



**MOBİL CİHAZ ADLİ BİLİŞİMİ KAPSAMINDA İMAJ ALMA SÜRECİNE
İLİŞKİN KARAR DESTEK SİSTEMİ OLUŞTURULMASI**

Furkan YILMAZ

DOKTORA TEZİ

ADLİ BİLİŞİM ANA BİLİM DALI

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

NİSAN 2023

Furkan YILMAZ tarafından hazırlanan “MOBİL CİHAZ ADLI BİLİŞİMİ KAPSAMINDA İMAJ ALMA SÜRECİNE İLİŞKİN KARAR DESTEK SİSTEMİ OLUŞTURULMASI” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Hüseyin ÇAKIR

Eğitim Bilimleri Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

.....

Başkan: Prof. Dr. Refik SAMET

Bilgisayar Mühendisliği, Ankara Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

.....

Üye: Prof. Dr. Mustafa ALKAN

Elektrik-Elektronik Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

.....

Üye: Prof. Dr. Olgun DEĞİRMENCİ

Hukuk, TOBB Ekonomi ve Teknoloji Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

.....

Üye: Doç. Dr. Talip KELLEGÖZ

Endüstri Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

.....

Tez Savunma Tarihi: 19/04/2023

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Prof. Dr. Aslıhan TÜFEKÇİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Furkan YILMAZ

19/04/2023

MOBİL CİHAZ ADLİ BİLİŞİMİ KAPSAMINDA İMAJ ALMA SÜRECİNE İLİŞKİN KARAR DESTEK SİSTEMİ OLUŞTURULMASI

(Doktora Tezi)

Furkan YILMAZ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

NİSAN 2023

ÖZET

Adaletin zamanında tecellisine adli bilişimin katkısı yadsınamaz olduğundan, bu kapsamdaki sürecin en kısa zamanda sağlıklı şekilde nihayete erdirilmesi önemli bir gerekliliktir. Günümüzde mobil cihazlar, barındırdığı veri itibarıyla adli bilişim açısından en önemli delil kaynaklarından birisidir. Mobil cihazların gerek çeşitliliğindeki gerekse de kabiliyetlerindeki hızlı artış, mobil cihaz adli bilişim sürecini günden güne daha karmaşık hale getirmektedir. Aynı zamanda, bu faaliyetlerin devamını sağlayacak yeni personellerin sürece adaptasyonunu zorlaştırmaktadır. Mobil cihazlardan imaj alınmasındaki başarı, mobil cihaz adli bilişimi sürecinin tamamını doğrudan etkilemektedir. Bu tez çalışması kapsamında mobil cihazların imajlarının alınması sürecinde, personelin hızlı ve etkin karar vermesini sağlamak amacıyla bir karar destek sistemi geliştirilmiştir. Bu amaçla, mobil cihaz adli bilişim sürecini yürüten bir birimin faaliyetleri incelenmiş, problem tanımı yapılmış ve gerekli veriler toplanmıştır. Bu veriler üzerinde literatürde yer alan çeşitli algoritmalar test edilmiş ve verileri açıklama kabiliyetleri belirlenmiştir. Bu yolla, verinin içerdiği girdi-çıkı ilişkisini en iyi şekilde açıklayan yöntem, karar destek modeli olarak seçilmiştir. Karar destek sisteminin diğer bileşenlerine yönelik teknik gereksinimlerin belirlenmesi amacıyla kalite fonksiyonu göçerimi metodolojisi takip edilerek, karar vericilerin ihtiyaç ve beklentileri mümkün mertebe sağlıklı şekilde geliştirilen sisteme uygulanmıştır. Erişilebilirlik ve esneklik ihtiyaçlarına daha yüksek düzeyde cevap verdiği için, önerilen karar destek sistemi web tabanlı bir yazılım olarak geliştirilmiştir. Yazılımın çalıştırdığı karar destek sistemi, hem mobil cihazdaki arızanın tespitinde hem de yapılan tespit neticesinde mobil cihazın imajının alınması için yapılacak işlemlere karar verilmesinde destek sağlamaktadır. Geliştirilen yazılım belirli bir süre ile mobil cihaz adli bilişim personeli tarafından kullanılmış ve yazılımı kullanan personelden kullanımı sonucunda geri bildirimleri istenmiştir. Geri bildirimlerin analizi, karar destek sistemi yazılımının kullanımının kolay olduğu, anlaşılır olduğu ve mobil cihaz adli bilişim sürecine gerek hız gerekse de doğruluk açısından katkı sağlayacağını göstermiştir.

Bilim Kodu : 92401

Anahtar Kelimeler : Adli bilişim, dijital delil, imaj alma, mobil cihaz adli bilişimi, karar destek sistemi, karar ağacı algoritması, kalite fonksiyon göçerimi

Sayfa Adedi : 180

Danışman : Doç. Dr. Hüseyin ÇAKIR

DEVELOPING A DECISION SUPPORT SYSTEM REGARDING THE ACQUIRING IMAGE PROCESS WITHIN THE SCOPE OF MOBILE FORENSICS

(Ph. D. Thesis)

Furkan YILMAZ

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

APRIL 2023

ABSTRACT

The contribution of digital forensics to the timely manifestation of justice cannot be denied, therefore, it is an important requirement to bring the process in this scope to a healthy conclusion as soon as possible. Nowadays, mobile devices are one of the most important sources of evidence in terms of digital forensics due to the data they contain. The rapid increase in both the diversity and capabilities of mobile devices makes mobile forensics processes more complex day by day. At the same time, this makes it difficult for new personnel to adapt to the process that will continue these activities. The success of acquiring images from mobile devices directly affects the entire mobile forensics process. In the scope of this thesis, a decision support system was developed to ensure that personnel can make quick and effective decisions in the process of acquiring images of mobile devices. For this purpose, the activities of a unit carrying out mobile forensics were examined, problem definition was made, and necessary data were collected. Various algorithms in the literature were tested on these data, and their abilities to explain the data were determined. In this way, the method that best explains the input-output relationship of the data was selected as the decision support model. Following the quality function deployment methodology to determine the technical requirements for other components of the decision support system, the needs and expectations of decision-makers were applied to the developed system as much as possible. Due to its higher level of accessibility and flexibility needs, the proposed decision support system was developed as a web-based software. The decision support system run by the software supports both the detection of malfunctions in mobile devices and the decision-making process for acquiring the image of the mobile device as a result of the detection. The developed software was used by mobile forensics personnel for a certain period of time and feedback was requested from personnel using the software. The analysis of the feedback showed that the decision support system software is easy to use, understandable, and contributes to the mobile forensics process in terms of both speed and accuracy.

Science Code : 92401

Key Words : Digital forensics, digital evidence, acquiring image, mobile forensics, decision support system, decision tree algorithm, quality function deployment

Page Number : 180

Supervisor : Assoc. Prof. Dr. Hüseyin ÇAKIR

TEŞEKKÜR

Benim içim oldukça yoğun geçen doktora eğitimim ve tez sürecim boyunca değerli yardımlarını eksik etmeyen, bana yol gösteren ve önümü açan değerli danışman hocam Doç. Dr. Hüseyin ÇAKIR’a,

Tez izleme sürecimde bana yol gösteren, değerli tavsiyeleriyle ışık tutan ve hayatımda karşılaştığım diğer problemlerde dahi danışabildiğim saygıdeğer hocalarım Prof. Dr. Olgun DEĞİRMENCİ ve Doç. Dr. Talip KELLEGÖZ’e,

Takıldığım yerde haftanın her günü, günün her saati arayabildiğim ve her seferinde cevap aldığım kıymetli abilerim Hamza Aytaç DOĞANAY ve Dr. Onur CERAN’a,

Çalışmam boyunca bana destek olan mesai arkadaşlarımdan öte kardeşlerim olan Bilal USLU, Fatih DEMİR ve Oğuzhan KAYAR’a,

Teknik problemleri aşmam konusunda bilgisiyle bana yön gösteren, destek olan arkadaşlarım Oğuzhan AYDİN ve Murat AVŞAR’a

En önemlisi de ben tüm bu akademik telaşe içindeyken, yuvamızdaki durumu hep en iyi şekilde idare eden, bana sabır gösteren ve her zaman desteğini hissettiğim eşim Özge YILMAZ’a

Teşekkürlerimi sunarım.

Bu çalışma esnasında en çok ondan fedakârlık ettiğimi düşündüğüm, kimi zaman kendisinden saklanarak, kimi zaman uyumasını bekledikten sonra tamamladığım bu çalışmayı, bittiğinde henüz 3 yaşında olan canım oğlum Çağatay Efe YILMAZ’a atfediyorum...

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ	x
ŞEKİLLERİN LİSTESİ	xii
RESİMLERİN LİSTESİ.....	xiv
SİMGELER VE KISALTMALAR.....	xv
1. GİRİŞ	1
2. ADLİ BİLİŞİM.....	11
2.1. Adli Bilişim Nedir?	11
2.2. Dijital Delil ve Delil Zinciri	12
2.2.1. Dijital Delil.....	13
2.2.2. Delil Zinciri	14
2.3. Türkiye’de Adli Bilişim	17
2.3.1. Ceza Muhakemesi Kanunu	17
2.3.2. Adli ve Önleme Arama Yönetmeliği	21
2.3.3. Avrupa Siber Suçlar Sözleşmesi	22
2.3.4. Türkiye’de adli bilişim faaliyetleri	24
3. MOBİL CİHAZ ADLİ BİLİŞİMİ	27
3.1. Mobil Cihazlar.....	27
3.2. Mobil Cihaz Adli Bilişimi Süreçleri.....	29
3.2.1. Cihaza ilk müdahale	29
3.2.2. İmaj alma	31
3.2.3. İnceleme	35
3.3. Mobil Cihaz Adli Bilişimi Araçları	40
3.4. Teknik Müdahale Yöntemleri	42
3.4.1. Yazılımsal müdahale	42
3.4.2. Fiziksel Müdahale.....	43

Sayfa

4. KARAR DESTEK SİSTEMLERİ	45
4.1. Karar Destek Sisteminin Özellikleri.....	48
4.2. Karar Destek Sistemi Türleri.....	50
4.2.1. Model tabanlı karar destek sistemi	51
4.2.2. Veri tabanlı karar destek sistemi.....	51
4.2.3. Bilgi tabanlı karar destek sistemi.....	52
4.2.4. İletişim tabanlı karar destek sistemi	53
4.2.5. Doküman tabanlı karar destek sistemi	53
4.3. Karar Destek Sistemi Oluşturma	54
4.3.1. Model yönetim modülü.....	55
4.3.2. Veri yönetim modülü.....	55
4.3.3. Kullanıcı arayüz modülü.....	56
4.4. Karar Ağacı (Decision Tree) Algoritması	58
5. KALİTE FONKSİYON GÖÇERİMİ.....	63
5.1. Kalite Fonksiyon Göçerimi Faydaları	64
5.2. Kalite Fonksiyon Göçerimi Aşamaları.....	65
5.2.1. Kalite evi.....	65
5.2.2. Ürün tasarımı	69
5.2.3. Sürecin Planlanması.....	70
5.2.4. Üretimin Planlanması	70
6. YÖNTEM.....	71
6.1. Yöntemin Özeti	71
6.2. Verinin Toplanması ve Değerlendirilmesi	73
6.3. Yazılım İçin Kalite Fonksiyon Göçerimi Uygulanması.....	76
6.3.1. Kalite evinin bileşenleri.....	76
6.3.2. Kalite evinin oluşturulması ve yazılıma uygulanması	85
6.4. Karar Destek Sisteminin Oluşturulması	86
6.5. Web Tabanlı Yazılımın Oluşturulması.....	90
6.6. Yazılımın Değerlendirilmesi İçin Soruların Belirlenmesi.....	100

	Sayfa
7. BULGULAR.....	107
7.1. Mobil Cihaz Adli Bilişimine Etki Eden Öznitelikler	107
7.1.1. Mobil cihaz adli bilişimine etki eden öznitelikler konusunda uzman görüşleri	107
7.1.2. Mobil cihaz adli bilişimine ilişkin toplanan verilerin analizi.....	108
7.1.3. Mobil cihaz adli bilişimine etki eden özniteliklerin önemleri	126
7.2. Mobil Cihaz Adli Bilişimi Kapsamında İmaj Alma Sürecine İlişkin Karar Destek Sisteminden Beklentiler	127
7.2.1. Karar destek sistemi yazılımı için müşterinin sesi ve önem düzeyleri	127
7.2.2. Karar destek sistemi yazılımı için müşterinin sesi ve önem düzeylerinin karşılanması için teknik gereksinimler	129
7.2.3. Karar destek yazılımının değerlendirilmesi.....	129
8. SONUÇ VE ÖNERİLER	135
KAYNAKLAR	139
EKLER.....	150
EK-1. Mobil cihazlarda imaj almaya etki eden faktörlere ilişkin uzman görüş formu	151
EK-2. Mobil cihazlarda imaj almaya etki eden faktörlere ilişkin uzman görüş formu (İngilizce).....	152
EK-3. Etik kurul onayı	153
EK-4. Emniyet Genel Müdürlüğünden alınan izin.....	157
EK-5. Müşterinin sesi tespiti için görüşme formu.....	158
EK-6. Oluşturulan kalite evi.....	159
EK-7. Yazılım bileşenleri diyagramı.....	160
EK-8. Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri.....	161
EK-9. Geri Bildirim Ekranı İçin Uzman Görüş Formu	178
EK-10. Geri Bildirim Ekranı İçin Uzman Görüş Formu (İngilizce)	179
ÖZGEÇMİŞ	180

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 4.1 Veri seti örneği.....	60
Çizelge 5.1. İlişki sayısı ve anlamları (çinpolat, 2007)	68
Çizelge 6.1. Talepler ve önem düzeyleri.....	78
Çizelge 6.2. Teknik gereksinimler	79
Çizelge 6.3. Korelasyon matrisi	80
Çizelge 6.4. Hedef yazılım için ilişki matrisi	81
Çizelge 6.5. Planlama matrisi	83
Çizelge 6.6. Gerçek ve hedef değerler tablosu	85
Çizelge 6.7. Yazılım için oluşturulan kalite evi.....	86
Çizelge 6.8. Sınıflandırma algoritmalarının başarı oranları.....	87
Çizelge 6.9. Rapidminer karar ağacı algoritmalarının kıyası	88
Çizelge 6.10. Özniteliklerin önem düzeyleri	88
Çizelge 7.1. Cihaz markasına ilişkin frekans tablosu	109
Çizelge 7.2. İşletim sistemi sürümü frekans tablosu.....	110
Çizelge 7.3. Hafıza çipi markası frekans tablosu.....	112
Çizelge 7.4. Cihazın şifreli olma durumuna ilişkin frekans tablosu	112
Çizelge 7.5. Ekran arıza durumuna ilişkin frekans tablosu	113
Çizelge 7.6. Port arıza durumuna ilişkin frekans tablosu	113
Çizelge 7.7. Anakart arıza durumuna ilişkin frekans tablosu	113
Çizelge 7.8. Cihazın parçalanmış olma durumuna ilişkin frekans tablosu	113
Çizelge 7.9. Yazılımsal arızalı olma durumuna ilişkin frekans tablosu.....	114
Çizelge 7.10. Root ihtiyacı olma durumuna ilişkin frekans tablosu	114
Çizelge 7.11. Port değişimi durumuna ilişkin frekans tablosu	114
Çizelge 7.12. Batarya değişim durumuna ilişkin frekans tablosu.....	114
Çizelge 7.13. Ekran değişimi işlemine ilişkin frekans tablosu	115
Çizelge 7.14. Basit tamir işlemine ilişkin frekans tablosu.....	115
Çizelge 7.15. J-tag işlemine ilişkin frekans tablosu.....	115
Çizelge 7.16. Chip-off işlemine ilişkin frekans tablosu.....	116
Çizelge 7.17. Root işlemine ilişkin frekans tablosu.....	116
Çizelge 7.18. İmaj alma işlemi sonucuna ilişkin frekans tablosu	116

Çizelge	Sayfa
Çizelge 7.19. Anakart arızası ve sonuca ilişkin çapraz tablo	118
Çizelge 7.20. Cihazın markası ve sonuca ilişkin çapraz tablo	119
Çizelge 7.21. Cihazın parçalanmış olma durumu ve sonuca ilişkin çapraz tablo	120
Çizelge 7.22. Cihazın şifreli olma durumu ve sonuca ilişkin çapraz tablo	121
Çizelge 7.23. Cihazın ekran arızası olma durumu ve sonuca ilişkin çapraz tablo	121
Çizelge 7.24. Hafıza çipi markası ve sonuca ilişkin çapraz tablo	123
Çizelge 7.25. Cihazın işletim sistemi ve sonuca ilişkin çapraz tablo	124
Çizelge 7.26. Cihazın port arızası olma durumu ve sonuca ilişkin çapraz tablo	125
Çizelge 7.27. Cihazın yazılımsal arıza durumu ve sonuca ilişkin çapraz tablo	126
Çizelge 7.28. Özniteliklerin önem düzeyleri	127
Çizelge 7.29. Talepler ve önem düzeyleri	128
Çizelge 7.30. Teknik gereksinimler	129
Çizelge 7.31. Yazılımın kullanım kolaylığına ilişkin sorular ve cevaplar	131
Çizelge 7.32. Yazılımın anlaşılabilirliğine ilişkin sorular ve cevaplar	132
Çizelge 7.33. Yazılımın mobil cihaz adli bilişimi sürecine katkısına ilişkin sorular ve cevaplar	134

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 3.1. Mobil cihaz adli bilişimi araçları	32
Şekil 4.1. Yönetim seviyelerinde karar tipleri	46
Şekil 4.2. Turban ve aronson’a göre ideal bir karar destek sisteminin özellikleri ve yetenekleri	50
Şekil 4.3. Karar destek sistemleri temel bileşenleri	55
Şekil 4.4. Karar destek sistemi oluşturulması adımları.....	58
Şekil 4.5. Bir karar ağacı yapısı	59
Şekil 5.1. Kalite evi.....	66
Şekil 6.1. Yaşlara göre kişilerin dağılımı.....	73
Şekil 6.2. Tecrübe yıllarına göre kişilerin dağılımı	74
Şekil 6.3. Eğitim durumlarına göre kişilerin dağılımı	74
Şekil 6.4. Yaşlara göre dağılım.....	77
Şekil 6.5. Tecrübe yıllarına göre dağılım.....	77
Şekil 6.6. Eğitim durumlarına göre dağılım.....	78
Şekil 6.7. Karar destek sistemi modeli.....	89
Şekil 6.8. Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi bileşenleri	90
Şekil 6.9. RapidMiner işleyişi akış şeması	91
Şekil 6.10. Kullanıcı girişi ve cihaz eklemeye ilişkin aktivite diyagramı.....	94
Şekil 6.11. Arıza giriş aşamasına ilişkin aktivite diyagramı.....	96
Şekil 6.12. Yapılacak işlemlere ilişkin aktivite diyagramı	98
Şekil 6.13. Sonuç ekranına ilişkin aktivite diyagramı	99
Şekil 6.14. Uzmanların yaşlara göre dağılımı.....	101
Şekil 6.15. Uzmanların tecrübe yıllarına göre dağılımı	102
Şekil 6.16. Uzmanların eğitim durumlarına göre dağılımı	102
Şekil 6.17. Yaşlara göre kişi dağılımı.....	104
Şekil 6.18. Tecrübe yıllarına göre kişi sayısı	105
Şekil 7.1. Markaların sıklığına ilişkin grafik	110

Şekil	Sayfa
Şekil 7.2. İşletim sistemi sıklık grafiği	111
Şekil 7.3. Hafıza çipi marka sıklığı.....	112



RESİMLERİN LİSTESİ

Resim	Sayfa
Resim 6.1. İstatistik takip ekranı	93
Resim 6.2. Karar destek sistemiyle arıza tespit ekranı (örnek)	95
Resim 6.3. Kullanıcı tarafından yapılan işlemleri görüntüleyebildiği ekran.....	97
Resim 6.4. Mobil cihazın imajının alınması için yapılacak işlem diyagramı (örnek)...	97
Resim 6.5. Sonuç ekranı	99



SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

f

%

Açıklamalar

frekans

yüzdelik

Kısaltmalar

Açıklamalar

CART

Sınıflandırma ve regresyon ağacı

CDR

Arama detay kaydı

CHAID

Ki-kare otomatik etkileşim algılama

COE

Avrupa Konseyi

EGM

Emniyet Genel Müdürlüğü

GPS

Küresel konumlandırma sistemi

GSM

Küresel mobil iletişim sistemi

ICCID

Entegre devre kartı kimliklendirmesi

IEF

İnternet Kanıt Bulucu

IMEI

Uluslararası mobil ekipman kimliği

IMSI

Uluslararası mobil abone kimliği

IOT

Nesnelerin interneti

ISP

Sistem içinde programlama

JTAG

Ortak test eylem grubu

KDS

Karar destek sistemi

KFG

Kalite fonksiyon göçerimi

MSISDN

Mobil istasyon entegre hizmetleri dijital ağı

NIST

Ulusal Standart ve Teknoloji Enstitüsü

PCB

Baskılı devre kartı

PDA

Kişisel dijital asistan

PIN

Kişisel kimliklendirme numarası

PUK

Kişisel kilit açma anahtarı

RAM

Rastgele erişimli bellek

SIM

Abone kimliklendirme modülü

SPN	Servis sağlayıcı adı
SSMDB	Siber Suçlarla Mücadele Daire Başkanlığı
SUS	Sistem kullanılabilirlik ölçęęi
TBMM	Türkiye Büyük Millet Meclisi
TÜİK	Türkiye İstatistik Kurumu
UFED	Evrensel Adli Çıkarım Cihazı



1. GİRİŞ

Teknoloji, günlük yaşamın bir parçası değil artık kendisi olmuştur. Doğumla birlikte 11 haneli kimlik numarasının alınmasıyla başlayan sayısallaşan (dijitalleşen) hayata ilişkin en önemli bilgiler de dijital olarak tutulmaya başlanmıştır. Türkiye’de 2021 yılı verilerine göre %88,5’i internete erişim aracı olarak kullanılan mobil cihazlar, niteliği itibariyle en sık kullanılan ve sağlık durumu, resimler, iletişim, konum, ilgi alanları, zevkler, bankacılık bilgileri gibi en mahrem bilgileri barındıran teknoloji haline gelmiştir (TÜİK, 2022). Mobil teknolojilerin yaygınlaşmasının sonucu olarak dijital teknolojiler çeşitlenmekte, günlük yaşamın her bir noktasında varlığını göstermektedir. Kısaca teknoloji, hayata her gün daha fazla girmekte ve insan hayatı dijitalleşmektedir; ancak bilişim alanındaki bu gelişmeler bir yandan hayatımızı kolaylaştırmakta bir yandan da beraberinde bazı riskleri getirmektedir. (Yılmaz ve Güllüoğlu, 2020)

Bir suç ile karşılaşıldığında, suçun aydınlatılmasına ilişkin oldukça önemli bulgular, dijital materyallerden elde edilmektedir. Örneğin, Amerika Birleşik Devletleri’nde 2005 yılında incelenen bir disket, 1974’ten beri polis tarafından yakalanmayan ve en az 10 kurbanın hayatını kaybetmesinden sorumlu BTK (bind-torture-kill) seri katiline yönlendirmiştir (National Institute of Justice, 2020).

Bir suç dolayısıyla gerçekleştirilen aramada kişisel bilgisayar, tablet, cep telefonu, sim kart, hafıza kartı, harici harddisk, USB bellek gibi dijital materyaller ile karşılaşılmakta, bunlar üzerinde arama işleminin gerçekleştirilmesi ve elde edilen bulguların analiz edilmesi gerekmektedir. Adli bilişim faaliyetleri kapsamında dijital materyallerden delil elde edilmektedir. Ancak dijital delil yığını dünyada bir problem halini almıştır. İrlanda Ulusal Polisi tarafından hazırlanan raporda dijital materyallere ilişkin yürütülen inceleme ve raporlama süresinin 4 yılı aşmış olduğu belirtilmiştir (Lillis, Becker, O’Sullivan ve Scanlon, 2016).

Adli bilişim alanındaki uzmanların, delillerin raporlanmasıyla ilgili güvenilir kararlar vermesi hayati öneme sahiptir. Adli bilişim uygulayıcısı olan personel için dijital soruşturmaların sayısının çokluğu ve karmaşıklığı göz önüne alındığında biçimlendirilmiş karar verme modelinin eksikliği bir sorun teşkil etmektedir (Horsman, 2019).

Bunun yanı sıra taşıdıkları veri hacimlerinin gittikçe artması, mobil cihazlardaki işletim sistemleri ve dosya formatlarının çeşitlenmesi ile inceleme ve analiz için standart tekniklerin bulunmamasının sonucu olarak çeşitli sorunlar meydana gelmektedir (Scanlon ve Kechadi, 2014).

Sıklıkla başvurulmuş delil elde etme yöntemi olan adli bilişim uygulamaları, günümüzde hacim ve çeşitlilik (Lillis ve diğerleri, 2016) (Scanlon ve Kechadi, 2014) problemiyle karşı karşıya kalmıştır. Bu büyük yığılma aşmak için karşılaştığı olayda kullanılacak aracın seçilmesi de süreç için çok önemlidir (Ramadhani, Wahyuni ve Pratama, 2020).

Bilişim teknolojileri kullanılarak, elde edilen verinin toplanması, işlenmesi ile organizasyonların doğru ve hızlı karar vermesi için karar destek sistemlerine sıklıkla başvurulmaktadır. Teknolojinin suçta kullanımının yaygınlaşması gibi, suçla mücadelede kullanılması da kaçınılmaz bir hale gelmiştir. Bu sebeple suçla mücadele, suçları aydınlatma açısından karar destek sistemlerine başvurulması da beklenen bir sonuçtur.

Bu çalışmada sürecin en verimli ve etkili şekilde hızlandırması amacıyla adli bilişim faaliyetlerine ilişkin bir karar destek sistemi tasarlanmıştır. Bu sayede diğer dijital materyal türlerine göre nicelik ve bulundurduğu veri açısından nitelik olarak daha ön plana çıkan mobil cihazlardan imaj alınması süreçlerine destek olunması hedeflenmiştir.

Karar destek sistemi yazılımı için öncelikle yurt içinde ve yurt dışındaki uzmanlarla görüşmeler neticesinde mobil cihaz adli bilişim süreçlerinde önem arz eden faktörler belirlenmiş; sonrasında cihaza ait bilgiler, cihazın durumuna ilişkin tespitler ve bu cihaza yapılan işlemlere ilişkin veriler toplanmıştır. Tasarlama işlemi sırasında yazılımın ihtiyaçları için Kalite Fonksiyon Göçerimi yöntemine başvurulmuştur. Bu sayede yazılımı kullanması muhtemel personelin talepleri dikkate alınarak, oluşturulan teknik gereksinimler yerine getirilmiştir. Tüm bu elde edilen veriler ışığında karar ağacı algoritmaları test edilmiştir. En başarılı algoritma olarak tespit edilen ID3 karar ağacı algoritması kullanılarak bir karar destek sistemi oluşturulmuştur. Ortaya çıkan bu yazılımın son kullanıcı tarafından kullanılabilmesi için veri tabanları, yazılım ve arayüz hazırlanmıştır.

Hazırlanan yazılımın başarısının ölçülmesi ve geliştirilmesi için kullanımı hedeflenen kitleyle uygulanmıştır. Uygulama sonucunda alınan geri bildirimler neticesinde, yazılımı

kullanmanın kolay ve anlaşılır olduđu tespit edilmiştir. Ayrıca mobil cihaz adli bilişimi süreçlerine katkı sağlayacağı beklenmektedir. Bunun yanı sıra uygulayıcılar tarafından kullanıldıkça yapılan işlemler depolanmaktadır ve bu sayede karar destek sistemi için kullanılan veri tabanı büyütülebilecektir. Ayrıca yeni problemler için yeni çözümler de bu sisteme entegre edilme imkanı bulunmaktadır.

Çalışmanın sonunda bu karar destek sisteminin mobil cihaz adli bilişimi sürecine katkı sağladığı görülmüştür. Mobil cihazlarla ilgili veri tabanının da entegre edilmesi ve sistemin intranet üzerinden çalışıyor olması, delil incelemek için internete bağlanmaksızın kullanılan iş istasyonlarının network güvenliği açısından da önemlidir.

Bunun yanı sıra, bu çalışmadan beklenen bazı çıktılar da bulunmaktadır. Karar destek sisteminin doğru yönlendirmesi neticesinde daha az yanlış yöntemler denenecek ve süreç hızlanacaktır. Sistem kullanıldıkça tecrübeli personelin bilgi birikimi de dâhil olmak üzere uygulanan yöntemler veri tabanında tutulacaktır. Bu sayede kurumsal hafıza da sistematik bir şekilde oluşmuş olacaktır. Bunun yanı sıra mobil cihaz adli bilişimi alanında yeni başlayan personel için uygulayacağı yöntemler açısından yol gösteren böyle bir sistemin varlığı, tecrübeli personelin de iş yoğunluğunu olumlu yönde etkilemesi beklenmektedir.

Ayrıca bu sistem sayesinde mobil cihaz adli bilişimi açısından iş standardı oluşacak ve istenirse işlemleri yapan personelin performansı da ölçülebilecektir. Mobil cihaz adli bilişim süreçlerine etki eden faktörler tespit edilerek kurumsal açıdan alınması gereken eğitim ve yapılması gereken yatırım gibi stratejik kararların alınmasında da destek olunması beklenmektedir.

