	2	3

#### 5.2.1. II. yıl müfredatı ders içerikleri

Bilgisayar ağları, ağ ve sistem güvenliği dersleri öğrencilerin ağ ve üzerinden oluşabilecek güvenlik tehditlerini çözmelerini amaçlamaktadır.

Bilişim suçu donanımları dersi, adli bilişim kapsamına giren ve suça konu olabilecek dijital donanımları kapsamaktadır.

Adli bilişim kanunları, yasaların ve ceza hukukunun bilişimle ilgili olan bölümlerini kapsamaktadır.

Mühendislik Matematiği, Lineer Cebir ve İstatistik ve Olasılık dersleri mühendislik becerilerinin kazanılabilmesi için ileri matematik bilgilerini kapsamaktadır.

İnternet ve E-Ticaret Güvenliği, Çoklu Ortam Bilgi Sistemleri dersleri internet teknolojileri ve multimedya sistemler üzerinden gerçekleştirilebilecek dolandırıcılıkların anlaşılabilmesi için müfredata eklenmiştir.

### 5.3. III. yıl müfredatı

Üçüncü yılda verilen dersler Tablo 5’de gösterilmiştir. İlk iki yılda temel bilgileri edinen öğrencilere alanla ilgili daha ayrıntılı bilgilerin verildiği dersler eklenmiştir.

**Tablo 5.** III. yıl müfredatı

Üçüncü Yıl					
V. Yarıyıl			VI. Yarıyıl		
Dersin adı	K	AKTS	Dersin adı	K	AKTS
Veri Tabanı Yönetim Sistemleri	4	6	Dosya Sistem Analizi	4	5
Elektronik Deliller ve Bilgisayar Suçları	4	7	Kimliklendirme Yöntemleri ve Biyometri	4	6
İşletim Sistemleri	4	5	Web Üzerinden Bilgiye Erişim	4	5
Bilişim Suçu İnceleme Yazılımları	4	6	İş Hukuku	2	2
Bilişim Suçu İnceleme Donanımları	4	6	<b>Seçmeli Dersler</b>	8	12

**Tablo 6.** III. yıl müfredatı teknik seçmeli ders listesi

Online Suç Takibi	4	6
Optimizasyon Teknikleri	4	6
Veri Sıkıştırma	4	6
Veri Madenciliği	4	6
Metin Tabanlı Bilgiye Erişim Sistemleri	4	6
Biyoinformatik	4	6
Kablosuz/ Mobil Çoklu Ağlar	4	6
Güvenlik Öncelikli Bilgisayar Sistemleri	4	6
Veri Yapıları	4	6
Sayısal Yöntemler	4	6

### 5.3.1. III. yıl müfredatı ders içerikleri

Derslerin kapsadığı konular aşağıda belirtilmiştir.

Bilişim suçu inceleme yazılım ve donanımları dersleri ile öğrencilerin bu alanda kullanılan yazılım ve donanımları öğrenmesi amaçlanmıştır. Laboratuvar uygulamaları ile birlikte dijital delillerin incelenme süreçleri tam olarak anlaşılacak olmaktadır.

Veri tabanı yönetim sistemleri dersi ile veri tabanı işleme, veri modelleme, ilişkisel gerçekleştirimin temelleri, sorgu dilleri gibi kavramlar gösterilmektedir.

İşletim sistemleri dersi bilgisayar sistemi yapısı, işletim sistemi yapısı, süreçler, iş parçacıkları, bellek yönetimi, sanal bellek, yığın depolama araçları, işlemci iş dağıtımı, süreç eş zamanlama, ölü kilitler, dosya sistemi ara yüzü, dosya sistemleri gerçekleştirimi, girdi/çıkış sistemleri, farklı işletim sistemlerinin

kıyaslanması, sistem yapıları konularını kapsamaktadır.

Elektronik deliller ve bilgisayar suçları dersi bilgisayar suçları araştırmalarında yasal konular ve bilimsel yöntemlerle suç soruşturmalarına sistematik yaklaşımlar. Dosya sistemleri, veri kurtarma, internet takibi, elektronik delil toplama ve inceleme süreçleri ve araçları konularını kapsamaktadır.

Dosya sistem analizi dersi ikili kodlama, dosya formatları, bilgisayar suç kategorileri, ağ izleme ve analizi, klasik suçlarda elektronik deliller, dosya sistemleri, aktif sistemlerin analizi, şifre korumalı dosyalar, şifrelenmiş dosyalar, kurumsal veri güvenliği konularını kapsamaktadır.

Kimliklendirme yöntemleri ve biyometri dersi biyometrik özelliklerin ve özellik setlerinin elde edilmesi, sınıflandırılması, karşılaştırılması, karar mekanizması, doğruluk analizleri ve performanslarının değerlendirilmesi, konularını kapsamaktadır.