Problem

“Bilginin her yerde olması, potansiyel delilin her yerde olması anlamına gelmektedir” (Collie, 2018). Teknoloji, hayatın her alanındaki yaygınlığını arttırdığı gibi kriminal alanda da oldukça yaygın hale gelmiştir. Bu da suçla mücadele eden kolluk birimlerinin bu alanda kendini geliştirmesi, kapasitesini genişletmesi, yeni yöntemler üretmesi ihtiyacıyla karşı karşıya kalmasına sebep olmuştur.

Günümüzde hemen her suç soruşturmasında dijital materyaller delil için başvuru kaynakları haline gelmiştir. Dijital yönü olan soruşturmalar, adli bilişim personeli açısından

çeşitlilik gösteren formatlarda depolanan büyük miktarlardaki verinin anlamlandırılmasının gerekli olduğu çok yönlü ve karmaşık problemlerdir (Horsman, 2019).

Bu kapsamda, bilgisayarlar, hard diskler, mobil cihazlar, ağ yapıları gibi ortamlar en önemli delil elde edilme potansiyeli olan ortamlardır. Bunun yanında bu ortamların gittikçe artan kapasite büyüklüğü problemi daha dramatik hale getirmektedir. Bir bilişim sistemindeki toplam verinin yaklaşık on binde biri suçun aydınlatılmasında delil olarak kullanılabilir (Değirmenci, 2014: 62).

Özellikle dijital materyaller arasında yer alan mobil cihazların önemi, barındırdığı verilerin kritikliği sebebiyle adli bilişim açısından artmaktadır. Bunun yanında dünya genelinde 5 milyarın üstünde tekil mobil cihaz kullanıcısı var olduğu düşünüldüğünde, mobil cihaz adli bilişimi konusu da aynı şekilde önem arz etmekte ve bu yüzden mobil cihaz adli bilişimi faaliyetlerinin önünde azımsanamayacak bir iş yükü bulunduğu aşikârdır.

Adli bilişim alanındaki standartların eksikliği, farklı uygulamalara yol açmaktadır (Lillis ve diğerleri, 2016). Adli bilişim uygulayıcıları genelde bilgi, deneyim ve yetenek açısından farklılık göstermelerine rağmen, adli bilişim uygulayıcılarının çoğu, karmaşık suç soruşturmalarını çözmekle karşı karşıya kalmaktadır. (Horsman, 2019).

Türkiye’deki adli bilişim uygulamalarındaki eksiklikler arasında standartların olmaması ve uygulayıcıların eğitimsizliği de sayılmaktadır (Başlar, 2020). Ülkemizde uluslararası standartlara önem verilmekte ise de dijital delilin elde edilme şekline ilişkin işlemlerin nasıl olacağı ile ilgili düzenlemelerin eksikliği geri dönülemez hasarlara sebep olabilmektedir (Çiçek, 2008: 14).

Ayrıca bu alandaki profesyoneller için bile nereden başlayacağını bilmek zor olabilmektedir. Özellikle adli bilişim açısından dijital delillerin sağlam bir şekilde nasıl elde edileceğini bilmek daha karmaşık bir konudur (Collie, 2018).

Taşınabilir veya giyilebilir olması gibi sebeplerle mobil cihazlar, teknolojinin gelişiminden en fazla etkilenen ürün gruplarından ve bu durum mobil cihazlar için uygulanan adli bilişim yöntemleri açısından sürekli güncelleme ihtiyacına sebep olmaktadır. Özellikle mobil cihazların donanımları ile donanım üzerinde çalışan işletim sistemleri ve uygulama

çeşitliliğindeki artış, mobil cihaz adli bilişimi için uygulanan yöntemlerin standardizasyonunda problem teşkil etmektedir.

Mobil cihazlarda bulunan kasten veya yanlışlıkla meydana gelmiş fiziksel ya da yazılımsal arızalar, cihazın barındırdığı veriye erişimde önemli bir engel teşkil etmektedir. Hangi marka model cihazlarda, hangi arızalar için hangi müdahalelerin yapılmasına ilişkin kesin kaideler bulunmamaktadır.

Literatürde adli bilişim alanında karar destek modeli önerisi bulunan çalışmalar mevcuttur. Bunlar arasında adli bilişimi genel olarak ele alan, mobil cihazlar üzerine yoğunlaşan ve veri çıkarımı süreçleri üzerine odaklanan çalışmalarla karşılaşılmıştır.

Horsman'ın buna ilişkin DERDS (Digital Evidence Reporting and Decision Support) isimindeki karar destek modeli incelendiğinde (Horsman, 2019), yazılımlar kullanılarak gerçekleştirilen adli bilişimin, değerlendirilmesinin sağlam bir şekilde olmasını hedeflediği görülmüştür. İnceleme sonucunda ortaya konulan çıkarımlar, varsayımlar ve sonuçların nasıl değerlendirilmesi gerektiğine ilişkin önemli bir çalışma sunulmuştur.

Ancak DERDS model önerisinin süreci sağlamlaştırmaya odaklandığı, bu sebeple sürecin hızlandırılmasının göz ardı edildiği görülmüştür. Bulguların elde edilmesi sonrası süreç üzerinde durulmuş; ancak bulguların nasıl elde edildiği ve elde edilme konusundaki en önemli konu olan imaj alma konusu bu çalışmanın kapsamı dışında tutulmuştur.

Grigaliunas ve diğerleri, adli bilişim süreçlerine ilişkin DEO (Digital Evidence Object) isimli bir model önermişlerdir (Grigaliunas, Toldinas, Venckauskas, Morkevicius ve Damasevicius, 2021). Bu modelde kim, ne, ne zaman, nerede ve niçin sorularına cevap aranmaktadır. Her bir soru farklı değişkenlerle açıklanmaya çalışılmaktadır. Bu çalışma sayesinde adli bilişim personeline bazı faydaların sağlanması hedeflenmiştir. Bunlar, incelenecek veri miktarının azaltılması, daha az verinin analizi ve çıkarımı ile daha küçük veri setleri olarak belirtilmiştir.

DEO modelinde bilgisayar adli bilişimi tarafına odaklanılmıştır ve mobil cihazlar göz ardı edilmiştir. Ayrıca bu modelin uygulanabilmesi için verinin elde edilmiş olması ve bunlar

üzerinde analize başlanmış olması gerekmektedir. Verinin elde edilmesi için imaj almanın başlı başına bir problem olduğu mobil cihazlarda bunun nasıl uygulanacağı açık değildir.

Adli bilişime ilişkin bir diğer kural koyma çalışması Effiong tarafından yapılmıştır (Effiong, 2013). Bu çalışmada adli bilişimi genel hatlarıyla ele alan bir model önermiştir. Tüm süreç adım adım ele alınmıştır. Bilgisayar adli bilişimi üzerine yapılan bu çalışmada ön görülen adımların yüzeysel nitelikte olduğu görülmüştür.

Faheem ve diğerleri tarafından mobil cihazlar üzerine yapılan çalışmada ise, mobil cihaz adli bilişimi beş farklı adımda ele alınmıştır (Faheem, Kechadi ve Le-Khac, 2015). Bunlar koruma, elde etme, inceleme, analiz ve raporlama şeklindedir. Bu adımlar genel hatlarıyla süreci tasvir eden nitelikte olup, uygulayıcı açısından somut olarak bir yol gösterdiği anlaşılamamaktadır. Bu çalışma kapsamında veri çıkarımıyla ilgili olarak standardizasyon eksikliği vurgulanmış, mobil cihaz adli bilişiminin kendine has zorluklarından ve mobil bulut verilerinden de bahsedilmiştir. Mobil cihaz adli bilişimiyle ilgili sunduğu model makro nitelikte olup, bu süreçte karşılaşılan mikro düzey problemlerin göz ardı edildiği görülmüştür.

Al Mutawa ve diğerleri tarafından hazırlanan adli bilişim süreçleri için model önerisinde ise davranışsal delil analizi konusu ele alınmıştır (Mutawa, Franqueira, Marrington ve Read, 2018). Bu özgün model önerisinde, laboratuvar ortamındaki inceleme, analiz ve raporlama süreçlerine odaklanılırken, davranışsal analiz niteliğinde gözden geçirme aşaması modelin ilk adımı olarak öngörülmüştür. Bu aşamada viktimoloji ve suça ilişkin davranış üzerinde durulmaktadır.

Adli bilişim konusunda rehber hazırlayan NIST (National Institute of Standard and Technology), bu çalışmada tüm adli bilişim süreçlerini detaylı bir şekilde ele almıştır (Jansen, Ayers ve Brothers, 2014). Mobil cihaz adli bilişimi konusunda da önemli bilgileri barındıran bu çalışmada, mobil cihazlar için de bir model önerisi bulunmaktadır. Bu modelde, cihazın şifreli olup olmadığı ve batarya durumu gibi cihaza ilişkin bazı detayların da yer aldığı görülsede bu detayların sınırlı olduğu değerlendirilmektedir. Ancak çalışmada, bu modelin başlangıç niteliğinde olduğu ve uzmanlardan destek alınması gerektiği belirtilmiştir.

Mobil cihaz inceleme süreçleri üzerinde yaptığı çalışmada Akalın, bu konuda model önerisi geliştirmiştir (Akalın, 2016). Bu öneride dört farklı adımda ele almıştır. Bunlar koruma, elde etme, inceleme-analiz ve raporlama aşamalarından oluşmaktadır. Bu dört ana adımı on dokuz farklı alt adıma ayırmıştır. Alt adımların gerçekleşmesi için kontrol listeleri oluşturmuştur. Bunun yanı sıra mobil cihaz yazılımları ile inceleme süreçleri de gösterilmiştir. Mobil cihaz adli bilişimi açısından oldukça detaylı olan bu çalışmada, bu sürecin en önemli problemlerinden olan imaj alma safhasındaki karşılaşılan problemlere yer verilmediği görülmüştür.

Türkiye’deki mobil cihaz adli bilişimi süreçlerine odaklanan Doğanay, bu alandaki zorluklara ve delil zincirine odaklanmıştır (Doğanay, 2020). Bu çalışmada mobil cihazlardan delil elde etme sürecini anlatan bir iş akışına ve karşılaşılan güncel zorluklara yer verilmiştir. Oldukça fazla detaya yer verilen çalışmada mobil cihazların sorunlarının çözümüne ilişkin bazı detayların yüzeysel bırakıldığı görülmüştür.

Mobil cihaz adli bilişimi ve karar destek sistemine ilişkin çalışmasında Yılmaz ve Çakır, mobil cihazlara ilişkin ilk müdahale ve imaj alma aşamalarına ilişkin detaylı bir çalışma gerçekleştirmişlerdir (Yılmaz ve Çakır, 2021). Karşılaşılan problemlerin nasıl aşılabacağına ilişkin çözüm adımlarını da barındıran genel nitelikli bu çalışmada, mobil cihazların marka model bilgileriyle diğer bilgilerine ilişkin detaylar göz ardı edilmiştir.

Anlaşılabacağı üzere literatürde mobil cihazlarla ilgili olarak cihaz marka modeli de dâhil olmak üzere cihaza ilişkin bilgilerin bu kadar dikkate alındığı başka bir çalışma bulunmamaktadır. Mobil cihaz adli bilişimine ilişkin toplanan veriler ışığında dijital delil elde sürecine en önemli faktörün ne olduğunun tespitini de kapsayan bu çalışmanın, bu yönüyle adli bilişimi alanına önemli katkı sağlayacağı beklenmektedir.

Araştırmanın amacı

Bu çalışmayla özellikle mobil cihaz adli bilişimi alanında önemli katkılar sağlanması beklenmektedir. Genel olarak adli bilişim alanında benzer bir problem, bir adli bilişim personeli tarafından çözülebilirken, diğer personel tarafından çözülememektedir. Ayrıca cihazdan cihaza farklılık arz eden problemler karşısında doğru çözüme ulaşmak için deneme yanılma yöntemlerinin kullanılması sürecinde çokça iş gücü, zaman ve maliyet sarf edilmektedir. Oluşturulacak karar destek sistemiyle mobil cihaz adli bilişimi alanında

alıřan personelin karřılařtıęı olaylarda onu en hızlı řekilde en doęru özme ulařtırması hedeflenmektedir.

Mobil cihaz adli biliřimine iliřkin özmne katkı saęlanması beklenen problemler zet olarak řunlardır:

- Mobil cihaz adli biliřimi alanında artan iř yk hacmi,
- Geliřen teknoloji sebebiyle uygulanacak yntemin deęiřmesi ihtiyaı,
- zellikle mobil cihazlarda ve bunlar zerinde alıřan iřletim sistemleri eřitlilięindeki artıř,
- Cihazlarda bulunan fiziksel ya da yazılımsal arıza durumlarının tespiti ve özm,
- Benzer problemin bir adli biliřim personeli tarafından özlebilirken, dięer personel tarafından özlememesi,
- zellikle yeni bařlayanlar olmak zere personelin bu alandaki karar alma konusundaki destek ihtiyaı,
- Doęru özme ulařmak iin deneme yanılma yntemlerinin kullanılması srecinde harcanan emek, zaman ve maliyet.

Mobil cihaz adli biliřimi alanında katkı saęlanması beklenen problemlerin özmne iliřkin nihai amalara ulařmak iin alt amalar ise řunlardır:

1. Mobil cihaz adli biliřiminde imaj almaya etki eden znitelikler nasıl olmalıdır?
2. Mobil cihaz adli biliřiminde imaj almaya etki eden en nemli znitelikler nelerdir?
3. Mobil cihaz adli biliřimi personelinin, mobil cihaz adli biliřimi kapsamında imaj alma srecine iliřkin karar destek sisteminden beklentisi (mřterinin sesi) nedir?
4. Mobil cihaz adli biliřimi personelinin, mobil cihaz adli biliřimi kapsamında imaj alma srecine iliřkin karar destek sisteminden beklentisini karřılayacak teknik gereksinimler nelerdir?
5. Oluřturulan mobil cihaz adli biliřimi kapsamında imaj alma srecine iliřkin web tabanlı karar destek sistemi yazılımının kullanımı kolay ve anlařılır mıdır?
6. Oluřturulan mobil cihaz adli biliřimi kapsamında imaj alma srecine iliřkin web tabanlı karar destek sistemi yazılımı, mobil cihaz adli biliřimi srelerine katkı saęlamıř mıdır?

Sınırlılıklar

alıřmanın evreni, EGM Siber Sularla Mcadele Daire Bařkanlıęı (SSMDB) Adli Biliřim řube Mdrlęne bir yıl iinde gelen akıllı telefon nitelięindeki mobil cihazlardan oluřmaktadır. Bu birim, 81 il emniyet mdrlę atısı altında faaliyet gsteren Siber

Sularla Mcadele Ŗube Mdrlė tarafından imajı alınamadıėı iin bu birime gnderilen mobil cihazların zm iin uėrařmaktadır. Bu sebeple alıřmanın veri seti, il birimindeki yetersizlikler veya mobil cihazlarda bulunan arızalar sebebiyle SSMDDB’ye gnderilmiř olan cihazlar ve bu cihazlara yapılan iřlemlerden oluřmaktadır.

Mobil cihaz adli biliřimi sreci, temelde ilk mdahale, imaj alma ve inceleme olmak zere  ařamada ele alınmaktadır. Ancak oluřturulan karar destek sistemi sadece imaj alma srelerine odaklanmıřtır. Diėer sreler alıřmanın kapsamı dıřında tutulmuřtur.

Uzman grřmeleri sonucunda znitelikler belirlenirken alıřmanın rnekleme iin en nemlileri tespit edilmiřtir. Ancak teknolojinin geliřim hızı ve ngrlmesi zor ihtimalleri dikkate alındıėında, belirlenen arızalar veya zm yolları dıřında da durumlarla karřılařılması muhtemeldir. Ancak bu durumlar da alıřma kapsamı dıřında tutulmuřtur. Karar destek sistemi yazılımına eklenen aıklama alanı sayesinde yeni karřılařılan durumların, uygulama ařaması sonrasındaki geliřtirme ařamasında sisteme dhil edilmesi planlanmaktadır.

Yazılımın bařarısının llmesi ařamasında geri bildirim alınan uygulayıcı personel, bir btn olarak ele alınmıřtır. Tm kullanıcılar alanda tecrbesi olan, bu alandaki farkındalıėı yksek kiřilerden oluřmakta iken; bu kullanıcıların bireysel nitelikleri ve farklılıkları gz ardı edilmiřtir.



2. ADLİ BİLİŞİM

2.1. Adli Bilişim Nedir?

Adli bilişim bir alt disiplin olarak adli bilimler altında kalmaktadır ve günümüzde teknolojinin hayatın vazgeçilmez alanında iyiden iyiye yer edinmesiyle her geçen gün önemi artan bir disiplin haline gelmiştir. Adli bilişimi temelde dört ana başlık altında toplamak mümkündür. Bunlar; bilgisayar adli bilişimi, mobil cihaz adli bilişimi, ağ adli bilişimi ve bulut adli bilişimidir (Lin, Chao ve Peng, 2011). Bu kısımda adli bilişimin tanımı ve adli bilişim kavramıyla ilgili literatürdeki yer alan çalışmalara yer verilmiştir. Literatürdeki çalışmalar harmanlanarak, adli bilişimin tam olarak ne anlama geldiği aktarılmaya çalışılacaktır.

“Adli Bilişim, bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür.” (Henkoğlu, 2014:1).

Grigaliunas ve diğerlerine göre (2021) adli bilişim, dijital cihazlar, ağ bağlantıları ve buluttaki büyük veri gibi çeşitli platformlardaki verilerin toplanması, incelenmesi ve analizi süreçleridir (Grigaliunas ve diğerleri, 2021).

“Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür” (Ekizer, 2014).

Ramadhani ve diğerleri ise adli bilişimi; bilgisayarlar, cep telefonları, tabletler, PDA’lar, ağ cihazları, depolama ortamları gibi dijital cihazlardaki veriyi bulmayı ve incelemeyi hedefleyen adli bilimlerin parçası olarak tanımlamıştır (Ramadhani ve diğerleri, 2020).

“Adli Bilişim en basit tanımıyla, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz tekniklerinin kullanılmasıdır. Bilgisayardaki verilerin korunması, tanınması, çıkarılması, dökümü ve yorumunu içerir

ancak bunun yanında hukuki kurallar, süreçler, delillerin bütünlüğü gibi konulara da riayet ederek bulunan veriler hakkında rapor yazılmasını da kapsar” şeklinde tanımlamıştır. (Aydoğan, 2009:7).

“Adli Bilişim, bilişim sistemlerine iletilen, işlenen ve/veya depolanan dijital verinin adli talimat üzerine elde edilerek bulgu olarak tespit edilmesinden, raporlanarak delil olarak değerlendirilmesi amacıyla mahkemeye sunulmasına kadar geçen süreçte delil zinciri her aşamada uygulanarak gerçekleştirilen multidisipliner (çoklu disiplinli) ve interdisipliner (disiplinler arası) halde işletilen teknik ve hukuki adımlar ile işlemler bütünüdür” (Doğanay, 2019 s:4).

Adli bilişimin amacı, zaman açısından kısıtlı olan karar vermeyi kolaylaştırmak için, dijital delillerin tanımlanması ve korunması, bilgilerin çıkarımı ve çıkarılan bilgilerin analizi açısından durumun farkındalığını sağlamaktır (Grigaliunas ve diğerleri, 2021).

Adli bilişimi, hukuki uyumsuzluk konusu delilin elde edilmesi amacıyla sayısal veriler üzerinde teknik ve hukuki prensipler çerçevesinde gerçekleştirilen; ilk müdahale, imaj alma, veri kurtarma, inceleme, analiz, çıkarım ile bu işlemleri raporlama süreçlerinin her biri veya bütünü olarak tanımlayabiliriz.

2.2. Dijital Delil ve Delil Zinciri

Anayasa Madde 38’de “Kanuna aykırı olarak bulunmuş bulgular, delil olarak kabul edilemez.” ifadesi geçmektedir. Bu madde delillerin niteliği açısından hukukumuzda çok önemli bir ilke olarak yer almaktadır. Bu maddede iki önemli unsur vurgulanmaktadır. İlki delil ve bulgunun farkıdır. Delil ve bulgu terimleri her ne kadar birbirine benzeyen kelimeler olsa da konunun derinlemesine inildiğinde birbirine oldukça yakın anlamları olan ancak küçük de olsa farklı anlamları taşıyan kelimeler olduğu anlaşılmaktadır. İkincisi ise deliller açısından hukuka uygunluğun ne kadar önem arz ettiğidir. Özellikle yapısı gereği oldukça hassas olan dijital materyallerden elde edilen bulguların hukuka uygunluğunun yanı sıra güvenilirliği ve bütünlüğü hususları, bulgunun delil niteliğini kaybetmemesi açısından ayrıca özen gösterilmesi gereken konulardır.

Delil kavramı ile bulgu kavramını birbirinden ayıran en temel özellik, bulgunun anlam kazanarak delil haline gelmesidir. Olay yerinden elde edilen, işlenmemiş maddi unsurlar

bulguyken, bu bulgu işlenip olayla ilgisi ve bağlantısı sağlanınca delil niteliği kazanır. Yani bulgu henüz kesinlik kazanmamış maddi olgulara verilen isimken, delil ise bulgunun olayla bağdaştırılarak biraz daha kesinlik kazanmış hali olarak düşünülebilir.

Delilin ne anlama geldiğini biraz daha kapsamlı bir şekilde aktaracak olursak; “Arapça kökenli olan kelime Türk Dil Kurumunun Türkçe Sözlüğünde, insanı aradığı gerçeğe ulaştırabilecek iz, emare, kanıt olarak tanımlandığı görülür. Diğer bir ifadeyle delil, öncesinde mahkeme dışında ortaya çıkan olayların yargı sürecine dâhil edilmesini sağlayan, ispat faaliyetlerinde kullanılan ve olayı temsile uygun olan araçlardır.” (Mulaj, 2019) şeklinde tanımlanmıştır.

2.2.1. Dijital Delil

Günümüzde bir problem olarak dijital delillerin yığınlarından bahsedilmektedir (Lillis ve diğerleri, 2016). Bu bölümde delil kavramından yola çıkarak literatürde elektronik delil olarak da geçen dijital delil kavramının ne anlama geldiği birkaç farklı dijital delil tanımıyla aktarılmaya çalışılacaktır.

Aknar, dijital delili, “Bilişim sistemlerinin veya veri kaydetme özelliğine sahip elektronik cihazların içerisinde yer alan ve suçun aydınlatılmasında önemli rol oynayacak verilere verilen genel isim.” (Aknar, 2019) olarak ifade etmiştir.

Bir başka kaynakta ise dijital delil kavramı; “Bir suç için delil özelliğine sahip ve mahkemelerde delil olarak kullanılabilecek her türlü manyetik ve elektronik ortamda veri saklayabilen bilgisayar, sabitdisk, flashdisk, CD/DVD, bellek kartı, akıllı telefon, yazıcı, tarayıcı, kredi kartı okuyucuları, bilgisayarda tutulan LOG dosyaları, dijital fotoğraf ve videolar, ses kayıt cihazları, chat kayıtları, e-posta hesapları, abonelikler, SIM kartı vb. farklı birçok dijital alet ve ortam dijital delil sayılmaktadır.” (Altındağ, 2018) şeklinde tanımlanmıştır.

“Dijital deliller, adli bilişimle ilgili bir çalışma esnasında bilişim sistemleri (bilgisayarlar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital fax makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delillerdir.” (Henkoğlu, 2014:5).

Dijital Delillerin Bulunduğu Ortamlar:

- Harddisk, SSD, Nand Bellek,
- Uçucu verileri barındıran RAM,
- Floppy Disk ve CD/DVD/BluRay
- Hafıza Kartı,
- Cep telefonu, tablet, el bilgisayarı (PDA),
- Dijital kamera ve fotoğraf makinası,
- Hafıza birimi olan müzik çalar,
- DVR ve NVR cihazları,
- Modem, ağ yapıları, sunucular,
- Taşınabilir bellek,
- Yazıcı, fax, fotokopi makinaları,
- IOT cihazları
- Giyilebilir teknolojiler,
- Bulut bilişim,
- Araba, dron, uçaklar vs. veri depolayan işleyen her şey adli bilişim konusu olabilir.

Dijital delilleri barındırdığı elektronik verilerin niteliğinden dolayı diğer delil türlerinden ayıran bazı özellikleri vardır. Bunlar:

- Elektronik verilerin kopyalanması ve çoğaltılması kolaydır.
- Elektronik veriler nem, sıcaklık ve manyetik alandan dolayı bozulabilirler.
- Elektronik veriler, çeşitli müdahaleler yapmak suretiyle değiştirilebilirler.
- Elektronik verilerin geri kurtarılamayacak şekilde silinmesi mümkündür.
- Elektronik veriler üzerinde başkaca gizlenmiş, şifrelenmiş bulunabilir. (Kılıç, 2014:146).

Dijital delillerin toplanması ve elde edilmesi sürecinde dijital verilerin kolay değiştirilmesi ve zarar görmesi ihtimalinden dolayı dikkatli hareket edilmesi gerekmektedir. Bu sebeple dijital delillerin toplanmasında uzman ve yeterli düzeyde eğitimi olan personel görevlendirilmelidir. Dijital delillerin toplanması, incelenmesi ve değerlendirilmesi sürecinde alanında uzman olan personel gerekli prensip ve prosedürlere uymalıdır.

2.2.2. Delil Zinciri

Bulgunun delil olarak kabul edilebilmesi için ispatlanmış olması gerekir. Delilin nerede tespit edildiği, nasıl toplandığı, nasıl muhafaza edildiği, kim tarafından hangi zamanlarda hangi işlemlerin yapıldığı hususlarının belgelenebilmesi ve ispatlanabilmesi gerekmektedir. Yani delillere ulaşmada objektif ve güvenilir verilerin kullanılmasının yanı sıra, işlemin başından sonuna kadar dijital delillerin değiştirilmeden ve tutarlı bir şekilde adli makamlara sunulması delil zincirini ifade etmektedir.

Mahkemelerde dijital delillerin geçerliliği açısından, el koyma işleminden itibaren herhangi bir değişiklik olmadığının, nereden, ne zaman ve kimden alındığının doğrulanabilir olması çok önemlidir (Solmaz, 2008).

Adli yargılamanın en önemli dayanaklarından birinin usulüne uygun elde edilmiş delil olmasından dolayı delillerin değiştirilmesi, bozulması veya kaybolmasına karşı uzman personel görevlendirilmelidir. Delil zinciri olarak adlandırılan uygulama ile delilin her el değiştirmesi işlemi delil takip formuna işlenmektedir. Bunun yanında delilin muhafaza edildiği ambalajın üstüne delilin hassasiyeti ile ilgili etiket yapıştırılması gerekmektedir (Bıçak, 2013:534). Bu sayede delil ile temas kuran tüm kişiler kayıt altına alınmış olur.

Dijital delile ulaşıldığında delil zincirini sağlamak için ilk müdahale ekipleri tarafından başvuru bazı prosedürler vardır. Bu prosedürler delilin değiştirilmesini önlemekte ve delil bütünlüğünü temin etmektedir. Dijital delilin bütünlüğünü koruyabilmek adına yapılacak en önemli şey, delil üzerinde çalışmak yerine delilin imajının oluşturulması ve çalışmaların bu kopya üzerinden gerçekleştirilmesidir.

İmaj (adli kopya) alma işlemi, dijital delil niteliğindeki bir bilgi saklama ünitesinin veya dosya içeriğinin veri bütünlüğünün korunması ve sürdürülmesi prensipleri içinde bire bir kopyalanması işlemidir.

Delil zinciri bütünlüğünün korunması adına, adli bilişimde kullanılan bir diğer önemli kavram ise hash (veri özeti) değeridir. Hash değeri, belli bir veri üzerinde değişiklik olup olmadığının tespiti için kullanılan bir yöntemdir. Kısacası herhangi bir dijital verinin orijinali ile farklı yönleri var mı sorusunun cevabı için hash değerine bakılmalıdır. Hash değeri işlem öncesinde ve sonrasında aynı ise verilerde herhangi bir değişiklik yapılmadığı anlamına gelir. Eğer hash değeri işlem öncesinde ve işlem sonrasında farklılık gösterir ise, el konulan dijital materyallerde değişiklik yapıldığı anlamına gelir. Bu da delil zinciri güvenliğini olumsuz etkiler.

Dijital delildeki verilerin güvenilirlik ve bütünlük açısından değiştirilmediğinin ve bu verilerin güvenilirliğinin tespiti için kullanılan en yaygın ve en önemli yöntem ise hash algoritmalarının kullanılmasıdır. Hash değeri, bir verinin tek yönlü olarak matematiksel

işleme sokulması sonucu elde edilen özet veridir. MD5, SHA1 ve SHA256 en sık kullanılan hash algoritmalarıdır (Doğanay, 2020:93).

Delil zinciri, hassas ve kolay manipüle edilebilir yapısından dolayı dijital deliller açısından çok daha önemlidir. Bu sebeple olay yerinde gerçekleştirilen ilk müdahale işleminden itibaren dijital delillerin güvenliği alınmalı ve gerçekleştirilen her temas kayıt altında olmalıdır. Özellikle büyük bir yapı altında yürütülen adli bilişim faaliyetlerinde, bir dijital materyalin, ihtiyaç duyduğu uzmanlıklara göre farklı farklı birimler arasında transferi söz konusu olabilir. Ancak olası bir bozulma ya da manipülasyon iddiası karşısında, temas eden herkesin hangi uzmanlık ile ilgili hangi müdahalelerde bulunduğu belgesi olmalıdır. Bunun en iyi yöntemlerinden birisi de delil zincirine ilişkin tutanağın yanında, işlemi gerçekleştiren her birimin kendi işlemleri için ayrıca rapor tutmasıdır.

Kolluk görevlileri tarafından dijital delillerin elde edileceği ortamlarda yapılacak bazı iş ve işlemler bulunmaktadır. Delil zincirinin korunmasıyla ilgili adımlara aşağıda sırasıyla yer verilmiştir:

- Herhangi bir işleme başlamadan önce farklı ve geniş açılardan çok sayıda fotoğraf çekilmelidir.
- Arama yapıldığı sırada arama yapılan bölge video kaydına alınmalı ve elde edilebilecek olan delillerin olay yerinden alındığı açıkça görünecek şekilde kayıt altına alınmalıdır.
- Tespit edilen delilin fiziki durumu ve seri numarası gibi ayırt edici niteliklerini de içeren fotoğrafları çekilmelidir.
- El konulan dijital materyaller arama tutanaklarına yazılırken cihazların fiziki durumları; varsa kırık, çizik, arıza veya cihazlardaki eksikler de yazılmalıdır.
- İşlemler yapılırken laboratuvar eldiveni kullanılmalıdır.
- El konulduktan sonra cihaz açılmamalı, yapılan tüm müdahaleler ile cihazın aidiyet bilgileri ve diğer ayırt edici bilgileri tutanak altına alınmalıdır.
- Alınan imajların bulunduğu diskler ve el konulan tüm materyaller etiketlenmelidir. Etiketlerde yeterli açıklayıcı bilgiler olmalıdır. Etiketlerin cihazların veri aktarım yollarına, cihazların seri numarası ve kapasitesi gibi belirleyici açıklamaların olduğu kısımlara yapıştırılmamasına özen gösterilmelidir.

- Telefon açıksa telefonu uçak moduna alma ya da faraday çantası kullanma gibi yöntemlerle dış sinyallerden izole edilmelidir.
- İşlemler bitiminde mümkünse tekil numaralı delil poşetleri ya da mühür bantları kullanılarak mühürlenmelidir.
- Mühür açma işlemleri mümkünse kayıt altına alınmalı, tutanak ile mühür açma işlemi belgelendirilmelidir.
- Mühür açıldıktan sonra delilin zarar görmesini engellemek için gerekli önlemlerin alındığı ve sadece yetkili personelin girebildiği delil odalarında muhafaza edilmelidir.
- Delilin, tüm işlemleri ve transferleri tutanak ile imza karşılığı gerçekleştirilmelidir.

2.3.Türkiye’de Adli Bilişim

2.3.1. Ceza Muhakemesi Kanunu

Ülkemizde adli bilişim faaliyetlerinin yürütülmesinde en temel ve geçerli mevzuat Ceza Muhakemesi Kanunu 134. maddesidir. Bu madde Kanunun yürürlüğe girdiği 2005 yılından beri uygulanmaktadır. Geçen süre boyunca bazı değişiklikler geçirmiş ve nihayetinde bu halini almıştır.

“Bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma Madde 134 – (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklenmesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.”

Değişikliklerden ilki 6526 sayılı Kanun ile 2014 yılında gerçekleştirilmiştir. İlk fıkraya “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve” ifadesi eklenmiştir. Tedbirin başvurulması için gereken şart başka surette delil elde etme imkânının bulunmasıyken somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı da eklenerek gerçekleşmesi gereken kanaat daha da zorlaşmıştır.

Yine aynı Kanunla gerçekleştirilen diğer değişiklik ise maddenin dördüncü fıkrasında yer alan “İstemesi halinde, bu” ifadesi “Üçüncü fıkraya göre alınan” şeklinde değiştirilmiştir. Bu cümle ile de elkoyma işlemi sırasında yapılan yedekleme işlemi sonucu yedeğin bir kopyasının şüpheli veya vekiline verilmesi gerekmektedir. Bu değişiklik yürürlüğe girdiğinden beri bu madde kendi içinde birçok zorluğu da beraberinde getirmiştir.

2018 yılında 7145 sayılı Kanun ile ilk fıkrada yer alan “Cumhuriyet savcısının istemi üzerine” ifadesi “hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından” olacak şekilde değiştirilmiştir. Bu değişiklik ile diğer tedbirlerde öngörülmüş olan gecikmesinde sakınca bulunma durumu dijital deliller için arama, kopyalama ve elkoyma tedbirinde de uygulanma niteliği kazanmıştır.

Ayrıca yine 7145 sayılı Kanun ile ikinci fıkrasına “ya da işlemin uzun sürecektir olması” ifadesi eklenmiştir. Elkoyma şartlarının düzenlendiği bu fıkraya uygulamada, diğer elkoyma tedbirlerine göre daha çok karşılaşılan durum olan arama, yedekleme, kopya alma işlemlerinin uzun sürmesi halinde de elkoyma tedbirini düzenlemiştir.

Birinci fıkra değerlendirmesi

Ceza Muhakemesi Kanunu 134. maddesinin soruşturma ve kovuşturmayı kapsamak yerine sadece soruşturmaya sınırlı olması, uygulamayla madde hükmünün farklılaşması gibi istenmeyen bir sonuç doğurmaktadır. Ancak hem soruşturma hem kovuşturma aşamasında başvurulmuş bir tedbir olduğu bilinmektedir.

Oldukça sık başvurulmuş bu tedbirin “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması” şeklinde ağır bir şarta bağlanmasından ziyade; bu tedbire ikincillik niteliği kazandıran “başka surette delil elde etme imkânının bulunmaması” ifadesinin kaldırılmasının uygun olduğu değerlendirilmektedir.

Öte yandan arama konusu bilgisayar, bilgisayar programları ve bilgisayar kütükleri olarak kanun maddesinde sayılmıştır. Ancak delil elde edilmesi beklenen ortam cismen varlığı olan medyalardan ziyade sayısal verilerdir. Günümüzde verilerin bulunabileceği ortamları sayma yöntemiyle belirlemenin oldukça zor olması sebebiyle daha genel bir ifade olarak “sayısal veri” ifadesinin kullanılması daha uygun olacaktır.

İkinci fıkranın değerlendirilmesi

İkinci fıkra genel olarak elkoyma şartları düzenlenmiştir. Bu şartlar, “şifrenin çözülememesinden dolayı girilememesi, gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecektir olması” şeklinde sayılmıştır. Her ne kadar bu kanun maddesi uygulanırken elkoymaya sıklıkla başvurulsa da, elkoyma için gerekli olan şartların uygulamaya ve uygulamada karşılaşılan durumlara göre yeniden düzenlenmesi gerektiği değerlendirilmektedir. Hâlihazırda uygulamada olay yerinde inceleme işleminin gerçekleştirilmesi nadiren olmakta, bu yüzden şifre çözümü veya gizlenmiş verilerin tespiti durumlarıyla karşılaşmamaktadır.

Ancak olay yerinde adli kopya alma durumları sayılanlar dışında birçok sebepten yerine getirilememektedir. Bunlara örnek olarak: aramanın gerçekleştirildiği fiziksel ortamda güç kaynağı bulunmaması, delil olan cihazın güç ve veri bağlantı kablolarının bulunmaması, cihazın arızalı, kırık veya farklı bir sebeple cihazla iletişim kurulamıyor olması, cihazdan veri elde edilmesi için gerekli uygun teknolojinin olay yerine getirilememesi, işlemi gerçekleştirebilecek uzman personelin bulunmaması ve olay yerinde gerçekleştirilen canlı inceleme işleminde tespit edilen verilerin yetersiz olduğu ve silinmiş alandan gelmesinin muhtemel olduğu durumlar sayılabilir.

Sayılan sebeplerden dolayı madde metnindeki elkoyma şartlarının yerine veya ilave olarak tüm verilere ulaşılamaması veya adli kopya alma işleminin gerçekleştirilememesi durumlarının eklenmesinin uygulamayla daha çok örtüşeceği değerlendirilmektedir.

Üçüncü fıkranın değerlendirilmesi

Bu fıkra elkoyma işlemi esnasında verilerin yedeklemesinin yapılacağından söz edilmiştir. Ancak maddenin diğer fıkralarında kopya alma ifadesi geçerken, bu fıkradaki yedekleme ifadesi ile kanun koyucunun amacı anlaşılamamıştır. Bu fıkra elkoyma sırasında yedekleme işleminin olması gerektiği bahsedilirken, uygulamada olay yerinde

kopyası alınamadığı hallerde elkoyma işlemi gerçekleştirilmekte ve ikinci fıkraya göre kopya alma işlemi sonrası iade edilmektedir. Bu yüzden üçüncü fıkranın uygulamada bir karşılığı olmadığı kanısına varılmıştır.

Dördüncü fıkranın değerlendirilmesi

Dördüncü fıkranın silahların eşitliği ve çelişmeli yargı ilkelerinin uygulanması için düzenlendiği değerlendirilmektedir. Bu fıkra şüpheli veya vekiline kopya verilmesi durumu düzenlenmiştir. Maddenin ilk halinde istemesi halinde kopya verilmesi durumu söz konusuysa, 2014 yılında yapılan değişiklikle herhangi talepten bağımsız olarak zorunlu hale getirilmiştir. Bu zorunluluk ise üçüncü fıkraya atıf yapılarak, “üçüncü fıkraya göre alınan yedekten” yani elkoyma sırasında yapılan yedeklemenin kopyasının teslim edilmesini kapsamaktadır.

Bu şekilde uygulanmasını zorlaştıran bazı durumlarla karşı karşıya kalınmaktadır. İlk olarak kopyanın verilmesinin zorunlu hale gelmesiyle, kopyanın oluşturulacağı diskin maliyetinin nasıl karşılanacağı sorun haline gelmiştir. Şüpheliden mi, kolluk bütçesinden mi yoksa savcılık bütçesinden mi karşılanması gerektiği sorusu, Adalet Bakanlığı tarafından yazılan görüşle Başsavcılık bütçesinden karşılanması gerektiği şeklinde cevaplanmıştır.

Diğer bir sorun ise suça konu verinin bulunmasıdır. Kopyası alınan verinin bizatihi suç olması ya da sahip olunması durumunda suç işlemeye devam edilmesinin muhtemel olması hallerinde dahi verinin bir kopyasının verilmesini engelleyici bir hüküm olmaması konusudur.

Suçta konu verinin bulunması durumuyla ilgili olarak Avrupa Siber Suçlar Sözleşmesi’nde verinin erişilmez kılınması veya kaldırılması düzenlenmiştir. Erişilmez kılma veya kaldırma işleminin zararlı yazılım programları, bombanın nasıl yapılacağını anlatan bilgiler gibi tehlike içeren veya çocuk müstehcenliği gibi verinin veya içeriğinin bizatihi suç olduğu durumlarda uygulanması önerilmiştir.

Bu fıkranın varlığı, şüpheli veya vekiline kopya verilmesi silahların eşitliği veya çelişmeli yargı kapsamında olumlu bir adımdır. Ancak bunun nasıl işletilmesi gerektiği konusunda bazı düzenlemelerin yapılması gerekmektedir. Uygulamada ise verilerin silinmesine ilişkin gelen talimatlar Adalet Bakanlığının görüşü doğrultusunda yerine getirilmektedir.

Beşinci fıkranın değerlendirilmesi

Bu fıkra elkoyma işlemi olmadan da kopya alma işleminin gerçekleştirilebileceği anlatılmıştır. Bu fıkra ile olay yerinde imaj alma işlemlerinin temeli oluşmaktadır. Ancak bu fıkra kopyası alınan verilerin kâğıda yazdırılması hükmü geçmektedir. Günümüz veri depolama teknolojileri dikkate alındığında bir kütüphane dolusu kitap verisinin, cebe sığacak bir dişte depolanabileceği düşünüldüğünde, bunun uygulanmasının teknik açıdan neredeyse imkânsız olacağı aşikârdır.

2.3.2. Adli ve Önleme Arama Yönetmeliği

Bu Yönetmelik, kanunlar ile düzenlenmiş olan adli ve önleme aramasına ilişkin karar verme yetkisi ile bu aramaların uygulanmasında uyulacak esas ve usulleri göstermesi amacıyla 2005 yılında yürürlüğe girmiştir.

Yönetmeliğin 17. maddesinde dijital delillere ilişkin düzenleme yapılmıştır. Madde metnine bakıldığında Ceza Muhakemesi Kanunu'nun 134. maddesi ile oldukça benzer olduğu görülmektedir.

“Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma Madde 17 - Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.

Üçüncü fıkraya göre alınan yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir.”

Madde metni incelendiğinde Ceza Muhakemesi Kanunu Madde 134'te 2018 yılında 7145 sayılı Kanun ile düzenlenen gecikmesinde sakınca bulunan hallere ilişkin Cumhuriyet

savcısına verilen yetki ile elkoyma şartı olarak eklenen işlemin uzun sürecek olması durumunun henüz işlenmediği anlaşılmaktadır.

Ayrıca üçüncü fıkrasında elkoyma sırasında yapılan yedeklemenin, bilgisayar ağları, diğer uzak bilgisayar kütükleri ve çıkarılabilir donanımları sayılarak, bunlar için de uygulanacağı belirtilmiştir. Bilgisayar ağlarının ve uzak bilgisayarların sayılması, geldiğimiz noktada önem arz eden bulut bilişimi kast ettiği şeklinde yorumlanabilir. Zaten benzer hüküm Avrupa Siber Suçlar Sözleşmesi'nde de geçmektedir.

Ancak bu uzak sistemler ve ağlar üzerinden erişilen sistemlerden delil elde edilmesi süreci, Avrupa Siber Suçlar Sözleşmesi'nde bazı sınırlar içinde öngörülmüştür. Bu sınırlar kendi ülkende olması, farklı ülkede ise talep edilmesi gerektiği şeklindedir. Farklı ülkede bulunması durumunda talep edilmesinin istisnası ise, halka açık durumda bulunan veri ile erişilen veri için kişinin rıza göstermesi durumudur. Bu sebeple Yönetmelik'te belirtilen bu tip bir aramanın, bulut bilişim hizmeti sağlayıcılarının hemen hepsinin yurtdışında olmasından dolayı çok uygulanabildiği söylenememektedir.

2.3.3. Avrupa Siber Suçlar Sözleşmesi

Avrupa Siber Suçlar Sözleşmesi'nin dayanağı, 1996 yılında Suç Sorunlarına İlişkin Avrupa Komitesi (European Committee on Crime Problems) tarafından Avrupa Konseyine bilişim suçlarına ilişkin bir adım atılmasına ilişkin önerisidir. (İçel, 2011). Bunun üzerine Siber Uzak Suçlarına İlişkin Uzman Komitesi (Committee of Experts on Crime in Cyber-Space) kurulmuştur. Komite tarafından yapılan çalışmalar sonucunda hazırlanan metin 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmiş ve ardından devletlerin imzasına açılmıştır (Vatis, 2010: 208).

Türkiye Cumhuriyeti ise 10 Kasım 2010 tarihinde imzaladığı Sözleşmeyi 01 Ocak 2015 tarihinde yürürlüğe konulması üzere onaylamıştır. (COE, 2021) Uygun bulunmasına ilişkin kanun tasarısındaki gerekçede, Sözleşme "... siber ortamda özgürlüklerin, insan haklarının ve güvenliğin korunması ile risklerin azaltılmasına ilişkin kabul edilmiş tek uluslararası rehber olan belge, hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç ..." olarak nitelendirilmiştir. Bununla birlikte Sözleşmenin iç hukuk gereklerinin yerine getirilmesi üzerine imzalandığı da aynı metinde yer almaktadır. (TBMM, 2012).

Türkiye’deki adli bilişim uygulamaları açısından, dijital deliller ile ilgili olarak iç mevzuat doğrultusunda ne derece uygulanabilir olduğu oldukça tartışmalıdır. Klasik suçlar bakımından oldukça eksik ve sorunlu bulunan yasanın Ceza Muhakemesi Kanununun 134. maddesinin, Sözleşme’de düzenlenen usul hükümlerini tam anlamıyla karşılayamadığına ilişkin görüşler bulunmaktadır (Aliusta ve Benzer, 2018).

Avrupa Siber Suçlar Sözleşmesi’nde yer alan dijital deliller ve adli bilişim ile ilgili düzenleme “Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması” başlıklı 19. Maddesidir.

“Başlık 4 - Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması

Madde 19 - Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması

1. Taraflardan her biri, kendi ülkesindeki yetkili makamların,
 - a. bir bilgisayar sisteminin tamamını veya bir kısmını ve içerisinde depolanmış bilgisayar verilerini; ve
 - b. bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtını arama ve benzer şekilde bunlara erişme yetkisine sahip olmaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2. Taraflardan her biri, paragraf 1.a uyarınca, makamlarının özel bir bilgisayar sisteminin tamamını veya bir kısmını araması veya benzer şekilde bunlara erişim sağlaması söz konusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğuna inanmak için gerekçeleri bulunduğu ve söz konusu veriler yasalara uygun biçimde ilk sistemden erişilebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
3. Taraflardan her biri, yetkili makamlarına, paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koymaya veya benzer şekilde güvence altına almaya yetki tanımak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Bu tedbirler:
 - a. bir bilgisayar sisteminin tamamına veya bir kısmına veya bilgisayar verileri depolama aygıtına el koymaya veya bunları benzer şekilde güvence altına almaya;
 - b. sözkonusu bilgisayar verilerinin bir kopyasını oluşturmaya ve bunu muhafaza etmeye;
 - c. ilgili depolanan verilerin bütünlüğünü korumaya;
 - d. erişim sağlanan bilgisayar sistemindeki bilgisayar verilerini erişilemez hale getirmeye veya kaldırmaya yönelik yetkileri içerecektir.
4. Taraflardan her biri, paragraf 1 ve 2’de belirtilen tedbirlerin tatbik edilmesine olanak sağlanması amacıyla, kendi yetkili makamlarına bilgisayar sisteminin işleyişi veya içerisindeki bilgisayar verisinin korunması için uygulanan tedbirler hakkında bilgisi olan herhangi bir kişiden, makul ölçüde gerekli bilgileri temin etme konusunda yetki tanınması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
5. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15’e tabi olacaktır.”

Mevzuatımızdaki benzer nitelikli Ceza Muhakemesi Kanunu Madde 134’e göre daha kapsamlı ve daha uygulanabilir olduğu anlaşılan 19. madde hükümlerinde neyin

amaçlandığını ortaya koymak ve tartışmak için sözleşmenin açıklayıcı raporunda yer almaktadır (COE, 2001). Açıklayıcı rapor ışığında değerlendirildiğinde Türkiye'deki uygulanmasıyla ilgili literatürde birçok tartışma mevcut olan Ceza Muhakemesi Kanunu'nun 134. Maddesi, Avrupa Siber Suçlar Sözleşmesi ile kıyaslandığında bazı farklılıklar görülmektedir. Sözleşme'de yer alan bilgisayar sistemi kavramı, gereken aramanın derecesi, e-posta veya anlık mesajlaşma uygulamaları gibi iletişim niteliğindeki potansiyel dijital delil kaynaklarının nasıl ele alınması gerektiği, verinin erişilmez hale getirilmesi ve bilgi işlem personelinin desteğinin alınmasına ilişkin hususların Ceza Muhakemesi Kanunu'nda açıklanmadığı görülmektedir.

Ülkenin yetki sınırları dışında yer alan bilgisayar verilerinde arama yapılması için Sözleşmenin Madde 31 ve Madde 32 hükümlerine bakılması gerekir.

“Madde 31 - Depolanan bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma Taraflardan biri, bir diğer Taraftan Madde 29 uyarınca korunan veriler de dâhil olmak üzere, sözkonusu Tarafın ülkesindeki bir bilgisayar sistemi aracılığıyla depolanan veride arama yapmayı veya benzer şekilde buna erişim sağlamayı, el koymayı veya benzer şekilde güvence altına alınmasını veya açıklanmasını talep edebilir...”

“Madde 32 - Depolanmış bilgisayar verilerine izni şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması

Bir Taraf, diğer Tarafın izni olmaksızın:

- a. halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine, bunların coğrafi konumuna bakmaksızın erişebilir; veya
- b. kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer Tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu Taraf, sözkonusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, sözkonusu verilere erişebilir veya bunları temin edebilir.”

2.3.4. Türkiye’de adli bilişim faaliyetleri

Türkiye’de adli bilişim faaliyetleri öncelikle kolluk kurumları ve kanuni olarak bilirkişilik görevi verilmiş olan kurumlar tarafından gerçekleştirilmektedir. Kolluk birimleri olarak adli bilişim faaliyetleri İçişleri Bakanlığı altındaki Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı tarafından yapılmaktadır. Kanuni bilirkişilik göreviyle görevlendirilmiş kurum ise Adalet Bakanlığı çatısı altında olan Adli Tıp Kurumudur. Bunların yanı sıra adli bilişim faaliyetleri bireysel olarak bilirkişiler ve uzmanlar tarafından yerine getirilmektedir.

Emniyet Genel Müdürlüğü çatısı altında adli bilişim faaliyetleri 1998 yılında Kriminal Polis Laboratuvarları bünyesinde yerine getirilmeye başlanmıştır (EGM, 2019). Daha sonrasında

ise gelişen teknolojiyle birlikte suçla mücadele yöntemlerinin de gelişmesi ihtiyacı karşısında 2011 yılında kurulan Siber Suçlarla Mücadele Daire Başkanlığı tarafından yerine getirilmektedir.

Jandarma Genel Komutanlığı çatısı altındaki adli bilişim faaliyetleri ise Jandarma Kriminal Daire Başkanlığı tarafından yerine getirilmektedir. 2007 yılında kurulan Bilişim Laboratuvarları adli bilişim konusunda asli görevli birimleridir (JGK, 2019).

Adli Tıp Kurumu'ndaki adli bilişim faaliyetleri 2016 yılında başlamıştır. 672 sayılı Kanun Hükmünde Kararname ile kurulan Adli Bilişim İhtisas Dairesi, adli bilişim konusunda faaliyet göstermektedir.





3. MOBİL CİHAZ ADLI BİLİŞİMİ

3.1. Mobil Cihazlar

Mobil cihazlar, kendine özgü işletim sistemleriyle hücresel bağlantı ve wi-fi gibi diğer kablosuz bağlantı kanallarını kullanarak verileri iletmek, işlemek ve depolamak amacıyla tasarlanmışlardır. İş ve sosyal hayatta zaman ve verimlilik açısından avantaj sağlayan mobil cihazlar sınıfına taşınabilir nitelikte olan dizüstü bilgisayarlar girmemektedir. Öte yandan dizüstü bilgisayarlar gibi kullanılabilen ve onun yerini almaya başlayan tabletler bu sınıfa girmektedir. Ayrıca akıllı veya klasik cep telefonları, SIM kartlar, PDA cihazları, GPS cihazları, dron adı verilen insansız hava araçları, akıllı saatler, IoT cihazları da mobil cihaz olarak kabul edilmektedir (Doğanay, 2020: 56).

Gelişen teknolojiyle birlikte mobil cihaz özelliği taşıyan materyal sayısında ve çeşidinde büyük bir artış gözlemlenmiştir. Mobil cihaz niteliğindeki başlıca cihazları sıralayacak olursak:

Cep telefonları

İlk kullanılan cep telefonlarında telefon rehberi, arama kayıtları ve mesajlar gibi kısıtlı verilere erişilebilirken, son teknolojiyle birlikte yaygın akıllı telefonlarda resim, video, ses dosyaları gibi birçok multimedia içeriğe ve internet hesaplarında kullanılan kullanıcı bilgilerine de erişilmesi mümkündür. Bazı adli soruşturmaların çözümünde cep telefonları, başka şekilde ulaşılamayan deliller barındırdığından kritik rol oynayabilir (Kişeci, 2014: 184-185).

SIM kartlar

GSM hizmetleri alabilmesi için cep telefonları, tablet gibi cihazlarda kullanılmaktadır. SIM kartların hafızalarında rehber bilgisi yanında arayan, aranan ve cevapsız çağrı bilgileri gibi arama bilgileri, kısa mesajlar, IMSI bilgileri ve GSM şebekesine ait bilgiler de bulunmaktadır (Kişeci, 2014: 185).

Hafıza kartları

Bilişim sistemlerinde veri depolama kapasitesini artırmaya yarayan veri depolama birimleridir. Hem bağımsız olarak kullanılabilmekte hem de taşınabilmektedir. Cep telefonu, MP3 çalar, fotoğraf makinesi, tablet gibi birçok bilişim sisteminde ilave saklama

alanı imkânı amacıyla kullanılmaktadır. Hafıza kartlarında, adli bilişim açısından da önem arz eden değerli verilerle karşılaşılması mümkündür (Doğanay, 2020: 60).

Tablet

Tabletler, günlük yaşamda kullanılan bilgisayarların neredeyse tüm işlevlerini yerine getirebilirler. Tabletlerin genelde SIM kart ve hafıza kartı yuvaları bulunmaktadır. SIM kartlar vasıtasıyla hücresel internet bağlantısına erişebilirken; hafıza kartı sayesinde ilave veri kapasitesi kazandırılabilir. Bilgisayara benzer kullanımından dolayı, bilgisayarda karşılaşılabilecek dijital deliller ile karşılaşılması mümkündür (Kişeci, 2014: 184). Ancak bilgisayarlardan farklı olarak mobil işletim sistemlerine de daha sık rastlanılmaktadır.

Akıllı Saatler

Gittikçe yaygınlaşan bu teknolojinin, herhangi bir dijital saate göre çok daha fazla işlevi bulunmaktadır. Hatta akıllı telefonlara benzer işlevleri en ön plana çıkan özellikleridir. Cihazda bulunan dâhili hoparlör ve mikrofon sayesinde telefon gibi görüşme sağlaması, anlık mesajlaşma programlarının kullanılabilmesi, sesli komut alabilmesi, ses kaydetme, kamera, müzik dinleme gibi özellikleriyle günlük yaşantıda oldukça işlevsel hale gelmiştir. Ayrıca sağlık konusundaki adım ve nabız sayma özellikleri akıllı saatlere bu sektörde de talebi artırmıştır. (Doğanay, 2020: 62).

GPS cihazları

GPS, (the global positioning system) küresel konumlandırma sistemi ifadesinin kısaltması olup, bu sistem sayesinde Dünya çevresinde bulunan uydular aracılığıyla yeryüzündeki bir noktanın konumunun tespit edilmesi mümkündür. Bu cihazlar vasıtasıyla Dünya etrafında dönen uydular kullanılarak, yeryüzündeki konum belirlenebilmektedir. (Doğanay, 2020. 61)

Dron

Uzaktan kontrol edilebilen pilotsuz bir hava taşıtıdır. Bir tür insansız hava aracıdır (İHA). Önceleri askeri amaçlı tasarlanmış olan dronların, son yıllarda sivil kullanımı önemli ölçüde artmış, özel sektördeki ve endüstrideki payı büyümüştür (Al-Dhaqm, Ikuesan, Kbande, Razak, ve Gabban, 2021). Helikopter, pilot gibi gider ve maliyeti olmadığı için hem askeri hem de sivil kullanımda giderleri oldukça düşürmüştür. Günümüzde farklı boyut, konfigürasyon ve işlevlerde dronların üretimi gerçekleştirilmektedir. (Doğanay, 2020: 63).

3.2. Mobil Cihaz Adli Bilişimi Süreçleri

Mobil cihazlarda adli bilişim süreçlerine dahil olabilecek çeşitli bileşenler vardır. Bunlar, verinin depolandığı hafıza çipi, RAM, hafıza kartı ve sim karttır. Ancak bunların yanında olayın konusuna ve niteliğine göre bluetooth ve wi-fi gibi bağlantılar da delil niteliği kazanabilir (Çakır, 2014: 375).

Bu bölümde, delil elde edilmesi amacıyla mobil cihazlara yönelik gerçekleştirilen adli bilişim süreçleri ele alınmıştır. Mobil cihaz adli bilişimi kapsamında ilk müdahale yöntemleri, adli kopya oluşturma yöntemleri, karşılaşılan zorluklar, kullanılan yazılım ve donanımlar, incelemesi yapılırken dikkat edilmesi gerekenler, ileri düzey müdahale yöntemleri bilgileri aktarılacaktır.

3.2.1. Cihaza ilk müdahale

Niteliği itibariyle oldukça hassas olan dijital delillere ilk müdahale işlemi oldukça önemlidir. Bunun yanı sıra zehirli ağacın meyvesi zehirli olur prensibi gereği, teknik konuların yanı sıra hukuki açıdan da bu sürece önem gösterilmesi gerekmektedir.

Türk hukuk sistemine göre, bir suç konusunda delil elde edilmesi için başvurulacak mevzuat Ceza Muhakemesi Kanunudur. Bu sebeple, dijital delillerin elde edilmesine ilişkin uygulanacak usuller için de bu kanununun 134. Maddesi uyarınca şüphelinin kullanmış olduğu dijital materyaller için hâkim kararı veya gecikmesinde sakınca bulunan hallerde savcı talimatı gerekmektedir. Hâkim kararı ve savcı talimatının varlığı yanı sıra bunların aramanın gerçekleştirileceği olaya, kişiye veya adrese uygunluğu da teyit edilmelidir.

Hukuki açıdan kontrollerin ardından olay yerinin, cihazların ve ekranların fotoğraflarının çekilmesi gerekir. Muhafaza altına alınan cihazlarla ilgili olarak, önce marka, model, imei numarası, seri numarası gibi ayırt edici özelliklerin aidiyet bilgisi ile birlikte kayıt altına alınması gerekmektedir (Yılmaz ve Çakır, 2021). Ayrıca mobil cihazların muhafazası esnasında tarih, saat, çalışan uygulamalar ve bunlara ait ekran simgeleri, cihaz durum bilgilerinin tespit edilmesi delil güvenliği ve bütünlüğü açısından önem arz etmektedir.

Mobil cihazın bilgilerinin tespitinden sonra, dikkat edilecek bir diğer husus ise mobil cihazın açık veya kapalı oluşudur. Mobil cihazların açık veya kapalı olma durumlarında yapılması gerekenler değişmektedir.