Web üzerinden bilgiye erişim dersi metin işlemede zipf kanunları, geri bildirim, sorgu dilleri, işlemleri ve yapısal sorgular, erişim modelleri, boolean modeli, uzay vektör modeli, metin benzerlik ölçüleri, istatistiksel dil modelleri, sosyal ağ analizi, öneri sistemleri ve veri filtreleme, içerik tabanlı filtreleme, kullanıcı geribildirimleri, web madenciliği, bulut bilişim, gelecek nesil arama motorları, ileri düzey arama, bilgi çıkarımı, çoklu dillerde bilgi çıkarımı konularını kapsamaktadır. Ayrıca öğrencilerin Tablo 6'da verilen teknik seçmeli derslerden de 2 ders seçebilmesine olanak sağlanmıştır.

### 5.4. IV. yıl müfredatı

Dördüncü yılda verilen dersler Tablo 7'de gösterilmiştir.

**Tablo 7.** IV. yıl müfredatı

Dördüncü Yıl					
I. Yarıyıl			II. Yarıyıl		
Dersin adı	K	AKTS	Dersin adı	K	AKTS
İşyeri Eğitimi	3	20	Elektronik Delil Toplanması ve Analizi	4	6
			Yazılım Etiği	4	4
			Bitirme Projesi	1	5
			<b>Seçmeli Dersler</b>	8	12

**Tablo 8.** IV. yıl müfredatı teknik seçmeli ders listesi

Konuşma Tanıma ve Üretme	4	6
Hareketli Yazılım Geliştirme	4	6
Karar Destek Sistemleri	4	6
Bilgisayarla Görü	4	6
İnsan Bilgisayar Etkileşimi	4	6

#### 5.4.1. IV. yıl müfredatı ders içerikleri

Dördüncü yılın ilk yarıyılı işyeri eğitimini kapsamaktadır. Öğrencilerin derslerde aldıkları teorik ve uygulamalı eğitimleri bir dönem boyunca kurum ve kuruluşlar bünyesinde pekiştirmesi amaçlanmaktadır. İkinci yarıyılıda ise aşağıda belirtilen dersler ve içerikleri verilecektir.

Elektronik delil toplanması ve analizi dersi sistem kayıtlarının analizi, program ve işletim sistemi kurulum kayıtları, işletim sistemi olay günlüğü, sistem olay günlüğü analizi, güvenlik duvarı ve saldırı tespit sistem kayıtları, online sohbet analizi, konuşma kayıtları analizi, kaydedilmiş görüşme geçmiş kalıntılarının analizi, bağlantı olay günlüğünün analizi, kullanılan online sohbet hesaplarının tespit edilmesi, sabit disk ve harici disk üzerindeki gizli alanların analizi, e-posta analizi, mesaj başlıklarının analizi ve sahte e-postaların belirlenmesi, sahte e-posta ayırımının analizi, mobil aygıt analizi, Windows kayıt defteri analizi, veri yedeklerinin adli bilişim açısından öneminin tespiti konularını kapsamaktadır.

Yazılım etiği dersi bilişim teknolojilerinde etik değerlendirme prensipleri ve modelleri, kötü amaçlı yazılım araştırmaları, Windows, şifre, eposta, web uygulamaları, web sayfası alan adı ve diğer sisteme izinsiz girme türleri, taşınabilir bilgisayarlarda bilişim suçları, ses bağlantılarında izinsiz giriş, güvenlik açığı testleri, istismar saldırıları, güvenlik duvarı, saldırı tespit sistemleri, kaçak giriş, saldırı tespit etmenin yolları, sistem ağları güvenliği konularını kapsamaktadır.

Bitirme projesi dersi ile öğrencilerin mezun olabilmesi için alanla ilgili bir proje gerçekleştirmeleri gerekmektedir.

Ayrıca öğrencilerin Tablo 8’de verilen teknik seçmeli derslerden de 2 ders seçebilmesine olanak sağlanmıştır.

## 6. Mezunların İş Alanı

Adli bilişim mühendisliğinde temel amaç, kurumlar veya özel sektörler için bilişim alanında faaliyet gösteren firmaların ihtiyaç duyduğu uygulama becerisi yüksek mühendisleri yetiştirmektir. Aynı zamanda bilişim suçları ile ilgili adli vakalarda kanun ve yönetmeliklerin öngördüğü şekilde deliller ve bilgiler sunabilmekte bölümün bir diğer amacını oluşturmaktadır. Bu alanda eğitim alan mezunlar bilişim suçlarından kişi, kurumu ya da firmayı koruyacak yetiye sahip vasıflı uzmanlardır. Bu nedenle programdan mezun olan bireyler, kişi, şirket ya da kurumların ihtiyaçlarını karşılayacak şekilde elektronik delil elde etme ve inceleme, adli yazılım ve donanım, kanun ve yönetmeliklerle ilgili iş çözümleri üretme ve yürütme konusunda deneyime sahip olacaklardır.