Mobil cihaz açık ise; cihaz kapatılmaz. Cihazın kapatılmama sebebi cihazda bulunan pin ve güvenlik kodlarının olup olmadığının bilinmemesinden kaynaklanmaktadır. Cihazı incelemek için tekrar açıldığında bu kodlara ihtiyaç duyulacağından bu kodlar bilinmiyorsa cihazın kesinlikle kapatılmaması ve şarj durumuna bakılarak cihazın şarjı az ise şarj edilmesi ya da powerbank gibi güç kaynağına bağlı tutulması gerekir. Telefona ait şifre ve seri numarası tespit edilir. Cihazların seri ve IMEI numarasını elde etmenin birkaç yöntemi vardır. İlk olarak cihazın ayarlar, genel, hakkında kısmından ulaşabileceğimiz gibi, telefonun tuş kombinasyonundan (*#06#) tuşlanarak da ekranda görüntülenebilir. IMEI ve seri numarası telefonun arka kısmında da yer alabilir. Açık olan cihazdaki güvenlik ayarlarının imaj alma işlemi için uygun hale getirilmesi gerekir. Sonrasında telefonun şarj durumu göz önünde bulundurularak Faraday çantası içerisinde muhafaza edilmeli ve en kısa sürede adli kopyası alınmalıdır. Faraday çantası mevcut değil ise telefonun uçuş modu aktif hale getirilerek network bağlantısı kesilmelidir.

Hafıza kartı kontrol edilir. Cihazda takılı hafıza kartı olup olmadığı kontrol edilir. Cihazda hafıza kartı mevcut ise batarya sökülmeden hafıza kartı çıkarılıp marka, model, kapasite ve seri numarası bilgileri alınmalıdır.

Mobil cihaz kapalı ise; cihaz açılmaz. Cihaz faraday çantasının içerisinde açılarak pin ve güvenlik kodlarının etkin olup olmadığı kontrol edilir ve içinde bulunması muhtemel hafıza kartı ya da sim kart gibi diğer hafıza bileşenleri kontrol edilir.

Tablet, PDA ve cep telefonları gibi mobil cihazlar kasaları içindeki bataryalardan güç alarak çalışmaktadırlar. Bu cihazlara karşılaşılmaması durumunda öncelikle cihazlar açık ise, kapanmaması için şarj aletleriyle devamlılığının sağlanması, uçuş moduna alınması ve şebeke sinyalleri ve bağlı olunan kablosuz ağlar ile bağlantılarının kesilmesi gerekmektedir. Mobil cihaza hariçten gelen sinyalleri engellenmesi amacıyla faraday kafesi isimli koruyucu ortamlar kullanılabilir. (Kişeci, 2014: 185). Bu sayede mobil cihazların dış dünyayla iletişimi kesilerek, veride değişiklik, verinin silinmesi veya farklı amaçlı müdahalelerin önüne geçilmiş olur.

3.2.2. İmaj alma

İmaj nedir ve mobil cihaz incelemesine geçilmeden önce neden imaj alma işlemi gerçekleştirilir sorusu önem arz etmektedir. Yapısı gereği hassas olan dijital delilin, delil niteliğini, özgünlüğünü ve bütünlüğünü koruyarak inceleme işlemlerinde kullanılması için imaj alınmaktadır. Bu sebeple delil güvenliği açısından, dijital delilin depolama biriminin bire bir kopyası oluşturulur. İnceleme çalışmaları bu kopya üzerinden gerçekleştirilir. Oluşturulan bu adli kopyaya imaj ismi verilir.

İmaj alma, asıl ortamdaki tüm verilerin bit düzeyinde bire bir olarak farklı bir ortamda kopyalanmasıdır. Bit düzeyindeki birebir kopyalama işlemi, asıl dijital materyaldeki verilerin binary (ikili sayı) formattaki dizisiyle kopyalanmasını ifade eder. Bu sayede oluşturulan yeni kopyada MFT (Master File Table), tüm dosya sistemi, kullanılmayan alanlar ve silinmiş alanlardaki verilerde bulunmaktadır. Bu şekilde elde edilen kopyaya forensic duplicate (adli kopya) denilmektedir (Aydoğan, 2009: 35).

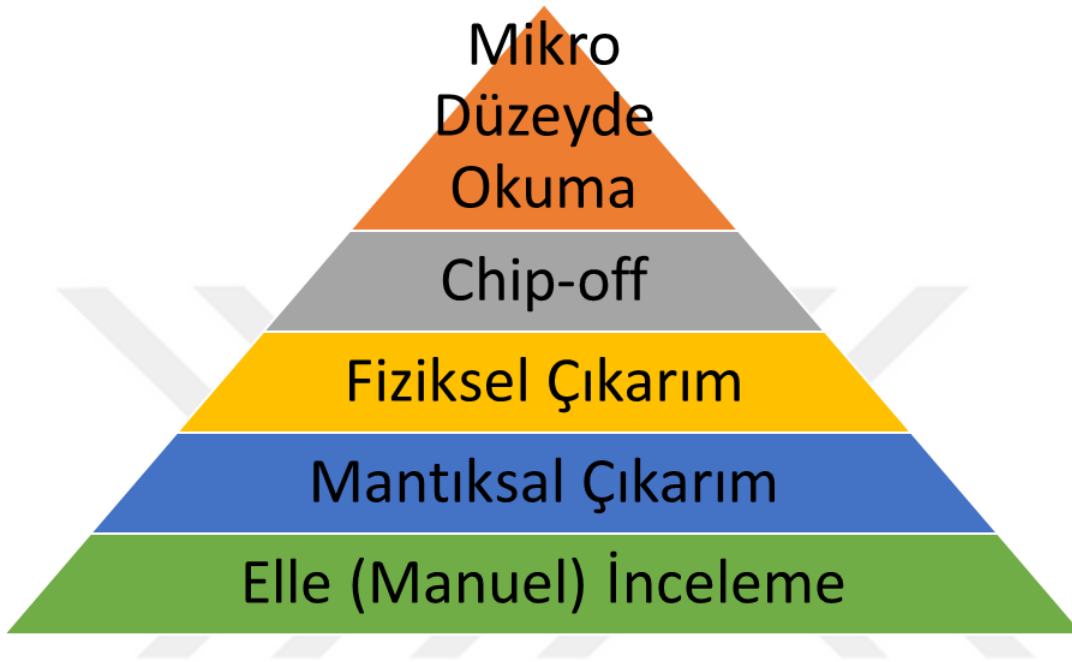
Günümüzde başvurulma yöntemleri ve türleri ele alındığından imaj alma işlemi için bir tanım yapılabilir. İmaj alma, delil elde etmek amacıyla içerisinde arama işlemi gerçekleştirilecek sayısal verilerin, özgünlüğünün ve bütünlüğünün korunarak bir kopyasının oluşturulması işlemidir.

Bir imaj alma cihazının güvenilir sayılabilmesi için sahip olması gereken özellikler şu şekilde belirtilmiştir (Wang, 2007):

- Asıl disk veya bölümün binary düzeyde birebir kopyasını alabilmeli,
- Asıl diskte herhangi bir değişiklik yapmamalı,
- Aldığı imajın bütünlük açısından doğrulamasını yapabilmeli,
- İşlem sırasındaki hataları kaydedebilmeli,
- Kaydedilen dokümantasyonun çıktısı doğru olmalıdır.

Adli bilişim alanındaki birebir kopyalama işlemi, imaj (forensic image) olarak adlandırılmaktadır. Bu kopyalama işlemi niteliği itibariyle sistemdeki tüm verilerin bazı özel araçları kullanılmasıyla ve bit bazında başka bir ortamda bir örneğinin oluşturulmasıyla gerçekleştirilir. Kopyalama işleminin alt seviyede yapılması, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilerin tespitini sağlamaktadır (Günel, 2012).

Mobil cihazlardan alınan veri niteliğine göre yöntemler değişmektedir. Elde edilen veriye ve yöntemin maliyetine göre mobil cihazlardan veri çıkarma yöntemleri Şekil 3.1’de gösterildiği üzere altı farklı kategori de sınıflandırılması mümkündür (Jansen ve diğerleri, 2014: 17.)



Şekil 3.1. Mobil Cihaz Adli Bilişimi Araçları (Jansen ve diğerleri, 2014)

Manuel İnceleme

Kullanıcı arayüzü aracılığıyla elde edilen bilgileri içermektedir (Jansen ve diğerleri, 2014: 17) Bu yöntem en temel seviye bilgiyle gerçekleştirilebilen yöntemdir. Uygulayıcı tarafından telefonunun açılarak menüler arasından gezinmesi suretiyle yaptığı tespitlerden oluşmaktadır. Bunun için cihazın çalışıyor ve şifresinin aşılmış olması gerekmektedir.

Normal bir kullanıcı gibi telefon kullanılarak menülerde ve alt menülerinde el ile dolaşılır. Bu aşamada tespit edilenler kamerayla belgelenir. Bu inceleme türünde dikkatsizlik sonucu delilde değişiklik meydana gelebilir. Mobil cihazdaki fiziksel arızalarsa, bu inceleme işlemi için sorun teşkil edebilmektedir. (Çakır, 2014:389)

Mantıksal çıkarım

Mantıksal çıkarım ya da mantıksal imaj alma yöntemi en fazla sayıda mobil cihazı destekleyen hızlı bir ayıklama yöntemi olarak bilinmektedir. Temel düzeyde eğitim ve orta

düzyey teknik bilgi, mantıksal çıkarım işlemini gerçekleştirmek için yeterlidir (Jansen ve diğlereri, 2014: 17). Daha üst seviyedeki imaj alma yöntemlerine göre daha az veri getirir de birçok cihaz için başvurulabilmektedir. Mantıksal imaj alma yöntemiyle ayıklanabilecek veri türleri, arama kayıtları, telefon defteri, SMS'ler, takvim etkinlikleri, çoklu ortam dosyaları (resimler, videolar, ses dosyaları) ve uygulama verileri olarak bilinmektedir. Ancak cihazın şifreli olması mantıksal imaj alma işlemi için büyük sorun teşkil etmektedir (Yılmaz ve Çakır, 2021).

Bazı mobil cihaz inceleme yazılımları tarafından daha fazla veri elde edilmesi amacıyla bir diğler mantıksal çıkarım işlemi sunulmaktadır. Buna gelişmiş mantıksal çıkarım ya da dosya sistemi çıkarımı denilmektedir. Mantıksal imaj alma yöntemine göre daha kapsamlı veriler getirebilmektedir. Dosya sistemi yöntemiyle alınan bir imajda, mantıksal bir uzantı ile görünmeyecek gizli sistem dosyalarına ulaşılabilir. Mobil cihazın belleğindeki resimler, videolar, veri tabanı dosyaları, sistem dosyaları olmak üzere çoğu dosyaya bu yöntemle erişim sağlanabilir. Cihazın sisteminde kurulu bulunan ya da daha sonra kullanıcı tarafından yüklenen mobil uygulamaların çoğu bu yöntemle çıkartılan veri tabanı dosyalarında saklanmaktadır. Bu yöntem kullanılarak imaj alındığında arama kayıtları, mesajlar, kullanıcı parolaları, uygulama verileri, rehber ve kullanıcıya tahsis edilmiş alanda yer alan diğler verileri elde etme ihtimali bulunmaktadır.

Fiziksel çıkarım

Bu yöntemle imaj alındığında, diğler imaj alma yöntemlerine göre daha geniş ve kapsamlı veriye ulaşılabilir. Mobil cihazda bulunan hafıza çipindeki verinin PCB (printed circuit board-baskı devre kartı) üzerindeyken elde edilmesi işlemidir. Bu işlem ileri düzey uzmanlık gerektirmektedir (Jansen ve diğlereri, 2014: 18-19). Mobil cihaz üzerinde, "bit-to-bit" yani her bir bit verinin kopyasının alınması yöntemi ile binary (1 ve 0'lar) seviyesinde ayıklama işlemi yapabilmektedir. Bu yöntem kullanılarak imaj alındığında veri raw (ham veri) formatında olduğundan silinmişleri de dahil olmak üzere kullanıcı verilerine, konumlara, baz istasyon bilgilerine, SMS'lere, MMS'lere, WhatsApp, Viber, Telegram, Messenger gibi üçüncü parti anlık mesajlaşma uygulamalarına, veri tabanı dosyalarına, gizli sistem dosyalarına ve ayrılmış alandan silinen verilere ulaşılması mümkündür. Bu yöntemde alınan veri binary seviyesinde olduğundan gerektirdiği uzmanlık yüksek seviyededir (Akalin, 2016: 45).

Chip-off

Bu yöntem de binary düzeyde veri elde edilmesine yönelik gerçekleştirilen işlemlerden biridir. Mobil cihazda fiziksel açıdan kalıcı hasarlar bıraktığından genelde son çare olarak başvurulmaktadır. PCB üzerinde bulunan kalıcı veriyi tutan hafıza çipinin sökülmesi ve özel donanımlarla iletişim kurulması işlemidir (Zareen ve Baig, 2010).

Chip-off yönteminin başarısı, çipteki verinin okunabilir olmasına bağlıdır. Apple marka akıllı telefonların hafıza çipindeki veriyi de şifrelenmiş olarak tuttuğu bilinmektedir. Ayrıca Android işletim sistemli akıllı telefonların da gelişen teknolojiyle birlikte hafıza çipindeki veriyi şifreli tutmasından dolayı, chip-off yöntemi işlevsiz hale gelmektedir.

Mikro düzeyde okuma

Mikro düzeyde okuma yöntemi, yüksek güçlü mikroskop kullanılarak çip üzerindeki fiziksel kapıların görüntülenmesiyle gerçekleştirilir (Jansen ve diğerleri, 2014). Bu işlem neticesinde her bir bit verinin karşılığı olan 1 ve 0'lar tespit edilir. Bu bitler bir araya getirilerek, işletim sistemi, dosya sistemi, metadata (üst veri) ve dosyaların verilerine erişilmesi amaçlanmaktadır. Ancak her bir bitin tespiti ve bu bit yığınlarının anlamlı hale getirilmesi işlemi çok zahmetli ve maliyetli bir işlemdir. 128 GB kapasitesindeki bir telefonun tüm verisinin çıkartılması işlemi için bir trilyondan fazla kez bu işlemin yapılması gerekmektedir. Dünya genelinde bu düzeyde çalışma gerçekleştirmiş olduğu bilinen gelişmiş laboratuvarlar vardır. Türkiye’de bu işlemin uygulandığında ilişkin herhangi bir veriye rastlanılamamıştır.

Özetle imaj alma, adli bilişim alanında bire bir nitelikteki adli kopyanın alınması anlamında kullanılmaktadır. Temelde fiziksel imaj alma ve mantıksal imaj alma olarak iki düzeyde gerçekleştirilmektedir. Fiziksel imaj alma işleminde, mobil cihazın “bit-to-bit” tabir edilen ilk sektörden son sektöre kadar olan bütün verilerin alınması şeklinde gerçekleştirilirken, mantıksal imaj alma işleminde ise verinin bir kısmının yedeğinin alınarak bunun adli bilişim standartlarına uygun hale getirilmesi şeklinde gerçekleştirilir. Getirdiği verinin niteliği itibariyle fiziksel imaj alınması tercih edilmektedir. Fiziksel imaj alınması için, chip-off ya da mikro düzeyde okuma yöntemlerine başvurulması mümkündür.

Cihazın donanımsal veya yazılımsal özelliklerinden dolayı veya teknik imkân bulunmuyor olmasından dolayı fiziksel imaj alınamaması mümkündür. Bu durumda mobil cihaz adli

bilişiminde alınan adli kopyalar yaygın olarak mantıksal imaj yöntemiyle elde edilmektedir. Mantıksal imaj, niteliği itibarıyla iTunes Backup gibi üreticilerin cihazları yedeklemek için kullandıkları yazılımlardan elde edilen yedek şeklindedir (Doğanay, 2020: 90).

Mobil cihazların fiziksel veya mantıksal imajlarının alınması için bazı yazılımlara başvurulmaktadır. Bunların içinde en bilinenleri:

- Axiom (Magnet Forensic)
- UFED (Cellebrite)
- XRY (MSAB)
- Oxygen Forensic Detective
- PC3000 Mobile
- Hancom
- Belkasoft
- MobilEdit
- Paraben
- Katana Forensics
- Blackbag
- Andriller
- FTK (Access Data)

Bu yazılımlar, mobil cihazlardan imaj alma ve alınan imajlarda inceleme işlemleri yaparak dijital ortamlara delillerin ulaşmasına imkân sağlayan mobil cihaz inceleme yazılımlarıdır. Mobil cihaz üreticileri cihazlarındaki verinin güvenliği için teknolojiler üretirken, bu yazılımlar ise daha fazla veriyi elde etme amacıyla tasarlanmışlardır. Birbirlerine kıyasla artıları ve eksileri olmakla birlikte, gelişen teknolojiyle birlikte sürekli güncellenmektedirler. Mobil cihaz adli bilişimi uygulayıcıları, genellikle bu yazılımlardan birini kullanmaktadırlar.

3.2.3. İnceleme

İnceleme işlemi genellikle adli bilişim açısından uygun olarak oluşturulan imaj olarak da bilinen adli kopyalar üzerinden gerçekleştirilmektedir. İmaj alma işlemi sonrasında yapılacak işlemler sırasıyla, çözümleme, veri çıkarımı ve inceleme (delili tespit etme) işlemidir.

Çözümleme Süreci (Process)

Dijital materyallerden alınan adli kopya içerisindeki ham haldeki verilerin çeşitli yazılımlar vasıtasıyla anlamlandırılması, varsa dosya dizinlerinin oluşturulması, sistem bilgilerinin tespit edilmesi ve incelenmek üzere uygulayıcı önüne getirilmesi sürecine verilen isimdir. Kısaca adli kopyanın incelemeci tarafından anlaşılacak hale getirilmesi işlemidir. Bu işlem genelde yüksek kapasiteli iş istasyonları ve adli bilişim yazılımlarıyla gerçekleştirilmektedir.

Veri Çıkarımı (Export)

Adli kopya içerisindeki verilerin anlamlı hale getirilmesinden sonraki, teknik konulardan ziyade suç konusuna hâkim olan son kullanıcı (genelde soruşturmayı yürüten kolluk birimi ya da Cumhuriyet savcısı) seviyesinde sunulması işlemine verilen isimdir. Yani dijital verileri kategorize edilmiş şekilde kullanıcının önüne çıkarma işlemidir. Delil tespiti amacıyla yapılan inceleme işlemleri export veri üzerinden olabileceği gibi adli bilişim yazılımı vasıtasıyla da gerçekleştirilebilmektedir.

İnceleme İşlemi

Dijital deliller üzerinden elde edilen adli kopyaların ve çıkarımı yapılan dosyaların, adli bilişim yazılımları vasıtasıyla veya manuel olarak bulguların ortaya çıkarılmasına yönelik tespitlerin yapılması işlemidir. İnceleme işleminde, suçun aydınlatılması için 5N1K sorularının yanıtlanması gerekmektedir. Bu aşamada ne aranıyor / ne bulduk, nerede bulunabilir / nerede bulundu, nasıl bulunabilir / nasıl bulduk ile tespit edilen bulgu ne zamana ait ve kime ait soruları sorulmalıdır.

Adli kopyası alınan verilerin inceleme aşamasına geçilmeden önce kontrol edilmesi gerekmektedir. Alınan verilerin eksiksiz olduğundan emin olmak adına yazılım ile doğrulanması ve hash değerlerinin kontrolü en çok başvurulan yöntemlerdir.

İnceleme işlemi bitiminde raporda bu hususların belirtilmesi gerekmektedir. Bunun yanı sıra kullanılan yazılımlar ile yöntemlerin de detaylıca raporda yer alması, yapılan işlemin ileride doğrulanması durumları açısından önem arz etmektedir.

Mobil cihazdan veriler eksiksiz bir şekilde çıkarıldığı takdirde PIN ve güvenlik kodu biliniyorsa ya da aktif durumda değil ise, telefon kapatılarak SIM ve hafıza kartı

incelemesine geçilir. SIM ve hafıza kartı yoksa dijital delil raporlanarak ilgili birimlere nakli sağlanır.

Mobil cihaz incelemesi, bilgisayar ve disk incelemesine göre bazı farklılıklar ve zorluklar içermektedir. Mobil cihazların çeşitlilik açısından zengin oluşu ve bunların kullanmış olduğu işletim sistemi, dosya sistemi, uygulamalar, bağlantı kabloları gibi çevre birimleri de farklılıklar gösterdiğinden, yeni model mobil cihazın çıkması durumunda, bu modelin çıkış zamanı ile mobil cihaz inceleme yazılımları tarafından bu cihazın desteklenmesi arasında boşluklar olabilmektedir (Çakır, 2014: 384).

Mobil cihazların modellerinin çeşitliliği, sürekli değişen yazılım ve mobil uygulamalar ile teknolojiye gerçekleşen hızlı değişim, mobil cihazlar açısından adli bilişim inceleme sürecini oldukça zorlaştıran durumlardır. Bunların yanı sıra sayılan faktörler doğrudan etki etmektedir (SWGDE, 2019):

- Gelen ve giden sinyaller: Mobil cihazların yapısı gereği sürekli iletişim halinde olmasından dolayı gelen ve giden sinyaller veride değişikliklere sebep olabilir.
- Kablolar: Mobil cihazların veri kablolarındaki farklılık ile kullanılan adli bilişim yazılımının özel bir kabloyla kullanılıyor olması gibi durumlarda çeşitli kablolara ihtiyaç duyulabilmektedir.
- İletişim portları: Kullanılan adli bilişim yazılımlarından bazıları, mobil cihazdaki belirli iletişim portlarını kullanabilmektedir; ancak bu kullanım sonrası işletim sistemi portun tekrar kullanımına izin vermeyebilir.
- Delilin durumu: Delilin fiziksel hasarlarının bulunması, adli bilişim yazılımlarının başarısını olumsuz olarak etkilemektedir.
- Delilin tahrip edilmesi: Mobil cihazdaki verinin bozulması için cihaz üzerinde veya uzaktan erişimle uygulanmak üzere bazı yöntemlere başvurulmuş olabilir.
- Sürücüler: İşletim sisteminin kullandığı sürücüler ile diğer kaynaklardan elde edilen sürücüler arasında yetki ve sürümden kaynaklı uyumsuzluklar olabilir. Özellikle mobil cihaz incelemesi için kullanılan iş istasyonlarında birden fazla araç kurulu olduğu durumlarda sürücüler kaynağın kontrolünü almak için çatışabilir.
- Şifreleme: Veriye erişimi engelleyen bazı şifreleme tedbirleri mevcut olabilir.
- Kullanılan araçlar: İnceleme için kullanılan araçlar en güncel sürümde olmayabilir.

- Hash değeri: Resim, ses, video gibi dosyaların verilerin sabit olmasından dolayı hash değeri açısından tutarlılık gösterirken, dinamik yapıdaki işletim sistemi gibi sistem dosyalarında tutarlılık olmayabilir.
- Hukuki sorunlar: Mobil cihazda bulunan veya mobil cihaz üzerinden erişilen iletişime dair verilerin hukuki statüsü ülkeden ülkeye değişiklik göstermektedir.
- Güç kesintisi: Mobil cihazların şarjının bitmesi veya farklı sebeple kapatılması durumunda veri kaybı veya başkaca güvenlik tedbirleriyle karşılaşılabilir.
- Parolalar: Mobil cihazdaki kullanıcı verilerini korumak amacıyla konulmuş olan parolalar veriye erişimi kısıtlayabilir. Parolaları kırmak için kullanılan kaba kuvvet saldırısı gibi geleneksel yöntemler verilerin kalıcı olarak silinmesine sebep olabilir.
- Hafıza kartları: İnceleme aşamasında mobil cihazla bir bütün olarak incelendiği durumlarda, bu ortamdaki silinmiş veriler ile zaman damgasının değişme riski olabilmektedir.
- Tanımlama kartları (SIM): SIM kartın olmaması veya çıkarılmış olması durumunda, bazı mobil cihazlarda veriye erişim engellenebilir.
- Endüstri standartları: Mobil cihaz üreticileri açısından, cihazdaki verinin nasıl saklanması gerektiğine ilişkin bir standart bulunmamaktadır.
- Verinin dinamik yapısı: Çalışır durumda bulunan mobil cihazlardaki veriler sürekli değişmektedir; ancak mobil cihazlar için geleneksel bir yazma koruma yöntemi bulunmamaktadır.
- Silinmiş veriler: Fiziksel çıkarım yapıldığı durumlarda silinmiş veriye ulaşılabilenken; mobil cihaz adli bilişimi yazılımları genelde mantıksal çıkarımı desteklemektedir.

Delil elde edilmesi için başvurulduğu bir olayda, mobil cihazlarda üç temel veri kaynağından bahsedilebilir: servis sağlayıcı, telefonun kendisi ve telefonun harici kartları. İncelenen olayın niteliğine de bağlı olarak bu kaynaklardan farklı verilerin temini mümkündür (Çakır, 2014: 392).

- Servis sağlayıcıdan elde edilmesi muhtemel veriler beş başlık altında ele alınabilir. Arayan numara, aranan numara, aramanın süresi ve zamanı bilgilerini içeren arama kaydı detayları (CDR), aboneye ait kimlik ve adres bilgileri, sesli mesajlar, kullanım bilgisi ve Bağlantı kurulan baz istasyonları ile bağlantı zamanları ve mevcut konumu içeren izleme bilgisidir.

- SIM karttan elde edilecek veriler ise telefon numarası (MSISDN), uluslararası mobil abone kimliği (IMSI), kartın seri numarası niteliğindeki entegre devre kart tanımlayıcısı (ICCID), servis sağlayıcı adı (SPN), dil tercihleri ve cihaz kapatıldığında son konum bilgisinden oluşmaktadır.
- Sadece telefondan elde edilebilecek altı farklı veri türü vardır. Bunlar, uluslararası mobil ekipman kimliği (IMEI), telefon bilgisi, ağ bilgisi, GPS bilgisi, takvim ve hatırlatma gibi alanlardaki yapılacak listesi ve son olarak da radyo işlevlerinin durumu, baz istasyonu, gateway bilgisi, cihazın kaynak kullanım durumu gibi iletişim loglarından oluşmaktadır.
- Telefon veya SIM karttan elde edilecek veriler ise telefon rehberi, arama geçmişi ve süresi ile mevcut veya silinmiş SMS mesajları, MMS mesajlarıdır.
- Telefondan veya hafıza kartından elde edilecek veriler ise fotoğraflar, videolar, ses dosyaları, elektronik postalar, dokümanlar, internet kullanım bilgisi, tarayıcı geçmişi, favori siteler ve kurulan uygulamalara ait verilerden oluşmaktadır.

Mobil cihaz adli bilişimi işlemi teknik bir işlemdir ve uzman personel tarafından yerine getirilmesi gerekmektedir. (Çakır, 2014: 393). Veri ne şekilde elde edilmiş olursa olsun, genel yaklaşım şu şekildedir: (Casey ve Turnbull, 2011: 29).

- Mobil cihazlar üzerindeki başlıca bilgi kaynaklarına aşina olmak için araştırma yapılır.
- Dosya, mesajlar, arama kayıtları ve multimedya dosyaları gibi silinmiş ögeler kurtarılır.
- Silinmiş alanlardan kurtarılanlar da dahil olmak üzere dosyaların adı, zaman damgaları, aramanın gelen, giden ya da cevapsız çağrı olması veya mesajın okunup okunmadığı gibi üst veriler toplanır.
- Delillerin tespiti için anahtar kelime veya soruşturmaya özel bilgiler ile metodolojik bir araştırma yürütülür.
- Olayların zaman çizgisi ve ilişki tablosu dahil edilerek, cihazın belleğinden elde edilen bilgilerin zamansal ve ilişkisel analizi yapılır.
- Adli bilişim araçlarının hataları ve açıkları olabileceğinden önemli sonuçların doğruluğu sağlanır.

3.3. Mobil Cihaz Adli Bilişimi Araçları

Bu kısımda mobil cihaz adli bilişiminde Türkiye’de ve dünya genelinde en sık başvuru alan yazılımlar üzerinde durulacaktır. Mobil cihaz adli bilişimi yazılımları, nitelikleri itibarıyla uygulayıcıya imaj alma ve analiz imkânı sağlamaktadır. Bu yazılımların amacı mobil cihazdaki silinmiş dahi olsa verilere ulaşmak ve adli bilişim açısından analiz gerçekleştirmektir. Ayrıca her bir yazılımın diğerlerinden bazı farklılıkları bulunmaktadır. Mobil cihazların adli kopyasının oluşturulmasında ve incelenmesinde kullanılan yazılımlar kısaca:

Magnet Axiom

2019 yılında kurulan Magnet Forensics firmasının ürünüdür. Bu firma bilgisayar ve mobil inceleme yazılımı geliştirmektedir. Axiom, IEF (Internet Evidence Finder) yazılımının daha gelişmiş ve kompakt hale getirilmiş şeklidir. İnternet kalıntılarındaki başarısı, geniş uygulama desteği ve görsel arayüzündeki kolaylık sayesinde inceleme çalışmalarında fayda sağlayan bir yazılımdır. Axiom yazılımı, diğer adli bilişim yazılımlarıyla alınan imajları ve chip-off ya da j-tag yöntemleriyle alınan imajların da anlamlandırılmasını sağlayarak analiz imkânı sunmaktadır (Magnet Forensics, 2022).