Adli bilişim mühendisleri mezun olduktan sonra belirlenen eğitim programı ile farklı sektör ve kuruluşlarda doğrudan istihdam edilmesi hedeflemektedir. Mezunlar bilişim teknolojilerinin kullanıldığı herhangi bir sektörde, sistem, donanım, yazılım ve bilgisayar ağları, bilişim suçları, hukuki sorumluluklar, bilişim suçlarından korunma konularında çağdaş bilgilere sahip ve istihdamı sağlayacak kurum ya da kuruluşların belirtilen sorunlarla karşılaşmasını önleyebilecek yetilere sahip olacaklardır. Böylelikle ülkemizde ve dünyada bu alanda ihtiyaç duyulan yetişmiş insan gücüne önemli katkılar sağlanabilecektir. Özellikle son yıllarda artan bilişim kaynakları üzerinden işlenen adli vakalardan dolayı birçok devlet kuruluşu özel sektörden ve farklı ülkelerden adli bilişim uzmanlığı hizmetleri satın alma yoluna gitmektedir. Ülkemizde adli bilişim mühendisliği programı sayesinde aynı zamanda farkındalık oluşturularak yerli yazılım ve donanım oluşturma alt yapısı da sağlanabilecektir.

## 7. Sonuçlar

Bu çalışmada adli bilişim mühendisliği eğitiminin gereklilikleri ortaya konulmuştur. Bilişim teknolojilerinin ve kullanım alanlarının hızlı gelişimi karşısında bu alanda eğitim veren kurumlarında müfredatlarını güncel tutmaları gerekmektedir. Özellikle bilişim teknolojilerinin kullanımının artması bu alanda ortaya çıkan suç



türlerini de farklılaştırmaktadır. Adli bilişim mühendisliği eğitimi alan kişilerin yeni teknolojiler ve kavramlar hakkında bilgili olması iş hayatında karşılaşacakları sorunları çözmeye daha başarılı olmalarını sağlayacaktır. Çalışmada adli bilişim mühendisliği eğitimi adı altında literatürde eğitim veren kurumlar incelenmiştir. Mevcut verilen eğitimlerin müfredat dersleri incelenerek günümüz teknolojilerine en uygun derslerin belirlenmesi sağlanmıştır. Böylece bu alanda eğitim-öğretim faaliyetleri sürdürecektür kurumlara yol gösterilmiştir. Bölümün eğitim-öğretimi sürdürebilmesi için gereksinimlerinin neler olduğu da ortaya konmuştur. Özellikle öğrencilerin uygulamalı eğitimler görmesini sağlayacak farklı laboratuvar ortamlarının oluşturulması eğitimin doğru sürdürülebilmesi için büyük önem taşımaktadır. Adli bilişim mühendisliği eğitimi disiplinler arası bir yapıya sahip olduğundan doğru akademik kadroya sahip olmak gerekmektedir. Bilişim teknolojileri alanında bilgi güvenliği, bilgisayar ağları, kriptolama, adli bilişim gibi alanlarda uzmanlaşmış akademisyenlerin bölüm bünyesinde bulunması eğitimin başarısını arttıracaktır. Ayrıca hukuk alanında bilişim hukuku, kişisel bilgilerin korunması gibi konularda uzmanlaşmış akademisyenlerin de bulunması gerekmektedir.