Cellebrite UFED & Physical Analyzer

İsrail menşeli olan Cellebrite firması mobil cihaz inceleme yazılım ve donanımlarını geliştirmektedir. UFED yazılımı (Universal Forensic Extraction Device), mobil cihazlardan (cep telefonu, tablet, GPS cihazı, insansız hava araçları, hafıza kartı, taşınabilir HDD ve sim kart) adli kopya alma işlemlerini yaparak dijital ortamlara delillerin ulaşmasına imkân veren bir mobil cihaz inceleme yazılımıdır. Diğer adli kopya oluşturma yazılımlarına göre daha çok marka ve model desteği bulunmaktadır (Teel Technologies, 2012). UFED yazılımıyla, telefonlarda bulunan kullanıcı şifrelerini (pattern, pin, password) bypass etme, adli imajı alınamayan telefonların anlık ekran görüntüsünü alarak rapor haline getirebilme gibi işlemler de yapılabilmektedir. Yazılımda bulunan cihaz araçları bölümünden de imaj alma sırasında oluşan ya da cihaz elimize ilk ulaştığında tespit edilen, başlatma sorunları, hatalar ve yazılımsal arızalar giderilebilmektedir. UFED’in yazılım olarak UFED 4PC, donanım olarak UFED Touch2 ve yazılım kurulu bilgisayar olarak UFED Ruggedized Laptop ürünleri bulunmaktadır (Cellebrite, 2022).

Cellebrite Physical Analyzer yazılımı ile adli bilişim yazılımlarıyla alınmış olan imajları anlamlandırmaya ve detaylı olarak incelemeye yarayan programdır. Ufed Physical Analyzer programı vasıtası ile UFED, XRY, Oxygen, Axiom, Pc3000 Mobile, MobilEdit vb. yazılımlar ile alınmış olan imajlar anlamlandırılarak program vasıtası ile detaylı bir inceleme yapıp raporlanabilmektedir. Bu yazılım dijital delildeki anahtar parçaların ortaya çıkarılmasına, olayların takip edilmesine ve dijital verinin incelenmesine yardım etmektedir (Cellebrite, 2022).

XRY

İsveç menşeli Micro System firması mobil cihazlar üzerine imaj alma ve inceleme yazılım ve donanım ürünlerini geliştirmektedir. XRY yazılımı verileri, hızlı, güvenilir ve hukuki olarak aldığını iddia etmektedir. Başlıca olay yerinde hızlı sonuca gitmek için Frontline Extractions çözümüyle birlikte cihazın kilidini geçme, şifreleri elde etme ve dijital delili anlamlı hale getirmek için Lab Extractions çözümleri bulunmaktadır (MSAB, 2021).

Oxygen Forensic Detective

Oxygen Forensic isimli firmanın, mobil cihazlar, hafıza kartları, dron, bulut yapıları gibi çeşitli türdeki kaynaklardan adli kopya oluşturma, veri çıkarımı, şifre çözme ve analiz yapma gibi özellikleri içerisinde barındıran bir adli bilişim yazılımıdır. Bunların yanı sıra şifre kırma ve silinen verileri kurtarma gibi özelliklere de sahiptir (Oxygen Forensics, 2022).

PC3000 Mobile

Veri kurtarma çözümleriyle ön plana çıkmış olan ACE Laboratory firmasının mobil alanda sunduğu çözümdür. Mobil cihazlardan veri kurtarma ve adli kopya oluşturmak amacıyla kullanılan bir yazılım ve donanım kitidir (ACELab, 2022). Yazılımla birlikte çip okuma aparatları da mevcuttur. Daha çok chip-off yönteminde ön plana çıkmaktadır.

Hancom

Güney Kore menşeli olan mobil cihaz inceleme yazılımı iki alt modülden oluşmaktadır. MD-NEXT, akıllı telefonlar, nitelikli telefonlar, dronlar, akıllı TVler, giyilebilir teknolojiler gibi mobil cihazlardan adli kopya oluşturma amacıyla kullanılan modüle verilen isimdir. MD-RED: Adli kopyası oluşturulan mobil cihazlardan veri kurtarma, inceleme ve raporlama işleminin yapılması amacıyla oluşturulan modüldür (Hancom, 2017). Arayüzü kolay bir

yazılım olduđu için kullanımı basittir. Birden fazla cihazın aynı anda imajını alabilmesi yazılımın avantajları arasında değerlendirilmektedir.

Forensic Tool Kit

Exterro firmasının bu ürününe özellikle disk inceleme konusunda sıklıkla başvurulmaktadır. Disk inceleme alanında oldukça geniş imkanlar sunmaktadır (Exterro, 2022). Mobil cihaz alanında ise chip-off işlemi gerçekleştirilen cihazların ağaç yapısını görüntüleyebilmektedir. Bazı telefon ve tablet çiplerinin imajını alabilmektedir.

3.4. Teknik Müdahale Yöntemleri

Normal şartlarda veriyi elde etmek ve imaj almak için mobil cihaz yazılımlarına başvurulmaktadır. Ancak bu araçlar imaj alma konusunda her zaman başarılı olamamaktadır. Bunların sebebi ise genellikle cihazdaki veriye erişimi engelleyen sorunlardır. Verinin normal yollarla elde edilememesi durumunda fiziksel müdahaleyi de kapsayan bazı ileri düzey teknik yöntemlere başvurulması ihtiyacı hâsıl olmaktadır (Doğanay, 2019: 87). Bu müdahaleler fiziksel olabileceği gibi yazılımsal nitelikte de olabilir. Bu müdahaleler nitelikleri itibariyle orijinal cihazda ve üzerindeki veride değişikliklere sebebiyet vereceğinden dolayı, delil güvenilirliği açısından yapılan tüm işlemlerin detaylıca tutanak haline getirilmesi mutlak bir zorunluluktur.

3.4.1. Yazılımsal müdahale

Mobil cihazların imajının alınabilmesi için genellikle cihazın açık ve çalışır vaziyette olması gerekmektedir. İmajını alınması hedeflenen cihazda, işletim sistemi düzeyindeki hatalardan dolayı çalışmama ya da mevcut cihazın bazı özelliklerinin (işletim sisteminin sürümü, bootloader kilidi gibi) varlığı nedeniyle veriye erişimi engellemesi durumlarıyla karşılaşılabilir. Bu durumda yazılım düzeyinde bazı müdahalelerde bulunulması gerekmektedir. Mobil cihazların kurtarılmasında kullanılan yazılımsal işlemler:

Yazılım sorunlarını düzeltme

Cihazlara uygun yazılımların paket hali olan rom dosyaları yüklenerek cihazın çalışır hale getirilmesi işlemidir. Özellikle Android işletim sistemli cihazlarda recovery sorunları modele göre stock rom dosyası (üretici tarafından hazırlanan rom dosyası) yüklenerek yazılım düzeltilir.

Root atma

Telefon veya tablet gibi Android işletim sistemli cihazlarda kök klasöre erişim sağlanarak yönetici yetkisi alma işlemine verilen isimdir (Yılmaz ve Çakır, 2021). Bu sayede üretici tarafından yazılım düzeyinde alınan güvenlik tedbirlerinin aşılması hedeflenmektedir. Root işlemiyle kullanıcı, yazılım yükleme, standart kullanıcıların dosyalarını silme ve diğer işletim sistemi servislerine müdahale gibi hakları elde etmektedir (James, Sosha ve Gladyshev, 2012: 12).

Android işletim sistemini kullanan cihazın rootlanması, Linux işletim sisteminde olduğu gibi cihaz üzerindeki standart kullanıcıların yetkisinin ötesindeki işlemlere imkan sağlamaktadır. Root işlemiyle, kullanıcı mobil cihazını daha yüksek yetkilerle kullanabilmekte ve cihaz üzerindeki kontrolünü artırmaktadır (Sun, Cuadros ve Beznosov, 2015).

JailBreak

Root işleminin iOS işletim sistemli telefonlardaki halidir. IOS işletim sistemi Apple'a ait iPhone, iPad, iPod Touch gibi mobil cihazlardaki işletim sistemidir (Hoog ve Strzempka, 2011: 55). Bu işletim sistemi, kendi uygulama marketi olan App Store dışında uygulama veya eklenti kurulmasına müsaade etmemektedir (Govindaraj, Verma, Mata ve Gupta, 2014). Güvenlik maksadıyla kullanıcıları kısıtlaması ile bilinen Apple cihazlardaki bu kısıtlardan kurtulmasının bir özgürlüğe kavuşma olarak değerlendirildiğinden jailbreak yani hapisten kaçış olarak adlandırılmıştır. Apple şirketi, bu işlemin Apple cihazlardaki garantiyi bitirdiğini duyurmuştur (Kahney, 2010).

3.4.2. Fiziksel Müdahale

Normal şartlarda imaj alınamamasının veya veriye ulaşamamasının sebebi kimi zaman donanımsal bazı engellerden kaynaklanabilmektedir. Bu engellerin aşılması mümkünse, bunu gerçekleştirmek için fiziksel müdahale yöntemlerine başvurulmaktadır. Bu işlemler sonucunda cihazda kalıcı değişiklikler meydana geleceğinden, işleme başlamadan önce başarılı sonuç alma ihtimali ile risklerin birlikte değerlendirilmesi gerekmektedir. Mobil cihazların kurtarılmasında kullanılan fiziksel müdahaleler:

Cihazın tamiri

Normal yöntemlerle imaj işlemi için iletişim kurulamayan durumlarda bunun sebebinin tespiti yapılması gerekir. Kimi zaman cihazın ana kartındaki bir sıkıntı yüzünden cihaz

çalışmazken, kimi zaman da portlarındaki arıza yüzünden cihazla iletişim kurulamayabilir. Tamir işlemiyle bu arızaların giderilmesi ve veriye ulaşılması hedeflenmektedir. Bu yöntem diğer fiziksel müdahale yöntemlerine göre daha az maliyetli bir yöntemdir. Ayrıca verinin bütünlüğü açısından daha az risklidir (Yılmaz ve Çakır, 2021). Bu sebeple diğer yöntemlerden önce tamir işlemiyle aşılması denenmektedir.

J-Tag (Joint Test Action Group)

Bu işlem, cihazın ana kartı üzerindeki test pinlerine lehimleme yapılarak verilere erişilmesidir. Android işletim sistemli cihazların eski sürümlerinde başarılı sonuçlar alınan bu yöntem, Android işletim sisteminin 7 sürümüyle birlikte verilerin disk düzeyinde şifrelenmesiyle önemini yitirmiştir.

Chip-Off

Normal standartlarda mobil yazılımlar vasıtasıyla adli kopyası oluşturulamayan, parçalanmış, aşırı neme maruz kalmış cihazların, kalıcı veriyi tutan hafıza çiplerinin anakart üzerinden sökülerek çip okuma aparatları vasıtasıyla okutulması işlemine verilen isimdir.

“Telefonun bellek yongasının (NAND) fiziksel olarak çıkarılması ve tüm verinin birebir kopyasının bir okuyucu marifetiyle bilgisayara aktarılmasıdır. Bu yöntemde, imajı yorumlamanın zaman alması, bitişik olmayan veriler, yonga türlerinin çok çeşitli olması, yonganın çıkarılması esnasında zarar görmesi riski ve verinin şifreli olması gibi zorluklarla karşılaşilmektedir.” (Çakır, 2014: 390)

Bu işlemde, çipi karta bağlayan bacaklar ısıtılarak, kart ile bağlantı kesilmekte ve çipin pin dizilimine (pin-out) uygun adaptörler vasıtasıyla veriye ulaşılmaktadır. Bu yöntemle fiziksel imaj alınmaktadır. Ancak mobil cihaz üreticilerinin verileri disk düzeyinde şifrelemesi, bu yöntemin etkinliğini önemli ölçüde azaltmıştır.

ISP (In System Programming)

In System Programming, sistem üzerindeyken programlama işlemidir. Bu yöntemin işlevi, programlanabilir aygıtların, mikro denetleyicilerin ve diğer gömülü bileşenlerin bütünleşik sistem üzerindeyken programlanabilmesidir (Bonnett, 1999). J-tag işleminin desteklenmediği bazı çiplerde bu yöntemle başvurulmaktadır.

4. KARAR DESTEK SİSTEMLERİ

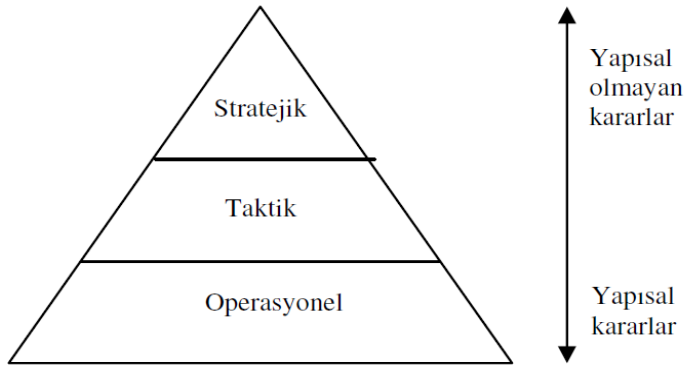
Bu bölümde karar destek sistemlerini (KDS) açıklamak için literatürde yapılmış olan tanımlara yer verilecektir. Daha sonra KDS türleri, KDS'nin özellikleri, KDS oluşturma ile KDS'de kullanılan karar ağacı algoritması ele alınacaktır.

Karar verme süreçleri, özellikle işletmeler açısından önem arz etmektedir. Çünkü rekabet koşullarındaki değişim, yönetime ilişkin sorunların karmaşık hale gelmesi, değişimler karşısında alınması gereken hızlı tedbirler ve yenilikçi yaklaşıma dair arzu, karar vericiler yani yöneticiler için baskı unsuru haline gelmiştir (Kapanoğlu, 2019: 3).

Daft, karar vermeyi, sorun çözümü ve çevreden oluşan fırsatları tanımlama süreci olarak belirtmiştir (Tekin, 2009: 8). Eren, karar vermeyi amaca ulaşmak için, alternatif yol ve araçlar arasında tercih yapmakla ilgili zihinsel, bedensel ve duygusal süreçlerin tamamı olarak tanımlamıştır (Demirci, 2012: 3).

Karar, basitçe seçenekler arasından birinin tercih edilmesi olarak tanımlanabilir. Yönetmel karar verme ise yapılan tercihin bilinçli ve akılcı olarak yapılmasıdır. Akılcı karar verme yönetmel amaçlar için seçeneklerin belirlenmesi, seçeneklerin başarı ölçütlerine göre değerlendirilmesi ve her bir seçeneğin faydalarının dikkate alınarak uygun seçeneğin tespit edilmesi süreçlerinden oluşmaktadır. Bilinçli karar verme ise karara, karar sürecine veya karar modeline etki edebilecek verilere mümkün olduğu kadar eksiksiz sahip olma durumunu kapsamaktadır (Kapanoğlu, 2019: 4).

Yönetim seviyelerine göre, farklı karar tipleri bulunmaktadır. Bunlar üç ana grupta ele alındığında, Şekil 4.1.'deki gibi yapısal, yarı-yapısal ve yapısal olmayan karar tiplerinden söz edilebilir (Gökçen, Özkil, Yardımoğlu ve Peker, 2010).



Şekil 4.1. Yönetim Seviyelerinde Karar Tipleri (Gökçen ve diğerleri, 2010)

Yapısal kararlar, her gün karşılaşılan problemlerin çözümünde alınan belirlilik düzeyi yüksek olan kararlardır. Karar veren için subjektif alanın olmadığı kararlardır. Yapısal olmayan kararlarda ise problemler için kesin bir belirlilik yoktur ve hiçbir kural çözümü garantileyemez. Karar veren için muhakeme ve sezgisini kullanarak subjektif değerlendirmenin yapıldığı kararlardır. Yarı-yapısal kararlar ise, problem kısmi olarak tanımlı ve belirliken, çözümünde karar vericinin muhakeme ve sezgisine dayanan kararlardır (Gökçen ve diğerleri, 2010).

Karar vericiler, bilişsel kapasitelerine göre kendi zekâ, bilgi, tecrübe, sezgi veya muhakemesine çerçevesinde hareket etmektedirler. Bazı sorunların çözümünde ise kendi bilişsel kapasiteleri yetersiz kalabilmektedir. Bu durumda bazı yollara başvurulabilmektedir. Bunlar, uygun karar yöntemlerini kullanmak ve bilgi teknolojilerinden yararlanmaktır (Kapanoğlu, 2019: 7).

İlk olarak J.D. Little'ın çalışmasıyla ortaya konan karar destek sistemi, karar vermenin kolaylaştırılması ve daha etkili hale getirilmesi için tasarlanan model, benzetim ve uygulamaları içinde bulunduran sistemlerdir (Marakas, 1999: 7).

Long, Karar Destek Sistemleri'ni, "karar verme sürecinde yönetime destek vermek için hedeflenen bilginin üretilmesi ve sunulması için kullanıcı etkileşimli yazılım ve donanım vasıtalarının bütünleşik kümesinden oluşan interaktif bilgi sistemleri" şeklinde tanımlamıştır (Demirci, 2012: 7).

Turban ise KDS'yi, özellikle yapısal olmayan problemlere çözüm üretilmesi için etkin karar vermelerini destekleyen interaktif, esnek ve adaptif bilgisayar destekli bilişim sistemleri şeklinde tanımlamıştır (Turban, 1995: 110).

Demirci ise “KDS tek başına karar vermeyen, karar vericiye muhakeme yeteneğini de kullanarak doğru ve etkin karar vermesini sağlayan, yarı-yapısal ve yapısal olmayan kararlarda destek olan, karar vericinin ihtiyaç duyduğu bilgiyi doğru zamanda minimum maliyetle sunan etkileşimli sistemlerdir.” şeklinde tanımlamıştır (Demirci, 2012: 8).

Haag ve diğerleri karar destek sistemleri için “kararın yapısal olmadığı durumlarda (doğru cevabı bilmenin mutlak bir yolunun olmadığı ve ortada birçok doğru karar bulunabildiği durumlarda) karar alma işlemine yardımcı olmak için tasarlanmış, esnek ve etkileşimli bilgi teknolojisi sistemleridir” tanımında bulunmuşlardır (Bilgen, 2011: 71).

Güvenç, “Karar destek sistemleri genel olarak karar verici uzman kişilerin kararlarını vermede daha etkin ve verimli olmalarını sağlamak amacıyla geliştirilmiş olan bilgisayar destekli araçlar veya yazılımlar” olarak tanımlamıştır (Güvenç, 2018: 13).

Karar Destek Sistemleri, karar vericilerin yarı-yapısal ve yapısal olmayan veri ve modellerinden yararlanmalarına yardım ederek, görevlerinde destekleyen bilgisayar temelinde etkileşimli bir sistemdir (Çil, 2002).

Zhou ve diğerleri ise karar destek sistemlerini, insanın karar verme sürecine dâhil olan ve destekleyen bir bilgi sistemi olduğunu belirtmişlerdir (Zhou, Yang, Li ve Chen, 2008).

Gökçen' göre KDS alınması gereken kararlar için verinin daha iyi anlaşılması sayesinde, daha etkili karar seçenekleri oluşturulması, alternatiflerin belirlenmesi ve değerlendirilmesi işlevlerinde destek sağlamaktadır. Bu sayede karar verme konusunda verilen kararların daha doğru olma olasılığını artıran sistemler olduğunu ve karar verme sürecinde destek sağlayan ancak hiçbir zaman karar verenin yerini almayan bilgi sistemi olduğunu belirtmiştir (Bilgen, 2011: 71-72).

Günümüzde evrensel bir karar destek sistemi tanımı olmadığını söyleyen Kapanoğlu, karar destek sistemlerini “bir kararın kalitesini arttırmak üzere geliştirilmiş, bir karar veya karar

vericiye ve onun beklentilerine göre yapılandırılmış bilgi sistemleri” şeklinde belirtmiştir (Kapanoğlu, 2019:7).

Karar verme sürecinin evrimi, Arslan ve Yılmaz tarafından geçmişte en büyük problem bilgi toplamak iken, günümüzde ise toplanan verilerden anlamlı sonuçların çıkarılması olarak değiştiği şeklinde dile getirilmiştir. Bu problemin çözümü için toplanan veri yığınlarından ihtiyaç duyulan bilgiler çıkartılmalı ve veriler arasındaki desenleri ve örüntüleri gösterecek sisteme ihtiyaç duyulmaktadır (Arslan ve Yılmaz, 2010).

“Karar Destek Sisteminde; ‘Karar’ kelimesi, problem çözmeyi ifade eder. ‘Destek’, karar verme sürecinde, bilgisayar ve yazılım teknolojileri kullanımıyla karar vericilerin desteklenmesini ifade eder. ‘Sistem’ ise insan-makine arasındaki etkileşim ve bunun dizayn ve tanımlanmasını ifade etmektedir.” (Bilgen, 2011: 74).

Karar Destek Sistemlerinin amacı çözümü yöntemsel açıdan belli olmayan, risk barındıran ve karmaşık kararlarda yöneticilere yardımcı olmaktır. Bu sistemler kişinin yerine geçip karar vermezler, sadece karar vermeyi kolaylaştırırlar (Akıncı, 2006: 32).

Artan bilginin idaresi ve kalite için bilgi sistemleri işletmelere yardımcı olmaktadır, bilgisayar teknolojilerindeki gelişmeler karar destek sistemlerinin gelişimine katkı sağlamıştır (Alexouda, 2005).

4.1. Karar Destek Sisteminin Özellikleri

Karar Destek Sistemleri, kullanıcının karar verme süreçlerine ne kadar dâhil oluyorsa o kadar faydalıdır. Karar Destek Sistemlerinin özellikleri, bu sistemin öneminin ve niteliğinin anlaşılması için önem arz etmektedir.

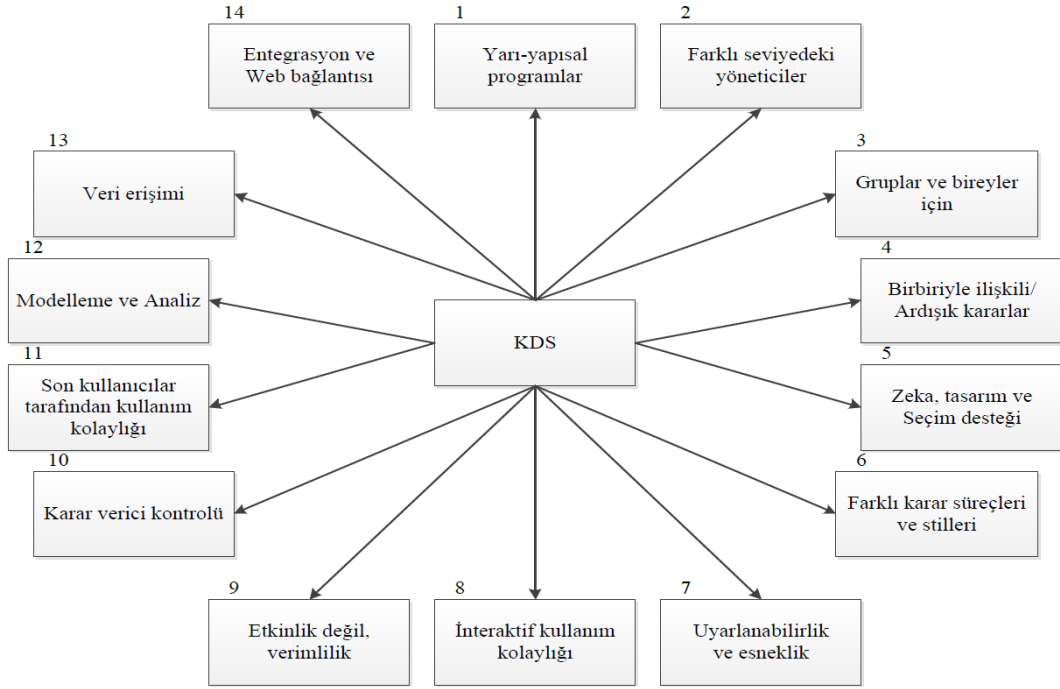
Çelik, karar destek sisteminin kullanılmasının kullanılmamasına göre avantajlarını şu şekilde sıralamıştır (Çelik, 2006: 54):

- Daha yüksek oranda karlılık sağladığı,
- Karlılığın zaman içindeki değişkenliğinin daha az olduğu,
- Karar verme süresinin kısaldığı,
- Daha çok sayıda alternatifin incelendiği,

- Kararların gerekçelenme imkânı olduğudur.

Turban ve Aronson ise ideal bir karar destek sisteminin özelliklerini ve yeteneklerini Şekil 4.2.'deki gibi ifade etmiştir (Demirci, 2012: 9). Bu şekli maddeler halinde sıralarsak:

- Karar Destek Sistemleri, standart bilgisayar yöntemleriyle çözülemeyen yarı-yapısal ve yapısal olmayan durumlarda uygulanır.
- Bu sistem, en alt düzeyden en üst düzeydeki karar vericiler için kullanılabilir.
- Hem gruplar hem de bireyler tarafından alınması gereken kararlarda, karar verme desteği sağlar.
- Birbiriyle ilişkisi olan ve ardışık kararlarda da kullanılabilir.
- Karar Destek Sistemi, karar verme sürecinin zekâ, tasarım, seçim desteği gibi tüm aşamalarında destek sağlar.
- Farklı karar verme süreçlerini ve farklı karar verme stillerini destekler.
- Karar Destek Sistemleri, hızla değişen koşullara uyum sağlaması için karar verici tarafından uyarlanabilir.
- Karar Destek Sistemleri esnektir. Bu sayede temel unsurları tekrar düzenleme, silme, ekleme veya birleştirme imkanı sunmaktadır.
- Karar Destek Sistemlerin amacı maliyeti indirmekten ziyade, verimliliği artırmaya yöneliktir.
- Karar Destek Sisteminin kullanıcısı, karar verme süreçlerindeki tüm adımlarda tam kontrole sahiptir. Karar Destek Sisteminin amacı kullanıcının yerine geçmek değil, onu karar verme aşamasında desteklemektir.
- Karar Destek Sistemleri gerektiğinde dayandığı karışık sistem mimarisinin üzerinde son kullanıcı için kullanımı kolay arayüz barındırır.
- Karar verme durumlarının analizi için modellerden yararlanarak, farklı yapılar altında farklı tecrübeler sağlamaktadır.
- Karar Destek Sistemleri, sistemin işlemesi için toplanan verilere erişerek bunlardan çıkarımlar yapılmasını sağlar.
- Karar Destek Sistemleri, erişim kolaylığının sağlanması ve daha geniş alanlarda kullanılması için entegre edilebilir ve internet bağlantısı kullanılabilir.



Şekil 4.2. Turban ve Aronson’a göre ideal bir karar destek sisteminin özellikleri ve yetenekleri

Haag ve diğerleri ise karar destek sistemlerinin genel özelliklerini yedi madde halinde sıralamıştır (Bilgen, 2011: 74).

- Yarı-yapısal ve yapısal olmayan kararlarda kullanım,
- Karar vericinin yerini alma değil, karar verme konusunda destek,
- Karar verme sürecindeki tüm aşamalarda destek,
- Kontrol karar vericide,
- Model kullanımı,
- Etkileşimin kullanıcı tarafından gerçekleşmesi,
- Kullanıcı için kolaylık ve esneklik.

4.2.Karar Destek Sistemi Türleri

Karar Destek Sistemleri, karar vericiye karar vermesi sürecinde yardımcı olmak için karar vericinin muhakemesinin yanında analitik modelleri, veri tabanlarını, modelleme sürecini kullanır. Bu temeller ışığında Karar Destek Sistemlerini beş farklı şekilde sınıflandırılması mümkündür (Power, 2002: 13-16).

1. Model Tabanlı Karar Destek Sistemi
2. Veri Tabanlı Karar Destek Sistemi
3. Bilgi Tabanlı Karar Destek Sistemi
4. İletişim Tabanlı Karar Destek Sistemi
5. Doküman Tabanlı Karar Destek Sistemi

4.2.1. Model tabanlı karar destek sistemi

Model tabanlı karar destek sistemi (model-driven decision support system) ilk geliştirilen karar destek sistemidir. Merkezi bir sisteme bağlı olmayan, son kullanıcı tarafından kullanılan ve geliştirilen bu sistemin, kullanımını kolaylaştıran bir arayüzle analiz yetenekleri artırılabilir (Bilgen, 2011: 81-82).

Model tabanlı karar destek sistemleri, büyük ve karmaşık optimizasyon ve benzetim modellerin kurulmasını, kurulan bu modellerin çözülmesi, duyarlılık analizi ile birlikte çeşitli senaryo analizlerini içermektedir. Büyük ve karmaşık problemlerin bir model aracılığı ile görselleştirilmesi dahi karar destek sistemi için önemlidir (Kapanoğlu, 2019: 17).

Bu sistem için kullanıcı grubu yöneticiler ve çalışanlar ile dışarıda var olan güncel müşterilerdir. Genel amacı ekibin planlanması olabilirken, özel amacı ise karar verilmesidir. Bu şekilde oluşturulan bir sistemin çalışması için tek bir bilgisayar (stand-alone PC) yeterlidir (Power, 2002: 16).

4.2.2. Veri tabanlı karar destek sistemi

Büyük çaplı sistemlerde bulunan veri ambarını analiz eden sistemlerdir. Bu sistemler, daha önceden büyük miktarlardaki verilerde ihtiyaç duyulan bilgilerin çıkarılmasını sağlayarak, kullanıcılara karar verme desteği sunmaktadır. Elde edilen veriler genellikle sistemin veri tabanında tutulmaktadır (Bilgen, 2011: 82).

Veri tabanlı karar destek sistemi, karar vericiye gerekli bilginin sunulması için veri ve bilgi işleme özelliklerine sahiptir. Veri madenciliği yazılımları bu karar destek sistemi altında yer almaktadır. Raporlama ve sorgulama yetenekleri veri tabanlı karar destek sistemlerinde güçlüdür (Kapanoğlu, 2019: 16).

Bu sistem için kullanıcı grubu içeride yöneticiler ve çalışanlar iken, dışarıda tedarikçilerdir. Amacı veri sorgulaması yapmak ve veri depolamak olan bu sistemin çalışması için gereken mimari, sunucu ve istemci ile ağ yapısından oluşmaktadır (Power, 2002: 13).

80'li yılların sonunda Frito-Lay yöneticileri, satış süreçlerini yeniden tasarlamak için ülke genelinde satış verilerini toplayarak şirketin Texas'taki merkezinde veri tabanlı karar destek sistemiyle işledi. Kullanılan bu teknoloji hantal olan süreci otomatikleştirdi ve hali hazırda toplanmakta olan verilerin kalitesini iyileştirdi. Ayrıca merkezi kontrol sistemleri korunurken merkezi olmayan karar verme süreçlerini desteklediği gözlemlendi (Power, 2002: 27).

4.2.3. Bilgi tabanlı karar destek sistemi

Bilgen, bilgi tabanlı karar destek sistemini tanımlarken “Bu sistemler uzman bir insanın yaptığı gibi, kullanıcıya birtakım sorular sorarak görüş alışverişi yapar ve gerekli bilgileri elde eder. Probleme ait tavsiyelerde bulunur ve görüş alışverişi sonunda karar verebilir. Ayrıca karara nasıl ulaştığını açıklayabilir. Bilgi tabanlı sistemler, iş ortamındaki talepten doğmuştur.” şeklinde niteliklerini vurgulamıştır (Bilgen, 2011: 82-84).

Bilgi tabanlı karar destek sistemlerinde Bilgi Tabanı olarak adlandırılan Bilgi Modülü ve Arayüz Motoru olarak adlandırılan Kontrol Modülü olmak üzere iki adet modül bulunur. Biraz daha karmaşık sistemlerde arayüz motoru kullanılacak bilginin metadatasını içerebilir (Hopgood, 2016: 3).

Bilgi tabanlı karar destek sistemiyle, analitik modelleme ile nitelikli bilginin bütünleşmesi hedeflenmiştir. Bu sayede kararların kalitesinin artırılması ve sistemin uygulama alanlarının genişletilmesi amaçlanmıştır (Bilgen, 2011: 82-84).

Bu sistem dâhili kullanıcılar ile müşteriler tarafından kullanılabilir. Amacı yönetime ilişkin tavsiyeler ve ürünün seçimidir. Bu sistem için gereken bileşenler, sunucu ve istemci ile ağ yapısıdır (Power, 2002: 13).

“Birçok yapılandırılmamış ve yarı yapılandırılmış sorunlar için çözümleri akıllı bir sistem gerektirecek kadar karmaşık olabilir. Gelişmiş KDS sistemleri alt bileşenleri bilgi tabanlı alt sistem olarak devreye girer. Bilgi tabanlı bileşenleri yapay sinir ağları, akıllı casuslar,

hatalı mantık, bilgisayar tabanlı vb. bilgi tabanları birçok bileşenlerden oluşmaktadır. Bilgi tabanlı KDS için kullanılan araçlara akıllı KDS denir.” (Uyanık, 2016)

Özetle bilgi tabanlı karar destek sistemi, verinin anlamlı hali olan bilgiyi kullanarak ve analiz ederek kullanıcıyı nitelikli şekilde yönlendirerek problemlerin çözümüne kaliteli katkı sağlayan sistemlerdir diyebiliriz.

4.2.4. İletişim tabanlı karar destek sistemi

İnsan grupları arasında iletişim imkânı sağlayan iletişim tabanlı karar destek sistemi bu sayede bilgi paylaşımını kolaylaştırır. İnsanlar arasında iş birliğini destekler. Bu sistemdeki kullanıcı arabirimi; koordinasyon, grup içi iletişim, bağımlı destek, paylaşılan bilgi, kullanıcı başvuruları ile oluşmuş açık bir çevreden oluşmaktadır (Çelik, 2006: 66).

İletişim tabanlı karar destek sistemleri insan grupları arasında bilgi paylaşımı, iş birliği ve koordinasyonu sağlamaktadır. Paylaşılan bilgi ile kullanıcı, kullanıcı arabirimi, destek, grup içi iletişim ile birleşmiş sistemden meydana gelmektedir (Uyanık, 2016).

İletişim tabanlı karar destek sistemleri, grup çalışmaları için iş birliğini ve iletişimi sağlamak amacıyla geliştirilmiştir. Kurumsal dayanışmayı güçlendirmek için oluşturulan karar destek sistemleri, iletişim tabanlı karar destek sistemi olarak kabul edilmektedir (Kapanoğlu, 2019: 16).

İletişim tabanlı karar destek sisteminin kullanıcı grupları içerideki takımlardan oluşmaktadır. Kullanım amacı ise, toplantı düzenleme, kullanıcıların iş birliği, ilan tahtası olabilir. Bu sistem için gereken bileşenler, sunucu ve istemci ile ağ yapısıdır (Power, 2002: 14).

4.2.5. Doküman tabanlı karar destek sistemi

Bilginin depolandığı veri bileşenlerinin bir araya getirildiği yönetme ve belge niteliğindeki bu veriye erişim sağlayan sisteme belge tabanlı ya da doküman tabanlı karar destek sistemi denilmektedir (Uyanık, 2016). Bu sistem için gereken dokümanlar pek çok formda olabilir; ancak temel olarak yazılı, görsel ve seslendirilmiş olmak üzere üç farklı gruba ayrılması mümkündür (Çelik, 2006: 67).

Yazılı dokümanlar, mektup, e-posta yazışmalar olabilirken görsel dokümanlar, reklam filmi, video kayıtları, resimler olabilir. Sesilendirilmiş olan dokümanlar ise görüşmelere ilişkin sesli kayıtlar olabilir.

Sistemin işlemesi için belirli bir standartta olmayan dokümanlar, belirli bir formata çevrilir. Bu çevirme işleminde yazılımlar kullanılmaktadır. Bu sayede karar vermesi gereken yöneticiler karşılaştırma yapabilirler (Bilgen, 2011: 85).

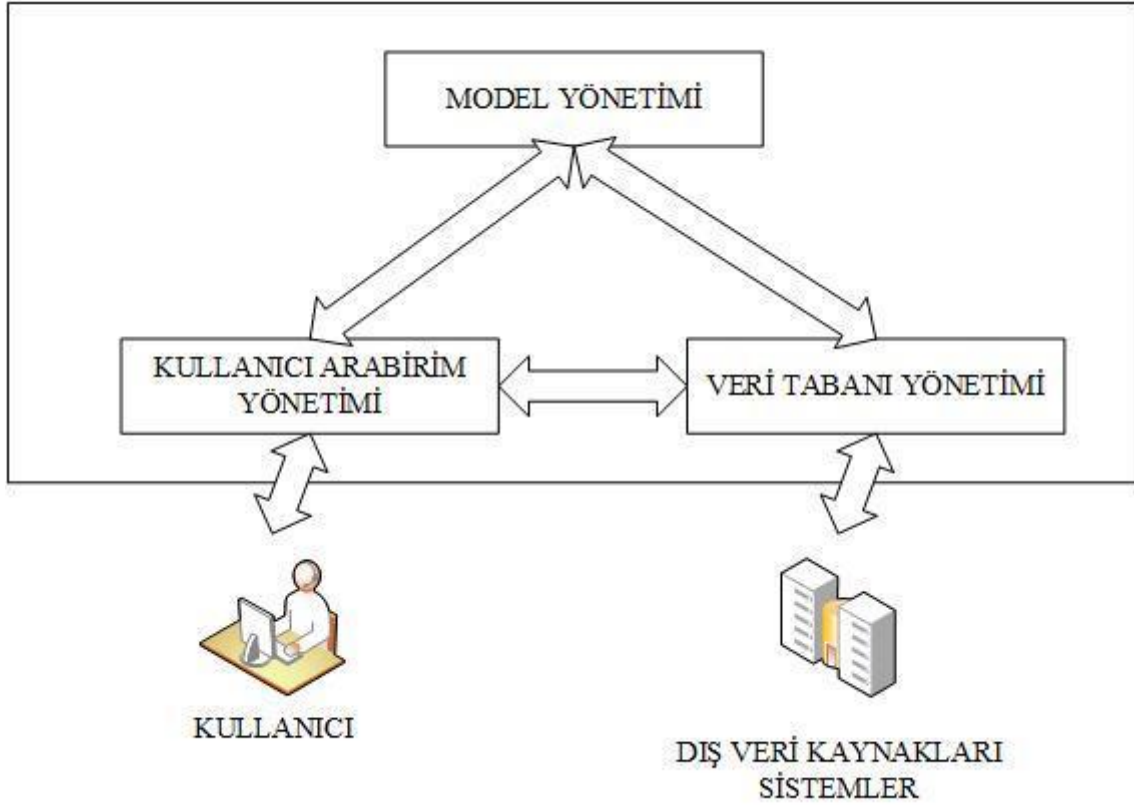
Bu sistem uzmanlar ve genişlemekte olan kullanıcı grupları tarafından kullanılmaktadır. İnternet sitelerinde arama yapma ve doküman bulmak için kullanılan bu sistemlerin çalışması için internet bağlantısı gerekmektedir (Power, 2002: 16).

4.3. Karar Destek Sistemi Oluşturma

Karar Destek Sistemi oluşturulmadan önce, hangi amaçla hazırlanacağı ve nasıl bir sistemle problemin çözüleceği belirlenmesi gerekmektedir. Sistemin başarısı için sistemi oluşturma işlemi belirli aşamalara ayrılmalı ve bu aşamalar sırayla, eğer gerekiyorsa eş zamanlı olarak gerçekleştirilmelidir.

Karar destek sistemi üç temel bileşenden oluşmaktadır: veri, model ve kullanıcı arayüzü (Koç, 2013: 14; Prytherch, 2005: 199; Uyanık, 2016). Bazı kaynaklarda ise bunlara ilave olarak bilgi/bilgi tabanı gibi dördüncü bir bileşenden de bahsedilmektedir (Noor ve Mohamed, 2010) (Gökçen ve diğerleri, 2010). Bunların yanında bu bileşenleri birbirine bağlayan, iletişim kurulmasını sağlayan ağ yapısı da sayılabilir (Power, 2007).

En özet haliyle bir Karar Destek Sistemi, model yönetimi, kullanıcı arabirim yönetimi ve veri tabanı yönetimi süreçlerini içermektedir. Şekil 4.3.'te karar destek sisteminin temel bileşenleri belirtilmiştir.



Şekil 4.3. Karar destek sistemleri temel bileşenleri (Uyanık, 2016)

4.3.1. Model yönetim modülü

Model yönetim modülü, karar vericinin kullanması amacıyla bir karar destek sisteminde yer alan analitik, benzetim ve optimizasyon araçlarını sunan modüldür. Model ile gerçeğin önemsiz ve gereksiz ayrıntılarından arındırılmış halinin, gerçeği yansıtma özelliği korunarak basitleştirilmiş gösterimi ifade edilmektedir. Bir model yönetim modülünde model tabanı, model dizini, model tabanı yönetimi ile model çözme ve yürütme olmak üzere dört adet bileşen bulunmaktadır (Kapanoğlu, 2019: 12-14).

4.3.2. Veri yönetim modülü

Veri yönetim modülünde, karar destek sistemi tarafından kullanılacak olan model ve algoritmalar için kullanılacak verilerin temin edilmekte ve hesaplamalar yapılmaktadır. (Kapanoğlu, 2019: 14). Sahip olunan bilgi arttıkça, daha zengin bir veri tabanına erişim mümkün olmaktadır. Bu modül üzerinde veriler tutulmakta, erişilmekte ve sorgulamalar yapılmaktadır.

Bir karar destek sistemindeki veri yönetim modülü temelde dört bileşenden oluşmaktadır (Kapanoğlu, 2019: 14-15):

- Karar destek sistemi veri tabanı
- Karar destek sistemi veri tabanı yönetim sistemi
- Karar destek sistemi veri dizini
- Karar destek sistemi sorgulama bileşeni

4.3.3. Kullanıcı arayüz modülü

Kullanıcı arayüz modülünün, kullanıcıyla doğrudan etkileşiminden dolayı en önemli modül olarak kabul edilmesi mümkündür. Bu modül, karar vericinin teknolojik ayrıntılardan ziyade sorunun çözümüyle ilgili düşünme, analiz, öğrenme ve sonuç olarak karara odaklanmasını sağlamaktadır. Karar verici, kullanıcı arayüz modülü sayesinde veri yönetim modülü ve model yönetim modülü ile etkileşime girebilmektedir (Kapanoğlu, 2019: 15).

Karar vericinin sisteme erişimindeki penceresi olan bu modül, oldukça önemlidir. Bu öneminden dolayı, tasarımına da özen gösterilmesi gerekmektedir. Tasarım aşamasında görsellikle birlikte, kullanım kolaylığı ve sistemin anlaşılabilirliği gibi bazı ölçütlere dikkat edilmesi gerekmektedir.

Karar destek sistemi oluşturulurken ilk olarak, ihtiyaçların tanımının yapılması gerekmektedir (Uyanık, 2016). Karar destek sistemi oluşturulurken hangi sorunun çözülmesi gerektiği belirlenmelidir.

Daha sonrasında kararların verilmesine etki eden girdilerin belirlenmesi gerekmektedir. Bu veriler iç veriler olabileceği gibi dış veriler de olabilir. Bu veriler, hali hazırda yürüyen işleyişten elde edilen veriler, iş akış şemaları ya da konuyla ilgili genel manada kabul gören kurallar olabilir.

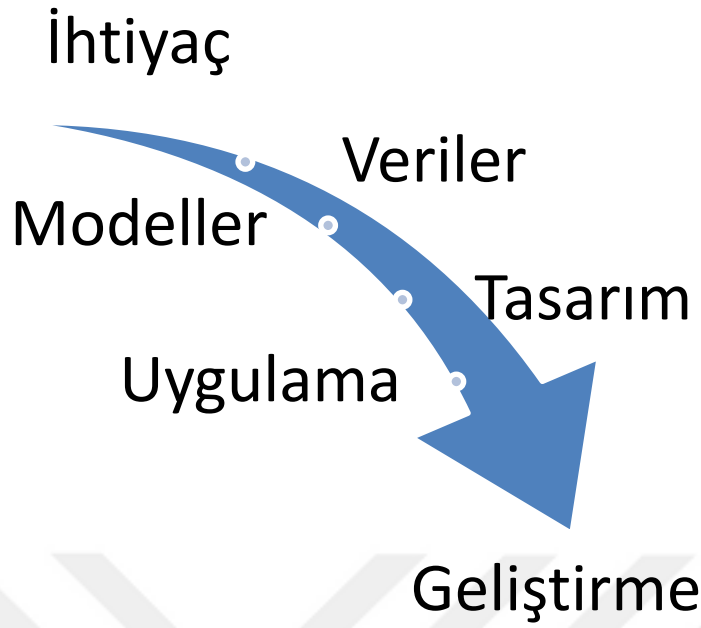
Diğer aşamada bu veriler ışığında modellerin oluşturulması gerekmektedir. Veriler analiz edilerek modeller planlanır. Bunlar problemin yapısına uygun karar modelleridir (Bilgen, 2011: 90). Bu modeller ile tasarım aşamasına geçilebilir.

Tasarım aşamasıyla, ihtiyaçlar ve modeller ile ulaşılmak istenen çözüm bir arada değerlendirilir. Belirlenen amaçlar operasyonel özelliklerine göre düzenlenmektedir (Bilgen, 2011: 80). En önemli adımlar, teknik mimari tasarımı ve sistem model tasarımıdır (Uyanık, 2016). Bu aşamada üç bileşen olan veri tabanı yönetimi, model yönetimi ve kullanıcı arayüz yönetimi tasarlanmalıdır. Tasarım aşamasının öncelikli amacı, öngörülen sistemin nasıl işleneceğine ilişkin teknik planın kurulmasıdır (Uyanık, 2016). Sistemin başarısı, model ile verilerin yazılım dili aracılığıyla uyum içinde karar destek sistemini desteklemesine bağlıdır. Sistemin tutarlılığı için testlere tabi tutulması gerekmektedir (Tokaylı, 2005: 15).

Uygulama aşamasında, tasarlanan sistem kullanıcılara sunulmaktadır. Burada etkileşimin nasıl kurulacağı büyük önem arz etmektedir (Bilgen, 2011: 80). Stand-alone bilgisayar veya sunucular veya web servisleri gibi hangi donanımlar ile çalışılacaksa sistemin bunlara kurulması da bu kapsamdadır. Kurulum aşaması esnasında, kullanıcıların eğitilmesi, sistemi benimsemesi ve bunun kendilerine fayda sağlayacağına inanması Karar Destek Sisteminin başarısı için elzemdir. Bu aşamada yapılması gereken başlıca faaliyetler: işlevsellik testi, modüllerin bütünleşmesi, programların kullanımı, kullanıcılara eğitim ve belge verilmesidir (Atak, 2003).

Son aşama ise geliştirme aşamasıdır. Karar Destek Sistemleri yapısı gereği gelişime açıktır (Bilgen, 2011: 80). Yapının kullanıcıların isteklerine, gelişen teknolojiye, değişen organizasyon ve iş yapısına veya yeni oluşan ihtiyaçlara göre gelişmesi mümkündür. Gelişmenin gerçekleşebilmesi için bileşenlerin tam oturması gerekmektedir. Bu bileşenler, düzenlemelerin tanımlanması, bu düzenleme için sistemin değişmesi ve yapılan düzenlemenin test edilmesidir (Tokaylı, 2005: 16). Geliştirme aşamasının avantajları, isteklerin belirlenmesi, katılımın artması ve Karar Destek Sisteminin gelişim hızının artması olarak sayılması mümkündür (Uyanık, 2016).

Sonuç olarak Karar Destek Sisteminin oluşturulması için gereken adımlar, ihtiyaç, veriler, modeller, tasarım, uygulama ve geliştirme olarak Şekil 4.4.'te gösterilmiştir.

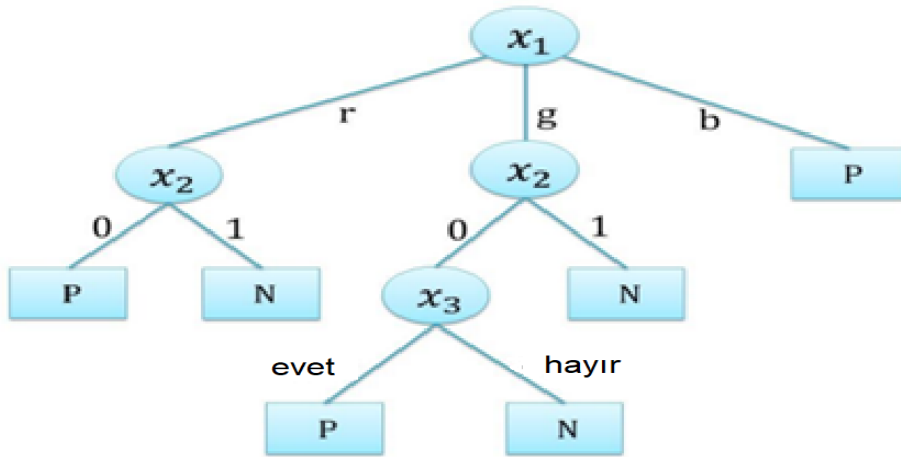


Şekil 4.4. Karar destek sistemi oluşturulması adımları

4.4. Karar Ağacı (Decision Tree) Algoritması

Karar ağacı (decision tree) algoritması adından da anlaşılacağı üzere, ağaca benzer şekilde karar verme modelinden almaktadır. Bu algoritma, girdi verisini ardışık bölümlere işlemiyle sınıflandırma problemini çözmeyi amaçlamaktadır (Avşar, 2015: 62). Karar ağacı algoritmaları, insanlar tarafından anlaşılması daha kolay algoritmalardır (Kabari ve Nwachukwu, 2013). Ağaç yapılarının oluşturulmasında kullanılan kuralların sade ve kolay anlaşılabilir nitelikte olmasından dolayı yaygın olarak kullanılmaktadır (Kavzoğlu ve Çölkesen, 2010).

Temelde bir karar ağacında iki farklı düğüm bulunmaktadır. Bunlar iç düğümler (internal nodes) ve uç düğümler (terminal nodes) şeklindedir. Kök düğümü (root node) de bir iç düğüm türüdür (Sui, 2013: 8). Bir karar ağacı modelinde kök düğümü en üstteki yapıyı ifade ederken; en alttaki yapılar yaprak düğümü (leaf node) olarak adlandırılmaktadır. Bunların arasında kalan düğümlere ise karar düğümü (decision node) denilmektedir (Alpaydın, 2010: 185). Bir karar ağacının alt bölümlerine alt ağaç (sub-tree) denilmekteyken; fazla dallanmayı önlemek için bazı dalların iptali işlemine budama (pruning) denilmektedir. Bir karar ağacı yapısı örneği Şekil 4.5'te gösterilmiştir (Sui, 2013: 8).



Şekil 4.5. Bir karar ağacı yapısı (Sui, 2013)

Bu model içerisinde yapraklar, sınıfları göstermekteyken; her bir düğüm karar testlerini göstermektedir. Yeni bir örnek ile karşılaşıldığında, sınıflandırma işlemi en tepede bulunan kök düğümünden başlanmaktadır. Sonrasında ise model üzerindeki bir yaprak düğümüne ulaşıncaya kadar alt düğümler ile karar testleri sürdürülmektedir (Avşar, 2015: 61).

Karar ağacı sınıflandırmasının gerçekleştirilmesi için çok aşamalı ve ardışık bir süreç izlenmektedir. Bu yöntem sayesinde çok karışık bir sınıflandırma problemi dahi aşamalı hale getirilerek bir karar verme işlemi gerçekleştirilebilmektedir (Safavian ve Landgrebe, 1991).

Eğitimde kullanılan verilerin özneteliklerinden faydalanılarak karar ağacı modeli oluşturulmasındaki temel prensip, verilere bazı sorular sorularak en kısa sürede sonuca gidilmesidir. Bu sayede bu sorulara aldığı cevaplar neticesinde karar ağacı meydana gelmektedir (Pal ve Mather, 2003).

Karar ağaçları, verileri yineleyerek bölümleyen, hiyerarşik, sıralı yapılarla verilerin kurallı olarak temsil etmenin bir yoludur (Murthy, Kasif ve Salzberg, 1994). Karar ağacı modelinde ortaya çıkan hiyerarşik yapı kendi mantığımıza çok benzemektedir. Bu yüzden karar ağaçları, diğer makine öğrenimi sınıflandırıcılarına göre daha kolay yorumlanabilmektedir. Çizelge 4.1'teki veri setinin anlaşılabilirliği, Şekil 4.5'te daha kolay olduğu görülmektedir (Sui, 2013: 9).

Çizelge 4.1 Veri seti örneği

X_1 (r, g, b)	X_2 (1, 0)	X_3 (Evet, Hayır)	Sınıf (Pozitif, Negatif)
r	1	evet	Negatif
r	0	evet	Pozitif
r	1	hayır	Negatif
r	0	hayır	Pozitif
g	1	evet	Negatif
g	0	evet	Pozitif
g	1	hayır	Negatif
g	0	hayır	Negatif
b	1	evet	Pozitif
b	0	evet	Pozitif
b	1	hayır	Pozitif
b	0	hayır	Pozitif

Bir veri seti için birden fazla karar ağacı algoritması geçerli olabilir. Farklı algoritmaların birbirine karşı başarı oranları da farklılık gösterebileceğinden, yüksek başarıya sahip olan algoritmanın seçilmesi gerekmektedir. En bilinen karar ağacı algoritmalarından biri Breiman ve ark. tarafından 1984 yılında yayınlanan “Classification and Regression Trees” adlı kitapta geçen CART algoritmasıdır. Bu çalışma istatistik biliminde CART yönteminin gelişmesine önemli katkı sağlamıştır (Saraç, 2020: 9). Karar ağacı konusunda bir diğer öneri ise 1986 yılında Quinlan tarafından gerçekleştirilen ID3 algoritmasıdır. Yine Quinlan 1993 yılında ise ID3 algoritmasını geliştirerek C4.5 adlı karar ağacı algoritmasını “Programs for Machine Learning” adlı kitabında tanıtmıştır (Witten, Frank, ve Hall, 2011: 144).

En bilinen karar ağacı algoritmaları olan CART, CHAID, ID3 ve C4.5 algoritmalarının farkları kısaca özetlenecek olursa:

- CART (Classification and Regression Trees) algoritması öznitelik seçim ölçütü olarak Gini Indexini kullanmaktadır (Tangirala, 2020).
- CHAID (Chi-squared Automatic Interaction Detector) algoritması CART algoritmasına benzemektedir. Ancak bu algoritma etkili bir şekilde çok yollu frekans tablolarından vazgeçer (Bartra ve Agrawal, 2018).
- ID3 (Iterative Dichotomiser) algoritması öznitelik seçim ölçütü olarak bilgi kazanımını (information gain) kullanmaktadır (Tangirala, 2020).

- C4.5 (J4.8-Successor of ID3) algoritmasında ise öznitelik seçimi olarak kazanç oranı (gain ratio) kullanılmaktadır (Karegowda, Manjunath ve Jayaram, 2010).

Öznitelik seçimi, bir hedef öğrenme problemi açısından ilgili özellikleri seçme sürecidir. Özellik seçiminin amacı, gereksiz ve alakasız özellikleri kaldırmaktır (Sui, 2013: 11). Aynı zamanda hangi özneliğin, farklı seviyeler bulunduran karar ağacının hangi seviyesinde yer alması gerektiği de algoritmalarındaki bazı işlemler neticesinde elde edilmektedir. En çok başvuru alan işlemler, entropy, bilgi kazanımı, gini endeksi ve kazanç oranıdır.

Entropy, veri kümesindeki belirsizlik veya düzensizlik ölçütüdür (Liu ve Cocea, 2018). Yani temel olarak bir düğümdeki saflık, kirlilik ve rastgelelik derecesidir. Verilerin ne kadar rastgele olduğunu bulmak için kullanılır.

Belirsizliğin 'L' olarak ifade edildiği formülde, 'p' bir olayın gerçekleşme ihtimalini, 'i' ise olayın indeksini ifade etmektedir (Eş. 4.1). Sınıflandırma açısından formüldeki entropy, farklı sınıflar arasındaki olasılık dağılımıyla ilgili olan ilk belirsizliğin ifadesinde kullanılabilir. Entropy değerinin sıfır olması bir belirsizlik olmadığı anlamına gelmektedir (Liu ve Cocea, 2018).

$$Entropy(L) = - \sum_{i=1}^j p_i \log_2(p_i) \quad (4.1)$$

Bilgi kazanımı (Information gain), entropy değerine dayanmaktadır. Bilgi kazanımının beklenen değeri, hedef değişken ile bağımsız değişkenin ortak bilgisinden oluşmaktadır. Bu, bağımsız değişkenin durumunun öğrenilmesiyle elde edilen hedef değişkenin entropy değerindeki azalmadır. Bilgi kazanımının en büyük dezavantajı, daha az bilgilendirici olsa bile, daha çok sayıda farklı değerlere sahip öznitelikleri seçme eğilimindedir (Vege, 2012: 11).

Bir karar ağacını oluşturmak için en yüksek bilgi kazanımı ve en küçük entropy değerine ulaşılmasını sağlayan özneliğin belirlenmesi gerekmektedir. Bilgi kazanımı, belirli bir özellik verilen belirsizliğin azaltılma durumunu ölçmektedir. Aynı zamanda karar veya kök

düğüm olarak hangi öz niteliğin seçilmesi gerektiğine karar veren bir ölçüttür (Tangirala, 2020).

Gini endeksini (Gini index), veri kümesindeki bölünmeleri değerlendirmek için kullanılan bir maliyet işlevi olarak tanımlanabilir. Gini endeksi, bölünen sınıfların saflığını belirlemek için kullanılır. Rastgele seçildiğinde yanlış sınıflandırılan belirli bir özelliğin olasılık miktarını hesaplar. Tüm öğeler tek bir sınıfa bağlantılı ise o zaman saf olarak adlandırılır. Gini endeksi 0 ile 1 değerleri arasında değişir. Burada sıfır sınıflandırmanın saflığını ifade eder. Yani tüm değerlerin belirli bir sınıfa ait olduğunu veya sadece bir sınıfın var olduğu anlamına gelmektedir. Değeri 1'e yaklaştıkça çeşitli sınıflar arasında öğelerin rastgele dağılımının arttığını göstermektedir. Karar ağacı tasarlanırken gini endeksi en düşük değere sahip olanı tercih edilir. Gini endeksi, her bir sınıfın olasılıklarının (p_i) karelerinin toplamının birinden çıkarılması ile belirlenir (Eş. 4.2) (Tangirala, 2020).

$$GINI(L) = 1 - \sum_{i=1}^j p_i^2 \quad (4.2)$$

Kazanç oranı (gain ratio) bilgi kazanımı üzerinden hesaplanmaktadır. Bilgi kazanımı, kök düğümler olarak çok sayıda değere sahip öznitelikleri seçmeye yönelik olduğundan dolayı çok sayıda farklı değere sahip özniteliği tercih ettiği anlamına gelmektedir (Shouman, Turner ve Stocker, 2011). Kazanç oranı, bölme yapmadan önce oluşacak düğüm sayısını dikkate alarak bilgi kazanımı sorununu ortadan kaldırır. Bir bölünmenin içsel bilgilerini hesaba katarak bilgi kazanımını düzeltmektedir. Formül Eş.4.3'te gösterilmiştir. (Silipo ve Melcher, 2019).

$$Gain\ Ratio = \frac{Information\ Gain}{SplitInfo} = \frac{Entropy\ (before) - \sum_{j=1}^K Entropy(j, after)}{\sum_{j=1}^K w_j \log_2 w_j} \quad (4.3)$$

5. KALİTE FONKSİYON GÖÇERİMİ

Bu çalışma kapsamında ortaya çıkartılması hedeflenen ürün olan mobil cihaz adlı bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımının geliştirilmesi için bu yazılımı kullanması muhtemel personelin taleplerinin dikkate alınmasının önem arz ettiğine karar verilmiştir. Bunun için ise Kalite Fonksiyon Göçerimi (KFG) uygulaması kullanılmıştır. Bu bölümde KFG için literatürde yapılmış tanımlara ve başta kalite evi olmak üzere KFG aşamalarına yer verilmiştir.