## 8. Kaynaklar

1. Turhan, O. (2006). Bilgisayar Ağları ile İlgili Suçlar, Planlama Uzmanlığı Tezi, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Hukuk Müşavirliği.
2. Boğa, U. (2011). Bilişim Suçlarıyla Mücadele Yöntemleri, Uzmanlık Tezi, T.C. Radyo Televizyon Üst Kurulu.
3. Eoghan, C. (2011). Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet.
4. Liu, J. (2006). Developing an Innovative Baccalaureate Program in Computer Forensics, *Frontiers in Education Conference*, 36th Annual, 1-6.
5. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M. (2005). Computer Forensics Programs in Higher Education: A Preliminary Study, *SIGCSE '05 Proceedings of the 36th SIGCSE technical symposium on Computer science education*, **37** (1), 147-151.
6. Garfinkel, S.L. (2010). Digital forensics research: The next 10 years, *Digital Investigation*, **7**, S64-S73, 2010.
7. Garfinkela, S., Farrella, P., Roussev, V., Dinolta, G. (2009). Bringing science to digital forensics with standardized forensic corpora, *Digital Investigation*, **6**, S2-S11.
8. Carrier, B. (2002). Open Source Digital Forensics Tools: The Legal Argument, *Stake*.
9. Reith, M., Carr, C., Gunsch, G. (2002). An Examination of Digital Forensic Models”, *International Journal of Digital Evidence*, **1**(3), 1-12.
10. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M. (2005). Computer forensics programs in higher education: a preliminary study. *ACM SIGCSE Bulletin*, **37** (1), 147-151.
11. Logan, P.Y., Clarkson, A. (2005). Teaching students to hack: curriculum issues in information security, *ACM SIGCSE Bulletin*, **37** (1), 157-161.
12. Internet: Abertay University, Forensic Sciences, <http://www.abertay.ac.uk/courses/ug/forsc/>, 10.04.2015.
13. Internet: Sam Houston State University, Digital Forensics Sciences, <http://www.shsu.edu/programs/master-of-science-in-digital-forensics/>, 09.03.2015.
14. Internet: Marshall University, Forensic Science Center, <http://forensics.marshall.edu/>, 08.02.2015.
15. Internet: The University of Alabama At Birmingham University, Computer and Information Sciences, <https://cis.uab.edu/academics/graduates/master-program/computer-forensics-and-security-management/>, 11.03.2015.
16. Internet: Bloomsburg University, Digital Forensics, [http://www.bloomu.edu/digital\\_forensics](http://www.bloomu.edu/digital_forensics), 02.01.2015.
17. Internet: Ball State University, Digital Forensics and Criminal Justice, <http://cms.bsu.edu/academics/collegesanddepartments/cjc/academics/minors/digitalforensics>, 05.02.2015.
18. Internet: University of Westminster, Cyber Security and Forensics, <http://www.westminster.ac.uk/courses/subjects/computer-science-and-software-engineering/postgraduate-courses/full-time/p09fpcyf-cyber-security-and-forensics-msc>, 12.12.2014.
19. Internet: Liverpool John Moores University, Computer Forensics, <https://www.ljmu.ac.uk/study/courses/undergraduates/2015/computer-forensics-mcomp>, 05.12.2014.
20. Internet: University of South Wales, Computer Forensics, <http://courses.southwales.ac.uk/courses/563-bsc-hons-computer-forensics>, 11.02.2015.
21. Internet: Birmingham City University, Forensic Computing, <http://www.bcu.ac.uk/courses/forensic-computing>, 20.04.2015.

- 22.** Internet: George Mason University, Computer Forensics, [http://catalog.gmu.edu/preview\\_program.php?catoid=5&poid=3308](http://catalog.gmu.edu/preview_program.php?catoid=5&poid=3308), 25.01.2015.
- 23.** Internet: Teesside University, Computer and Digital Forensics, [http://www.tees.ac.uk/undergraduate\\_courses/Crime\\_Scene\\_&\\_Forensic\\_Science/BSc\\_\(Hons\)\\_Computer\\_and\\_Digital\\_Forensics.cfm](http://www.tees.ac.uk/undergraduate_courses/Crime_Scene_&_Forensic_Science/BSc_(Hons)_Computer_and_Digital_Forensics.cfm), 05.11.2014.
- 24.** Internet: Portsmouth University, Forensic Computing, <http://www.port.ac.uk/courses/computing-and-creative-technologies/bsc-hons-forensic-computing/>, 15.01.2015.
- 25.** Internet: University of Sunderland, Computer Forensics, <http://www.sunderland.ac.uk/courses/appliedsciences/undergraduate/computer-forensics/>, 22.12.2014.
- 26.** Internet: De Montfort University, Forensic Computing, <http://www.dmu.ac.uk/study/courses/undergraduate-courses/forensic-computing.aspx>, 28.12.2015.
- 27.** Pollit, M. (2004). What is Digital Forensics?, *Presentation at DFEWG*.
- 28.** Hankins, R., Uehara, T., Liu, J. (2009). A Comparative Study of Forensic Science and Computer Forensics, *2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement*, 231-239.
- 29.** Zhijun, L., Ning, W. (2009). Developing a Computer Forensics Program in Police Higher Education, *4th International Conference on Computer Science & Education*, 1431-1436.
- 30.** Swartz, J. (2006). Cybercrime spurs college courses in digital forensics.
- 31.** Akbal, E., Güneş, F. (2016). Adli Bilişim Mühendisliği Eğitiminin Kurumlar Açısından Önemi, *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, **4**, S395-S402.
- 32.** Cole, A. (2006). Computer Forensics Examiners, *Ezine Article*.