Kalite Fonksiyon Göçerimi (KFG), İkinci Dünya Savaşı sonrası endüstrisini tekrar inşa etmeye çalışan Japonya’da ortaya çıkmıştır. Kavramsal olarak ilk ele alan 1972 yılındaki çalışmasıyla Yoji Akao’dur. Akao, KFG’yi “Müşteri tatminini amaçlayan, müşteri gereksinimlerini tasarım hedefleri haline getirip, bunların en önemli kalite güvenceleri olmasını sağlayan ve bu anlayışın üretimin her noktasında kullanılmasını gerekli kılan, kalite tasarımının geliştirilmesi” şeklinde tanımlamıştır (Yenginol, 2008).

Feigenbaum ise bu kavramı, tam müşteri memnuniyeti için bir organizasyondaki çeşitli grupların kalite-geliştirme, kalite-bakım ve kalite-iyileştirme çabalarını, pazarlama, mühendislik, üretim ve hizmeti mümkün olan en ekonomik düzeyde sağlayacak şekilde bütünleştiren etkili bir sistem olarak tanımlamıştır (Abu-Assab, 2011: 50).

Shillito’ya göre KFG, yeni veya geliştirilmiş ürün veya hizmeti dizayn etmek ve planlamak için başvurulacak bir disiplinler arası bir takım sürecidir. Bu süreçte, müşterilerin ihtiyaçlarına odaklanır, dizayn etme amaçlarını önceliklendirmek için rekabetçi ortamı ve piyasanın potansiyelini kullanır, takım çalışması işlevlerini kullanır ve güçlendirir, anlaşılır ve esnek bir dokümantasyon sağlar ve belli belirsiz müşteri taleplerini ölçülebilir amaçlara çevirir ve bu sayede doğru ürün ve hizmetlerin piyasaya daha hızlı ve doğru sunulmasını sağlar (Shillito, 1994: 2-3).

Müşteri ihtiyaçlarının göz ardı edilmesinin maliyeti, müşterinin ve pazar payının kaybıdır. KFG, ürünün müşteri istek ve ihtiyaçlarını karşılaması için, bu istek ve ihtiyaçların sistemin bütün elemanlarına yayılmasını gerçekleştiren bir süreçtir (Compton, 1999: 263).

Zultner ise KFG’yi, toplam kalite yönetimi (TQM) içinde müşterilerin talep ve ihtiyaçlarını, örgütün tüm işlevsel bileşenlerindeki çıktılarına dönüştürmeye yarayan ve multidisipliner

bir sistem ile yürütülen, anlaşılabilir ve müşteri memnuniyeti odaklı yapısal üretim, planlama ve geliştirme yöntemi olarak açıklamıştır (Zultner, 1993).

KFG, temelde tanımlamayı hedeflediği üç soru vardır. Bunlar (Zairi ve Yousef, 1995):

- Müşterinin kim olduğu,
- Müşterinin ne istediği,
- Müşterinin isteğinin nasıl yerine getirileceğidir.

5.1. Kalite Fonksiyon Göçerimi Faydaları

Yenginol KFG'yi, müşteri istek ve ihtiyaçlarının doğru şekilde tespitiyle pozitif kalitenin elde edilmesi, pozitif ve yeni değerlere ulaşılması ve bunun sayesinde daha fazla müşterinin memnuniyeti için kullanılabilecek en iyi sistem şeklinde tanımlamıştır (Yenginol, 2008).

Bu kadar iddialı bir sistemin, elbette birçok avantajı bulunmaktadır. Kalite Fonksiyon Göçerimi kullanan işletmelerin elde edeceği avantajlar (Han, Chen, Ebrahimpour ve Sodhi, 2001):

- Müşterilerin gerçek gereksinimlerinin tespiti,
- Ürün tasarım ve geliştirme gereksinimlerinin tespiti,
- Yeni ürün geliştirme süreçlerinin etkin planlanması,
- Sürece ilişkin stratejilerin oluşturulması,
- Üretim süreçlerinin kontrolü ve bu sayede kalite ve güvenilirlik artırılması,
- Ürünlerin özellikleriyle ilgili olarak veri tabanının oluşturulmasıdır.

Yıldırım ve Geydir ise KFG faydalarını; müşteri odaklılığı, takım çalışması teşviki, dokümantasyonun sağlaması ile tasarım ve geliştirme zamanını kısaltması olmak üzere dört farklı başlık altında toplamıştır (Çinpolat, 2007: 26):

- Müşteri odaklı: Müşteri ihtiyaçları, istekleri ve beğenilerine yoğunlaşma, kendi ürünlerini rakiplerinin ürünleri ile kıyaslama, geliştirme önceliklerini belirleme ve katılımcıların bilgi ve seviyelerinin ortak kullanımı
- Takım çalışmasını teşvik: Katılım esaslı olması ve birimler arası iletişimi güçlendirme

- Dökümantasyonu sağlama: Tasarım ve geliştirme konusunda müşteri odaklı bir dökümantasyon, dokümantasyonun benimsenmesi, bilgiyi yapılandırma, duyarlılık analizi ve değişikliklere uyum
- Tasarım ve geliştirme süresini kısaltma: Ürünlerde yapılacak değişikliklerin sayısının azalması, satış sonrası problemlerin azalması, gelecek fırsatların tanımlanması, öncelikli geliştirme çabalarına odaklanması ve detaylarla birlikte genel görüş imkanı sağlanması

5.2. Kalite Fonksiyon Göçerimi Aşamaları

Grover, Kalite Fonksiyon Göçerimi uygulamadaki başarısı için sürece ilişkin faaliyetlerin detaylı bir şekilde planlanmasını ve bu sisteme örgütün bir bütün olarak desteğinin vermesi gerektiğini belirtmiştir. Bu sayede bu sürecin gerçekleşmesi için gerekli olan zaman aralığı tespit edilmiş olacaktır. Ayrıca bu sistem içinde görev üstlenecek birimler arasında güçlü bir bilgi alışverişi kurulmuş olacaktır (Yıldız ve Baran, 2011).

Genellikle, Kalite Fonksiyon Göçerimi uygulaması müşteri ihtiyaçları tespit edildikten sonra dört aşamadan oluşmaktadır (Shillito, 1994: 2). Bunlar:

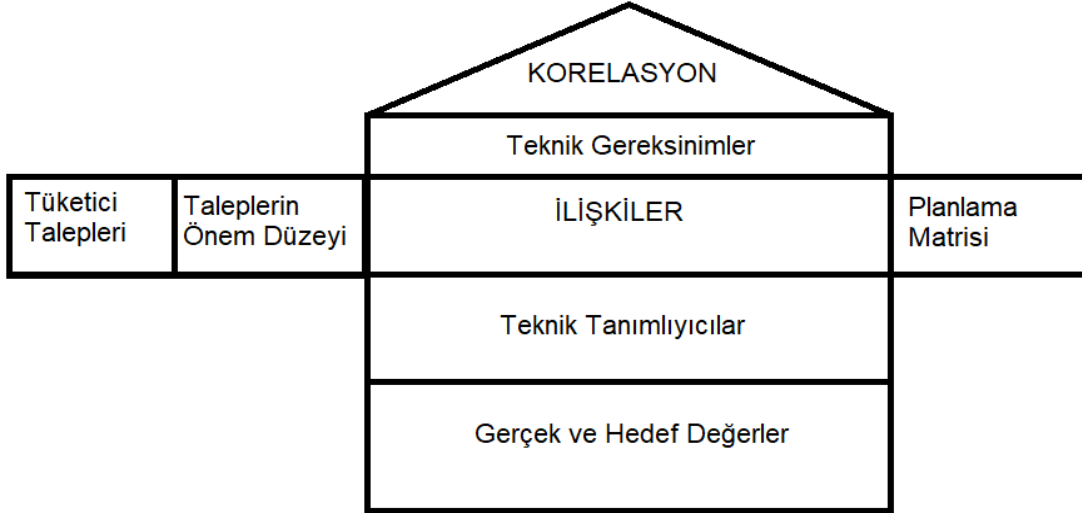
1. Ürün planlaması,
2. Parçanın planlaması,
3. Sürecin planlanması,
4. Üretimin planlanmasıdır.

5.2.1. Kalite evi

Kalite evi kullanılarak, müşteriler için en fazla önem arz eden hususlarda hedeflerin oluşturulması ve bunların teknik açıdan nasıl başarılacağı tespit edilir. Teknik taraf olan mühendisler için temel verilerin ölçülebilir şekilde ele alınmasını sağlarken; satış tarafı olan pazarlamacılar için müşterinin sesini temsil etmekte, bu sayede yeni fırsatların tespitine yardımcı olur (Bouchereau ve Rowlands, 2000).

Kalite evi, Korelasyon ve İlişkiler olmak üzere iki ana bölümden oluşmaktadır. Bunun yanı sıra bunlara bağlı altı alt bölüm bulunmaktadır. Bunlar Tüketici Talepleri, Taleplerin Önem Düzeyi, Teknik Gereksinimler, Teknik Tanımlayıcılar, Gerçek ve Hedef Değerler ve

Planlama Matrisidir (Kathiravan, Devadasan, Michael ve Goyal, 2008). Şekil 5.1.'de gösterilmiştir.



Şekil 5.1. Kalite evi (Kathiravan ve diğerleri, 2008)

Tüketici talepleri

Müşterilerden edinilen bilgiler doğrultusunda yapılandırılmış gereksinimlerdir (Yıldız ve Baran, 2011). Bir şirket için müşterilerin ne düşündüğünü ve neye gerçekten ihtiyaç duyduğunu bilmek, piyasada başarıyı elde etmek için büyük önem taşımaktadır (Gerst, 2004). “Müşterinin sesi” olarak da nitelendirilen taleplerin toplanması için bazı yöntemler mevcuttur. Bunlar anket, e-posta, bireysel veya toplu görüşmeler, beyin fırtınası, gözlem, panel, veri tabanları, müşteri şikâyet ve önerileri gibi farklı şekillerde olabilmektedir (Shillito, 1994: 146).

Tüketici önem düzeyleri

Taleplerin neler olduğu ve bu taleplerin ne kadar önemli olduğunun tespitinde kullanılan matristir. Müşteri taleplerine ait önem dereceleri ile karmaşık problemler için güçlü bir karar verme tekniği ortaya çıkmaktadır. İlişki matrisinde kullanılmak üzere önem derecesine göre 1-9 arasında puanlama yapılmaktadır. Bu ölçeğe göre 9 değeri aşırı derecede önemi; 7 değeri çok kuvvetli derecede önemi, 5 değeri kuvvetli derecede önemi, 3 değeri birinin diğerine göre daha az önemde olmasını ve 1 değeri de eşit önemliyi ifade etmektedir. Geriye kalan 2,4,6 ve 8 değerleri ise ortalama değerler olarak kullanılmaktadır (Wind ve Saaty, 1980).

Teknik gereksinimler

Teknik tarafın tespitlerini içeren kısımdır. Mevcut durumun teknik açıdan değerlendirmesi yapılarak taleplerin karşılanmasına ilişkin ölçütler oluşturulur (Kathiravan ve diğerleri, 2008).

Korelasyon

Korelasyon, kalite evinin çatısını oluşturmaktadır. Korelasyon matrisi çok sık başvurulanan bir yer olarak değerlendirilmese de tasarım mühendisleri açısından önemli bir kısımdır. Bu matriste teknik gereksinimlerin birbiriyle olan pozitif veya negatif ilişkileri tespit edilmektedir (Yıldız ve Baran, 2011). Talepleri karşılanması için teknik gereksinimler arasında olumlu veya olumsuz ilişkiler olabilir. Bu ilişkilerin anlaşılabilmesi için korelasyon matrisi kullanılır. Bunun amacı ihtiyaç duyulması muhtemel incelemeleri ve gelişmeleri tanımlamaktır (Kuru, 1997).

Korelasyon matrisinde ilişki olumsuz ve güçlü ise, KFG ekibinin bu teknik gereksinimlerin geliştirilmesinde özel çaba göstermesi gerektiğini göstermektedir. Aralarındaki olumsuz ilişki bulunan korelasyon durumu “aynı anda birbirine zıt iki fiziksel durumun gerçekleşmesi gerekliliği” şeklinde meydana gelmektedir (Süder, 2003: 59).

Teknik gereksinimlerin arasındaki doğal ilişkinin sonucu olarak bir teknik gereksinimin geliştirilmesi diğer bir teknik gereksinimi doğrudan ya da dolaylı olarak etkileyebilmektedir. Bu etkileme kimi zaman olumlu iken kimi zaman ise olumsuz nitelikte olabilmektedir. KFG matrisi oluşturulduktan sonra bu matrisin analizi sırasında dikkat edilmesi gereken bazı hususlar bulunmaktadır (Yıldırım, 2002: 78).

- KFG matrisi analizi yapılırken boş satır veya sütunun olması verinin eksikliğini göstermektedir.
- Matriste hiçbir talebi etkilemeyen bir teknik gereksinimin varlığı, taleplerden birinin gözden kaçırıldığı ya da ihtiyaç duyulmayan bir teknik gereksinimin tespit edildiği anlamına gelmektedir.
- Matrisin daha kolay anlaşılabilmesi için birbiriyle tamamen ilgisiz hücreler için başka bir sembol kullanılabilir.
- Sağlıklı bir değerlendirme için, talep sayısı ile teknik gereksinim sayısının çok fazla olmaması gerekmektedir.

İlişkiler

Tüketici taleplerinin karşılanması için yapılması gereken teknik gereksinimler belirlendikten sonra, bu teknik gereksinimler ile talepler arasındaki ilişkinin tespitine çalışılmaktadır. Bu çalışmadaki amaç, her bir teknik gereksinimin belirli bir tüketici talebini karşılamadaki etkisini ortaya koymaktır. Bu ilişki belirli semboller ile Kalite evi içerisinde gösterilmektedir (Çinpolat, 2007: 55). İlişki matrisi teknik gereksinimler (nasıllar) ve tüketici talepleri (neler) arasındaki ilişkinin derecesini belirlemektedir (Casamen, Mata ve Mantilla, 2005).

Çizelge 5.1’de gösterildiği gibi ilişki derecesi sayısal olarak puanlarla ve sembollerle gösterilmektedir (Çinpolat, 2007: 56). Güçlü ilişki 9 değeriyle, orta ilişki 3 değeriyle ve zayıf ilişki 1 değeriyle ifade edilmektedir. Bu değerler ile sütun ağırlıkları yani teknik gereksinimin o satırdaki talep için mutlak önem derecesi hesaplanabilmektedir (Sarsılmaz, 1999: 90; Savaş ve Ay, 2005).

Çizelge 5.1. İlişki Sayı ve Anlamları (Çinpolat, 2007)

İlişki Derecesi	Puan Değeri	Sembol
Güçlü ilişki	9	⊖
Orta ilişki	3	O
Zayıf ilişki	1	Δ

Planlama matrisi

Planlama matrisi, piyasa araştırmaları neticesindeki gözlemlenen müşteri algılarını göstermektedir. Bu matriste müşteri taleplerinin görece önemleri ve bu taleplerin karşılanmasındaki performanslar gösterilmektedir (Süder, 2003).

Planlama matrisinde, müşteri şikâyetleri ve rekabete yönelik değerlendirmeler bulunmaktadır. Bu kritik süreçlerin tespiti ile bu süreçlerin planlanması konusunda yol gösterici niteliktedir. Yenginol, planlama matrisindeki “satış noktası” sütunun gelen talepleri karşılamının satışlarda meydana getireceği öngörülen değişimi göstermektedir. Satışlarda önemli bir ilerleme için: 1,5; ilerleme için: 1,2 ve mevcut durum için ise: 1,0 olarak belirlenmektedir. (Yıldız ve Baran, 2011).

Planlama matrisinde bulunan önem derecesi sütunu ise, taleplerin görece önemlerini göstermek için kullanılır. Her bir talep için, önem puanının toplam önem puanlarına bölünmesiyle yüzdelik olarak hesaplanmasıyla elde edilir. Önem puanı, talebin puanı, satış

noktası ve ilerleme noktası değerlerinden elde edilmektedir. Bu değer matriste ağırlık faktörüdür ve yüksek olması öneminin çok olduğunu, düşük olması ise öneminin az olduğuna işaret etmektedir (Özdil ve Dönmez, 2002).

Teknik tanımlayıcılar

Teknik tanımlayıcılar, taleplerin nasıl karşılanacağını belirttiği kısımdır (Özdil ve Dönmez, 2002). Teknik karakteristikler, mühendisler gibi teknik bir ekip tarafından belirlenmektedir (Emiroğlu, 2001: 42). Teknik tanımlayıcıların düzgün oluşturulabilmesi için ölçü birimiyle birlikte bu değerlerin hangi yönde gitmesi ilişkilendirilmelidir. Ölçü birimlerinin tanımlanması sorun olması beklenmese de netlik ve bütünlük açısından KFG matrislerinde yer alması iyi olacaktır (Chan ve Wu, 2002).

Teknik tanımlayıcılar, teknik terminolojiyle ifade edilmektedir. Bu kısımda gerçekleştirilecek olan teknik gereksinimlerin teknik detayları açıklanarak sonraki süreç ve üretim planlama adımlarının temeli oluşturulmaktadır.

Gerçek ve hedef değerler

Sharma ve Rawani'ye göre, bu aşamada ürünün mevcut durumu rekabet açısından değerlendirilmek için teknik detaylarıyla birlikte ele alınır. Ürünlerin özelliklerine göre 1'den 5'e kadar değerlendirilme yapılmaktadır. Aynı şekilde bu talep için hedeflenen değer için de bir değerlendirme yapılarak bunlar kıyaslanmaktadır (Yıldız ve Baran, 2011).

5.2.2. Ürün tasarımı

Ürün tasarımı aşaması, mühendislik birimleri tarafından sürdürülen ve bu aşamada yenilik barındıran fikirlerin geliştirildiği aşamadır. Bu aşamada elde edilen sonuçlar ile hedeflenen ürünün özellikleri belirlenmektedir (Yıldız ve Baran, 2011). Teknik gereksinim aşamasında tespit edilen hususların nasıl gerçekleştirileceğine ilişkin ihtiyaçlar belirlenir ve teknik gereksinimler sütunlarından hangisinin müşteri talebi açısından daha önemli olduğu kararı verilir (Ay, 2003: 78).

Costin, ürün tasarımı aşaması esnasında önceden belirlenen hedef değerlerin müşteri taleplerine uygunluğunun kontrol edilmesi gerektiğini ve karşılaşılan uyumsuzlukların bu aşamadayken giderilmesi gerektiğini belirtmiştir (Yıldız ve Baran, 2011).

5.2.3. Sürecin Planlanması

Süreç planlaması aşamasında bundan önceki iki aşamada belirlenen özellikler, temel süreç operasyonlarına dönüştürülür (Abu-Assab, 2011: 57). Tespit edilen özelliklerden hangisinin yapılacağına dair karar KFG ekibi tarafından verilmelidir. Bu noktada getireceği fayda ile bu çalışma için gereken maliyet kıyaslanarak kararın verilmesi gerekmektedir (Çinpolat, 2007: 57).

Kalite evinde yüksek puana sahip olan süreç parametreleri, müşteri taleplerini karşılamak için daha fazla öneme sahiptir. Bunun belirlenmesi sayesinde geliştirilmesi gereken ürünün hangi aşamasının yeniden tasarlanması gerektiği anlaşılacaktır (Çetin, 2007: 66-67).

5.2.4. Üretimin Planlanması

Üretim planlama aşaması, planlama matrisinde belirlenen hedeflere ulaşmak için bir kontrol listesinin veya detaylı bir üretim sürecinin oluşturulduğu aşamadır. Üretimin planlama adımları ile tüketici talepleri arasındaki ilişkiyi sağlayarak, firmanın tüm işlevlerinin tüketici odaklı olmasını ve talepleri karşılamasını sağlamaktadır (Yıldız ve Baran, 2011).

Bu aşamada süreç planları, iş planlarına dönüştürülür. Yani planlanan süreçlerin aksamadan ve eksiksiz gerçekleşmesini sağlayan bir tür iç denetim mekanizması olarak kabul edilebilir (Ay, 2003: 92).

Kontrol listesinde belirlenen önemli süreç parametrelerini kapsayan bir tablo oluşturulur. Bu tablonun hücrelerinde; açıklamalar, hedef değerler ya da hücreye ilişkin bilgiler bulunur. Bunun sayesinde üretim planlama süreciyle müşterinin sesi bağlantı kurmuş olur (Çetin, 2007: 67-68).

6. YÖNTEM

6.1.Yöntemin Özeti

Mobil cihaz adli bilişimi alanında artan iş yükü hacmi, gelişen teknoloji sebebiyle uygulanacak yöntemin değişmesi ihtiyacı, özellikle mobil cihazlardaki ve bunlar üzerinde çalışan işletim sistemleri çeşitliliğindeki artış, mobil cihaz adli bilişimi alanındaki karşılaşılan problemler haline gelmiştir. Bunun yanı sıra mobil cihaz adli bilişimi uygulayıcıları açısından benzer problem, bir adli bilişim personeli tarafından çözülebilirken, diğer personel tarafından çözülememektedir. Özellikle yeni başlayanlar olmak üzere personelin bu alanda karar alma konusundaki destek ihtiyacı, doğru çözüme ulaşmak için deneme yanılma yöntemlerinin kullanılması sürecinde harcanan emek, zaman ve maliyet konuları sebebiyle böyle bir çalışmaya ihtiyaç duyulmuştur.

Bu çalışma kapsamında mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımının oluşturulması için öncelikle mobil cihaz adli bilişimine ilişkin verilerin toplanması ihtiyacı doğmuştur. Hangi verilerin toplanması gerektiğinin tespiti için mobil cihaz adli bilişimine etki eden faktörlere ilişkin yurt içinde ve yurt dışında bulunan uzmanlarla görüşmeler gerçekleştirilmiştir. Bu veriler cihaza ait bilgiler, cihazın durumuna ilişkin tespitler ve bu cihaza yapılan işlemlerden oluşmaktadır. Verilerin toplanması için verinin toplanacağı kurum olan Emniyet Genel Müdürlüğünden gerekli izinler alınmıştır. Gerekli izinler alındıktan sonra, bir yıl süreyle veriler toplanmıştır.

Mobil cihaz adli bilişiminde imaj alma süreçlerine ilişkin karar destek sistemi yazılımı hazırlanırken, muhtemel son kullanıcıların beklentilerini de karşılayacak bir yazılım olması hedeflenmiştir. Bu amaç doğrultusunda, Kalite Fonksiyon Göçerimi yöntemine başvurulmuştur. Bunun için bu yazılımı kullanması beklenen mobil cihaz inceleme personeliyle görüşmeler gerçekleştirilmiş ve talepleriyle birlikte bu taleplerin onlar için önem düzeyleri alınmıştır. Elde edilen sekiz farklı talebin gerçekleştirilmesi için dokuz farklı teknik gereksinim belirlenmiştir. Daha sonrasında ise bu teknik gereksinimlerin talepler ile ilişkisi, birbirileri arasındaki korelasyon ve teknik önemleri belirlenerek kalite evi oluşturulmuştur. Nihai olarak ortaya çıkan bulguların, yazılıma dâhil edilmesi hedeflenmiştir.

Mobil cihaz adli bilişimine ilişkin toplanan veriler ışığında sınıflandırma algoritmaları WEKA yazılımı ile kıyaslanmıştır. En yüksek doğruluk oranı karar ağacı algoritmasında elde edilmiştir. Çalışmada, doğru sonuçların (True Positive + True Negative) doğru veya yanlış sonuçların toplamına (True Positive + True Negative + False positive + False Negative) oranı olarak hesaplanan doğruluk oranı, başarı oranı olarak kabul edilmiştir. Karar ağacı (decision-tree) algoritmaları üzerinde, çapraz doğrulama (cross-validation) yöntemiyle gerçekleştirilen eğitim ve testler sonucunda %98,83 ile en başarılı sonuç veren ID3 algoritması kullanılarak bir karar destek sistemi oluşturulmuştur. Bunun son kullanıcı tarafından kullanılabilmesi için veri tabanları, yazılım ve arayüz hazırlanmıştır.

Yazılım iki farklı veri tabanından oluşmaktadır. Bunlar toplanan mobil cihaz adli bilişimine ilişkin yapılan işlem verileri ile personelin bu işlemleri yerine getirirken yardımcı olması için internet ortamından elde edilen mobil cihazların teknik özelliklerinden oluşmaktadır. Ayrıca yazılım iki farklı karar ağacı algoritması barındırmaktadır. Bunların ilki arızanın tespiti için cihazın marka model bilgilerine göre sırayla sorular sorarak kullanıcıyı yönlendirmektedir. Diğeri ise arıza tespitinden sonra imaj almak için kullanıcıya hangi yöntemleri izlemesi gerektiğine ilişkin karar ağacı diyagramı sunan algoritmadır. Bunun yanı sıra tecrübeli personel için arıza tespiti durumunda gelişmiş ekran ile yapılan işlemlerin detayını girebileceği açıklama kutuları da oluşturulmuştur.

Daha sonra, hazırlanan yazılımın başarısının ölçülmesi için personelin kullanımına sunulmuştur. Intranet ağ yapısı üzerinden yapılan yayın sonucunda personelin işlerinin kolaylaşıp kolaylaşmadığı ve sürece katkı sağlayıp sağlamadığına yönelik tespitler gerçekleştirilmesi hedeflenmiştir. Yazılımın başarısının ölçülmesi için yazılımın kullanılması sonucunda kullanıcının karşısına bir geri bildirim ekranı tasarlanmasına karar verilmiştir. Geri bildirim ekranı için Sistem Kullanılabilirlik Ölçeği (System Usability Scale – SUS) ve uzman görüşlerinden yararlanılmasının uygun olacağı değerlendirilmiştir. Toplamda 28 personelin kullanımına sunulan yazılım ile ilgili olarak kullanım kolaylığı, yazılımın anlaşılabilirliği ve mobil cihaz adli bilişim sürecine katkısına yönelik geri bildirimler alınmıştır. Alınan geri bildirimler neticesinde kullanımının kolay ve anlaşılır olduğu görülmüştür. Mobil cihaz adli bilişimi sürecini hızlandırdığı ve kolaylaştırdığı alınan geri dönüşlerden anlaşılmaktadır. Ayrıca adımların nasıl uygulanacağına ilişkin açıklık konusunda fikir birliği olduğu da dikkat çekmektedir. Doğru ve tutarlı bir şekilde kullanıcıyı yönlendiren bu yazılımın ayrıca iş yükünü de hafifletmesi beklenmektedir. Mobil cihaz adli

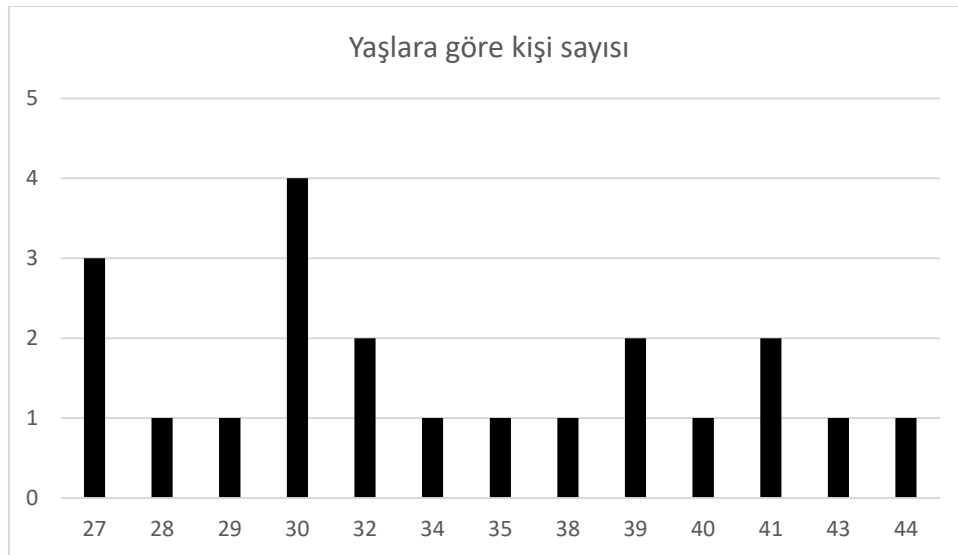
bilişiminde çalışmaya başlayan yeni personelin de kolaylıkla bu yazılımı kullanabileceği değerlendirilmektedir.

Ayrıca sistem yeni veriler girildikçe geliştirilmeye müsaittir. Sistem kullanıldıkça elde edilen veriler ile sistemin güncellemesi ve geliştirilmesi yapılacaktır. Bu sistemin Emniyet Genel Müdürlüğü tarafından kullanılması beklenmektedir.

6.2.Verinin Toplanması ve Değerlendirilmesi

Mobil cihaz adli bilişimine ilişkin sürece etki eden özniteliklerin belirlenmesinde uzmanlarla görüşülmesi kararlaştırılmıştır. Bu kapsamda Türkiye’de ve diğer ülkelerde bu alandaki uzmanlarla görüşmeler gerçekleştirilmesi için Türkçe ve İngilizce uzman görüş formu hazırlanmıştır (EK-1 ve EK-2). Görüşmelerin öncelikli olarak yüz yüze gerçekleştirilmesi amaçlanmıştır. Türkiye dışında Almanya, Arnavutluk, Belçika, Kanada, Romanya ve İsviçre ülkelerindeki birer uzmanla dijital iletişim ortamlarında görüşmeler gerçekleştirilmiştir. Toplamda 21 uzmanla görüşülmüştür.

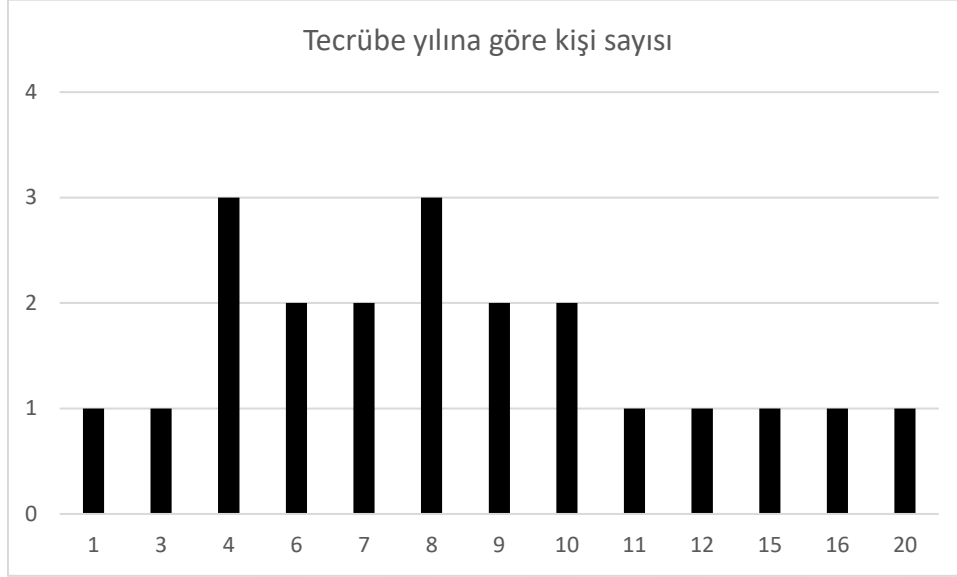
Görüşülen 21 kişiden 20’si erkek; 1’i kadındır. Görüşülen kişilerin yaş ortalaması 34 iken, yaşlara göre dağılımı Şekil 6.1’deki gibidir.



Şekil 6.1. Yaşlara göre kişilerin dağılımı

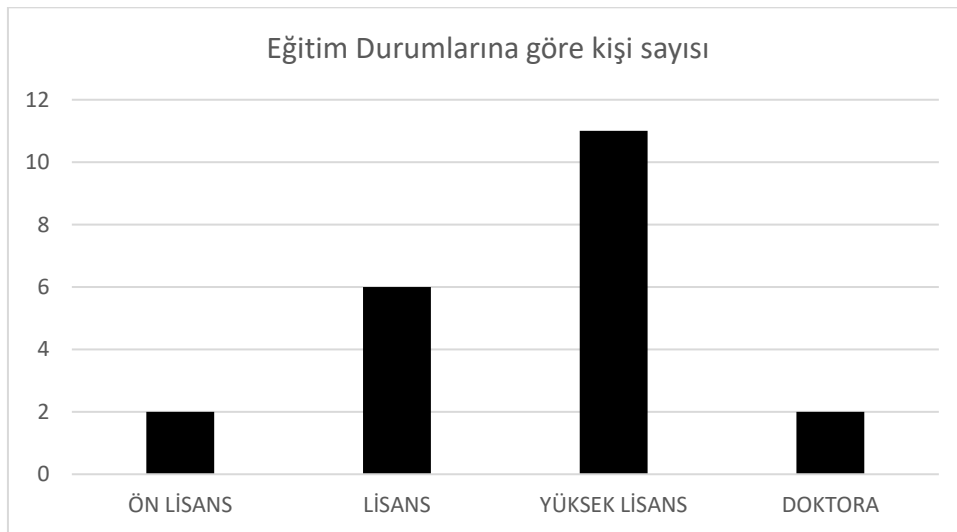
Görüşülen 21 kişinin 3’ü özel sektörde çalışırken, geriye kalan 18’i kamu sektöründe çalışmaktadır. Uzmanlık alanı olarak 16’sı diğer uzmanlık alanlarının yanında adli bilişimi

belirtmiştir. Uzmanlık alanı olarak adli bilişimi belirtmeyen geriye kalan 5 kişi ise, alanla ilgili olarak siber güvenlik, siber suçlar, elektrik-elektronik, bilgisayar teknolojilerini belirtmişlerdir. Alanlarındaki uzmanlık yıllarının ortalaması 8,4 iken; uzmanlıktaki tecrübelerinin yıllara göre dağılımını gösteren Şekil 6.2’de gösterilmiştir.



Şekil 6.2. Tecrübe yıllarına göre kişilerin dağılımı

Görüşülen kişilerin ön lisans, lisans, yüksek lisans ve doktora mezunu olduğu görülmektedir. 21 kişinin büyük çoğunluğunun 11 kişi ile yüksek lisans mezunu olduğu anlaşılmaktadır. Bu kişilerin eğitim durumuna ilişkin dağılımı Şekil 6.3’te gösterilmiştir.



Şekil 6.3. Eğitim durumlarına göre kişilerin dağılımı

Bu görüşmeler neticesinde mobil cihazlardan imaj alınmasına etki eden faktörlerin mobil cihaza ait bilgiler ve mobil cihazın durumuna ilişkin bilgiler olmak üzere iki kategori altında toplandığı görülmektedir. Cihaza ilişkin bilgiler; cihazın markası, modeli, işletim sistemi ve sürümü, hangi çip sete sahip olduğu gibi bilgilerden oluşmaktadır. Cihazın durumuna ilişkin bilgiler kısmında ise; cihazın şifreli olup olmadığı, ekran arızasının olup olmadığı, port arızasının olup olmadığı, anakart arızası olup olmadığı, cihazın parçalanıp parçalanmadığı, yazılımsal bir arızasının olup olmadığı bilgilerinden oluşmaktadır. Bunların yanı sıra karşılaşılan sorunların hangi yöntemle ile aşıldığının tespit edilmesi için de cihaza yapılan işlemlerin de toplanmasına karar verilmiştir. Yapılan işlemler ise port değiştirilip değiştirilmediği, batarya değiştirilip değiştirilmediği, ekran değiştirilip değiştirilmediği, basit tamir işlemi yapılıp yapılmadığı, j-tag işlemi yapılıp yapılmadığı, chip-off işlemi yapılıp yapılmadığı, root işlemi yapılıp yapılmadığı, TWRP/CVM kurulumu yapılıp yapılmadığı, kullanılan mobil cihaz adli bilişimi yazılımı, hangi personel tarafından işlemin yapıldığı ve bu işlemlerin sonucuna ait verilerden oluşmaktadır.

Belirlenen özniteliklere ilişkin verilerin toplanması için Gazi Üniversitesi Ölçme Değerlendirme Etik Alt Çalışma Grubu tarafından gerekli izinlerin alınması koşuluyla etik açıdan sakınca bulunmadığı kararı alınmıştır (EK-3). Bunun üzerine Emniyet Genel Müdürlüğünden gerekli izinler alınmıştır (EK-4). Bu kapsamda EGM Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğü tarafından bir yıl süresince 1710 adet akıllı telefon olan mobil cihaza yapılan işlemlere ilişkin veriler toplanmıştır.

Belirlenen özniteliklerden telefon markası için ülkemizde sıklıkla kullanılan ve toplanan verinin %87'sine tekabül eden 12 adet telefon üreticisi üzerinden frekans tabloları düzenlenmiştir. Belirlenenlerin dışında kalan markalar sayıları az olduğundan diğer kategorisinde yer almıştır.

Bu veriler ışığında en fazla karşılaşılan telefon markasının %41 ile Samsung olduğu görülmüştür. Ayrıca işletim sistemlerine yönelik yapılan değerlendirmede ise en yüksek oranın %70 ile Android 7.0 öncesinde olduğu görülmüştür. Hafıza çipi açısından bakıldığında en sık karşılaşılan hafıza çipinin Qualcomm olduğu görülmüştür.

Cihazların durumlarıyla ilgili olarak cihazların %15'inin şifreli olduğu, %12'sinde ekran arızası olduğu, %19'unda ise port arızası olduğu görülmüştür. Ana kart arızasının %3

oranında kaldığı ve yine yaklaşık %3 oranındaki cihazın parçalandığı görülmüştür. Yazılımsal arıza %6 oranında mevcut iken; %5'lik kısmında ise root ihtiyacının mevcut olduğu görülmüştür.

6.3.Yazılım İçin Kalite Fonksiyon Göçerimi Uygulanması

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için müşteri olarak mobil cihaz adli bilişimiyle uğraşan personel kabul edilmiştir. Müşterinin sesine ulaşmak için, onların bu şekilde bir yazılımdan beklentilerinin neler olduğuna ilişkin görüşmeler gerçekleştirilmiştir. Bu görüşmelerde taslak olarak oluşturulan bir yazılım üzerinden talepleri alınmıştır ve bunun yanı sıra bu taleplerin onlar için önemleri de belirlenerek, KFG oluşturulması için tüketici talepleri belirlenmiştir.

6.3.1. Kalite evinin bileşenleri

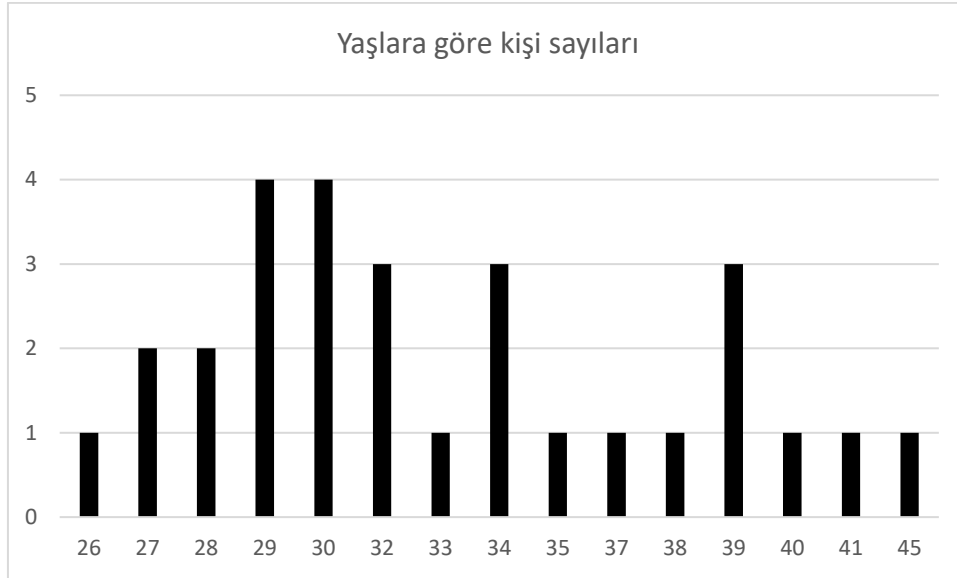
Tüketici talepleri

Bu çalışmada hedeflenen yazılımın tüketicisi olarak kabul edilen mobil cihaz adli bilişim personeliyle grup görüşmesi gerçekleştirilmiştir. Görüşmeler neticesinde mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için sekiz farklı talepte bulunulmuştur. Bunlar yazılımın anlaşılır olması, kullanımının kolay olması, kendi performansının izlenilebilmesi, cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi, cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi, benzer durumla karşılaşmış kişinin görüntülenebilmesi, açıklama verisi girme imkânı olması ve yöntemin nasıl yapılacağı konusunda bilgi vermesidir.

Tüketici önem düzeyleri

Taleplerin neler olduğu ve bu taleplerin ne kadar önemli olduğunun tespitinde kullanılan matristir. Müşteri taleplerine ait önem dereceleri ile karmaşık problemler için güçlü bir karar verme tekniği ortaya çıkmaktadır. İlişki matrisinde kullanılmak üzere önem derecesine göre 1-9 arasında puanlama yapılmaktadır (Wind ve Saaty, 1980).

Bu yazılımı kullanması beklenen 29 farklı personel ile görüşme yapılmıştır. Bu personel ile “Müşterinin Sesi Tespiti İçin Görüşme Formu” (EK-5) kullanılarak yüz yüze görüşmeler gerçekleştirilmiştir. Bu personelin yaş ortalaması 32,9 dur. Yaş dağılımını Şekil 6.4.’te gösterilmiştir.



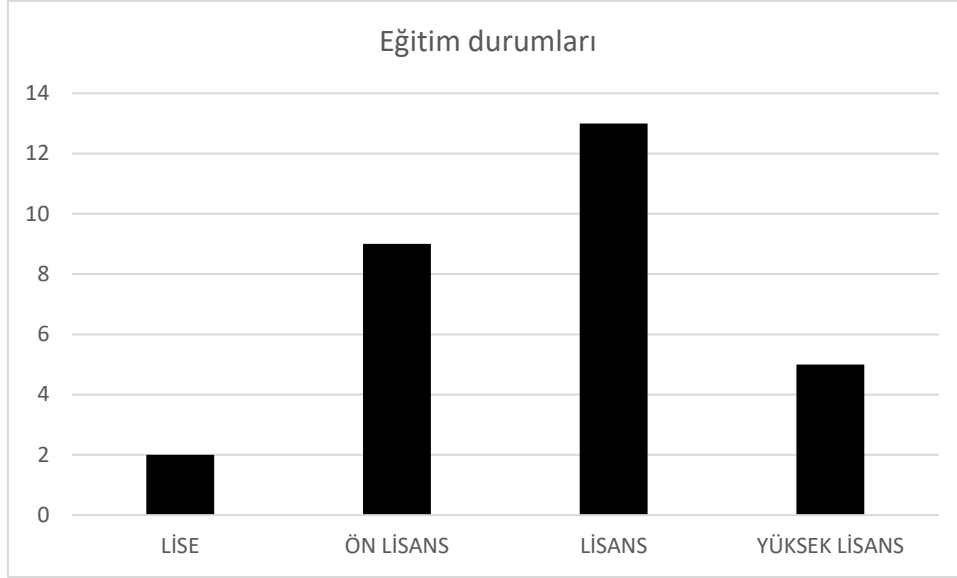
Şekil 6.4. Yaşlara göre dağılım

Görüşme gerçekleştirilen 29 kişinin 21'i erkek ve 8'i kadındır. Alandaki tecrübeleri açısından en tecrübelisi 11 yıl, en az tecrübelisi ise 1 yıl tecrübeye sahiptir. Tecrübe yıllarının ortalaması 5,4 yıl olup; tecrübe yıllarına göre dağılım, Şekil 6.5.'te gösterilmiştir.



Şekil 6.5. Tecrübe yıllarına göre dağılım

Görüşülen personelin eğitim durumlarına dağılımı incelendiğinde lise, ön lisans, lisans ve yüksek lisans mezunu oldukları görülmüştür. En sık karşılaşılan mezuniyet derecesinin, 13 kişi ile lisans eğitim düzeyi olduğu anlaşılmıştır. Eğitim durumlarına göre dağılım, Şekil 6.6.'da gösterilmiştir.



Şekil 6.6. Eğitim durumlarına göre dağılım

Gerçekleştirilen görüşmeler neticesinde elde edilen talepler için 1-9 arasında önem düzeyleri belirlenmesi istenmiştir. Talepler için belirlenen önem düzeyleri Çizelge 6.1.'deki gibidir.

Çizelge 6.1. Talepler ve önem düzeyleri

Talepler	Önem Düzeyi
Kendi performansının izlenilebilmesi	7,72
Kullanımının kolay olması	7,52
Yazılımın anlaşılır olması	7,52
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	7,14
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	7,38
Açıklama verisi girme imkânı olması	8,10
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45

Teknik gereksinimler

Bu çalışma kapsamında taleplerin karşılanabilmesi için, dokuz farklı teknik gereksinime karar verilmiştir. Bunlar temelde yazılımın arayüzünde bazı değişikliklerin yapılması ve akıllı telefonlara ilişkin açık kaynaktaki bazı veri tabanlarının yazılıma aktarılması olarak iki başlıkta toplanabilmektedir.

Yazılımın arayüzüyle ilgili olarak gereken teknik gereksinimlerin, sade arayüz, kullanım ipuçları, web tabanlı yazılım, veri girişi için listbox (veriyi el ile girmek yerine bir listeden seçilmesi) kullanılması, textbox (serbestçe metin girilebilecek alan) olması, karar ağacı diyagramı çıktı vermesi ve istatistik ekranı olarak belirlenmiştir. Başvurulacak veri

tabanının, mobil cihazlara ilişkin bazı verilerin bulunduğu “back4app¹” isimli internet sitesinden elde edilen veri setinden oluşturulmasına karar verilmiştir. Teknik Gereksinimler, Çizelge 6.2.’de gösterilmiştir.

Bu sitedeki veri setinde mobil cihazlara ilişkin marka, model bilgileri bulunmaktadır. Bunun yanında cihaza ilişkin çıkış tarihi, ses, batarya, işlemci, çip seti, renk, boyutlar, ekran çözünürlüğü, ekran boyutu, ekran tipi, GSM teknolojisi, GPS, ekran kartı, hafıza, hoparlör, hafıza kartı, NFC teknolojisi, network, network hızı, işletim sistemi, birincil kamera, RAM, SIM, ikincil kamera, sensörler, USB ve WLAN gibi bilgilerinin çekilmesinin çalışma açısından katkı sağlayacağı değerlendirilmiştir.

Çizelge 6.2. Teknik Gereksinimler

Teknik Gereksinimler
İstatistik ekranı
Sade arayüz
Kullanım ipuçları
Web tabanlı yazılım
Listbox kullanılması
Textbox kullanılması
Karar ağacı diyagramı
Mobil cihazlar için veri tabanı
Yapılan işlemlere ilişkin veri tabanı

Korelasyon

Korelasyon matrisi ile kalite evinin çatısını oluşturulmaktadır. Bu matriste teknik gereksinimlerin birbiriyle olan pozitif veya negatif ilişkileri tespit edilmektedir (Yıldız ve Baran, 2011).

Çalışma kapsamında belirlenen dokuz farklı teknik gereksinimin birbirleriyle olan ilişkisini gösterir korelasyon matrisi Çizelge 6.3.’teki gibidir. Bu matriste olumlu ilişkiler (+) ile gösterilirken; olumsuz ilişkiler (x) ile gösterilmiştir.

¹ Back4app sitesi, uygulamalar için düşük kodlu arka yüz imkanı sunan bir sitedir. <https://www.back4app.com/database/paul-datasets/cell-phone-dataset> Erişim tarihi: 21.01.2023

Çizelge 6.3. Korelasyon matrisi

KORELASYON MATRİSİ	İstatistik ekranı	Sade Arayüz	Kullanım ipuçları	Web tabanlı yazılım	Listboxlar oluşturulması	Textboxların oluşturulması	Karar Ağacı Diyagramı	Mobil cihazlar için veri tabanı	Yapılan işlemlere ilişkin veri tabanı
İstatistik ekranı		x		+					+
Sade Arayüz	x		x			x	x		
Kullanım ipuçları		x		+	+			+	+
Web tabanlı yazılım	+		+		+		+	+	+
Listboxlar oluşturulması			+	+				+	
Textboxların oluşturulması		x							
Karar Ağacı Diyagramı		x		+				+	+
Mobil cihazlar için veri tabanı			+	+	+		+		+
Yapılan işlemlere ilişkin veri tabanı	+		+	+			+	+	

İlişkiler

Çalışma kapsamındaki elde edilen sekiz farklı talebin karşılanması için dokuz farklı teknik gereksinim belirlenmiştir. İlişki matrisi hazırlanırken, güçlü ilişki için “O”, orta ilişki için “O”, zayıf ilişki için ise “Δ” sembolleri kullanılmıştır. Herhangi bir ilişkinin bulunmadığı durumlarda ise ilgili hücre boş bırakılmıştır. Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için ortaya çıkan ilişki matrisi Çizelge 6.4’te gösterilmiştir.

Çizelge 6.4. Hedef yazılım için ilişki matrisi

TALEPLER	ÖNEM DERECESESİ	TEKNİK GEREKSİNİMLER								
		İstatistik ekranı	Sade Arayüz	Kullanım ipuçları	Web tabanlı yazılım	Listboxlar oluşturulması	Textboxların oluşturulması	Karar Ağacı Diyagramı	Mobil cihazlar için veri tabanı	Yapılan işlemlere ilişkin veri tabanı
Kendi performansının izlenilebilmesi	7,72	○			Δ					
Kullanımının kolay olması	7,52		○	○	○	○	Δ	○	○	
Yazılımın anlaşılır olması	7,52		○	○	○	○				
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	7,14				○	○			○	
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10		○		○					
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	7,38			○						○
Açıklama verisi girme imkanı olması	8,10						○			
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45			○				○		○

Kendi performansını izleyebilme talebi için istatistik ekranı oluşturulması ile güçlü bir ilişki olması gerektiği değerlendirilmiştir. Bunun yanı sıra web tabanlı bir yazılımın zayıf da olsa etkisi olacağı değerlendirilmiştir.

Kullanım kolaylığı talebinin karşılanması için sade bir arayüzün olması, veri girişlerinde listbox kullanılması ve mobil cihazlara ilişkin entegre bir veri tabanının olması arasında güçlü bir ilişkinin olduğu anlaşılmıştır. Bunun yanı sıra kullanım esnasında işlemlere ilişkin ipuçlarının olması, yazılımın web tabanlı olması ile işlem sonunda görsel nitelikli karar ağacı diyagramı çıktı vermesi ile de orta dereceli bir ilişki olduğu, textbox oluşturulması ile zayıf dereceli bir ilişki olduğu kanaatine varılmıştır.

Anlaşılır bir yazılım talebiyle ilgili olarak ise, sade bir arayüzün yanı sıra kullanım ipuçlarının güçlü bir ilişkisi olduğu, web tabanlı yazılım ve veri girişi esnasında listboxların olması ile de orta derecede biri ilişkisi olduğu değerlendirilmiştir.

Cihaz bilgileri girerken modele göre diğer verilerin otomatik gelmesi talebi için web tabanlı yazılım, listboxların oluşturulması ve mobil cihazlar için veri tabanı oluşturulması arasında güçlü bir ilişki olduğu değerlendirilmiştir.

Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi ile ilgili olarak arayüzün sade olması ve yazılımın web tabanlı olması gerektiği değerlendirilmiştir. Her iki teknik gereksinimin de orta dereceli ilişkisi olduğu kanaatine varılmıştır.

Özellikle çözüme kavuşturulamamış bir konuda benzer durumla karşılaşmış ve bunu çözüme kavuşturmuş personelin bilgisine başvurulması gerekebilmektedir. Bu talebin karşılanabilmesi açısından yapılan işlemlere ilişkin bir veri tabanının oluşturulmasının güçlü bir ilişkisi olduğu, kullanım ipuçlarının ise orta derecede bir ilişkisi olduğu değerlendirilmiştir.

Standart dışı durumlarla karşılaşılması durumunda durumun tespiti veya uygulanan yöntemlerin detayları için açıklama verisi girme talebi alınmıştır. Bu talebin karşılanması için textbox alanların oluşturulması ile güçlü bir ilişkinin olduğu değerlendirilmiştir.

Yöntemin nasıl yapılması gerektiği ile ilgili bilgi vermesi talebiyle ilgili olarak, kullanım ipuçları, karar ağacı diyagramı çıktısı ve yapılan işlemlere ilişkin veri tabanı teknik gereksinimleri belirlenmiştir. Bu üç teknik gereksinimin de güçlü bir ilişki içerisinde bulunduğu değerlendirilmiştir.

Planlama matrisi

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımına ilişkin taleplerin gerçekleştirilmesi durumunda son kullanıcı açısından yazılımı kullanma isteği, satış noktası olarak kabul edilmiştir. Karşılanması halinde kullanma isteğinde önemli bir ilerleme oluşturacağı değerlendirilen talepler: kullanımının kolay olması, yazılımın anlaşılır olması, cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi ve yöntemin nasıl yapılacağı konusunda bilgi vermesidir.

Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi talebinin karşılanması durumunda kullanma isteğinde ilerleme olması beklenirken, kendi performansının izlenilmesi, benzer durumla karşılaşmış kişinin görüntülenmesi ve açıklama verisi girme imkânının olması taleplerinin karşılanmasının kullanma isteğinde bir değişiklik olması beklenmemektedir. Sekiz farklı talebe ilişkin hazırlanan planlama matrisi Çizelge 6.5.'te gösterilmiştir.

Çizelge 6.5. Planlama matrisi

TALEPLER	ÖNEM DERECEİ	SATIŞ NOKTASI
Kendi performansının izlenilebilmesi	7,72	1,0
Kullanımının kolay olması	7,52	1,5
Yazılımın anlaşılır olması	7,52	1,5
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	7,14	1,5
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10	1,2
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	7,38	1,0
Açıklama verisi girme imkanı olması	8,10	1,0
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45	1,5

Teknik tanımlayıcılar

Çalışma kapsamında taleplerin karşılanması için dokuz farklı teknik gereksinimin nasıl gerçekleştirileceğine ilişkin teknik detaylara yer verilmiştir. Bu kısımdaki teknik detaylar her ne kadar sayısal olarak ölçülebilen ve ölçü birimleriyle tanımlanabilen nitelikte olmasa da matriste teknik terminolojiyle yer verilmiştir.

İstatistik ekranı için hali hazırda veri tabanında sınıflandırılmış şekilde bulunan işlemlerin, veri türleri ve yapılan işlemleri sınıflandıran bir dashboard (gösterge paneli) şekline getirilmesi hedeflenmektedir. Bunu gerçekleştirmek için ise pie chart ve line chart gösterge seçenekleri kullanılmasına karar verilmiştir.

Bütün girdilerin tek bir ekranda olmasından dolayı sade arayüz talebiyle karşılaşılmıştır. Sade bir arayüz için alt menü sekmelerinin yer aldığı farklı ekranların oluşturulmasının gerekliliğine karar verilmiştir.

Kullanım ipuçları için ise yazılımda yer alan öğelerin işlevlerinin açıklanması gerekmiştir. Bunun için ise yazılım içerisinde üzerine gelince açıklayıcı nitelikteki metin kutularının eklenmesi gerektiğine karar verilmiştir.

Personel tarafından kullanılan bilgisayarlar internete bağlı olmadığından dolayı intranet üzerinden yayın yapan bir proje için yazılımın web tabanlı olması gerekmiştir. Bunu amacıyla Java Script kütüphanelerinden olan kullanıcı arayüzü oluşturmak için kullanılan React tercih edilmiştir.

Listboxlar oluşturularak, cihaza ilişkin marka, model bilgilerinin yanı sıra durumuna ilişkin bilgilerin de elle girilmesi yerine listeden seçilmesi hedeflenmektedir. Bunun için React kütüphanesinden listbox ögesi kullanılmasına karar verilmiştir.

Textbox oluşturulması için yine React kütüphanesinden textbox ögesi kullanılmasının uygun olduğuna kanaat getirilmiştir. Bu sayede işlem bitiminde kullanıcıya esnek veri girişi yapma imkânı sağlayan metin alanı oluşturulacaktır.

Cihaz verileri girildiğinde kullanıcıya işlemi nasıl yapması gerektiğini göstermesi için karar ağacı diyagramı çıktısı oluşturulması gerekmektedir. Karar ağacı çıktısı için decision tree algoritması kullanılmasına karar verilmiştir.

Mobil cihazlara ilişkin verilerin bulunduğu veri tabanı oluşturulmasında Python yazılımına ait BeautifulSoup kütüphanesi kullanılmıştır. Bu kütüphane sayesinde back4app isimli internet sitesinden mobil cihazlara ilişkin veri setleri çekilmiştir. Bu sayede cihazlara ait detay bilgileri veri tabanına entegre edilerek, personelin cihazı tanımak veya diğer bilgilerini girmek için ilave bir araştırma yapmasına gerek kalmayacaktır.

Yapılan işlemlere ilişkin veri tabanı oluşturularak, işlemlerin kim tarafından yapıldığı bilgisiyle birlikte yazılıma dahil edilmesi hedeflenmiştir. Bu konuda hali hazırda toplanan verilerin MySQL veri tabanı sayesinde kullanılmasına karar verilmiştir.

Gerçek ve hedef değerler

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımının KFG çalışması başlangıcındaki mevcut durumu daha öncesi olmadığı için 1 olarak kabul edilmiştir. Mevcut durum belirlendikten sonra, bu talebe ilişkin yazılımın hangi noktaya getirilmesi gerektiğine karar verilmiştir. Gerçek ve hedef değerlere ilişkin yapılan tespitlere ilişkin son durum Çizelge 6.6.'da gösterilmiştir.

Çizelge 6.6. Gerçek ve hedef değerler tablosu

TALEPLER	ÖNEM	Mevcut Durum	Hedef	İlerleme oranı
Kendi performansının izlenilebilmesi	7,72	1	3	3,0
Kullanımının kolay olması	7,52	1	5	5,0
Yazılımın anlaşılır olması	7,52	1	5	5,0
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	7,14	1	5	5,0
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10	1	4	4,0
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	7,38	1	4	4,0
Açıklama verisi girme imkanı olması	8,10	1	4	4,0
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45	1	5	5,0

6.3.2. Kalite evinin oluşturulması ve yazılıma uygulanması

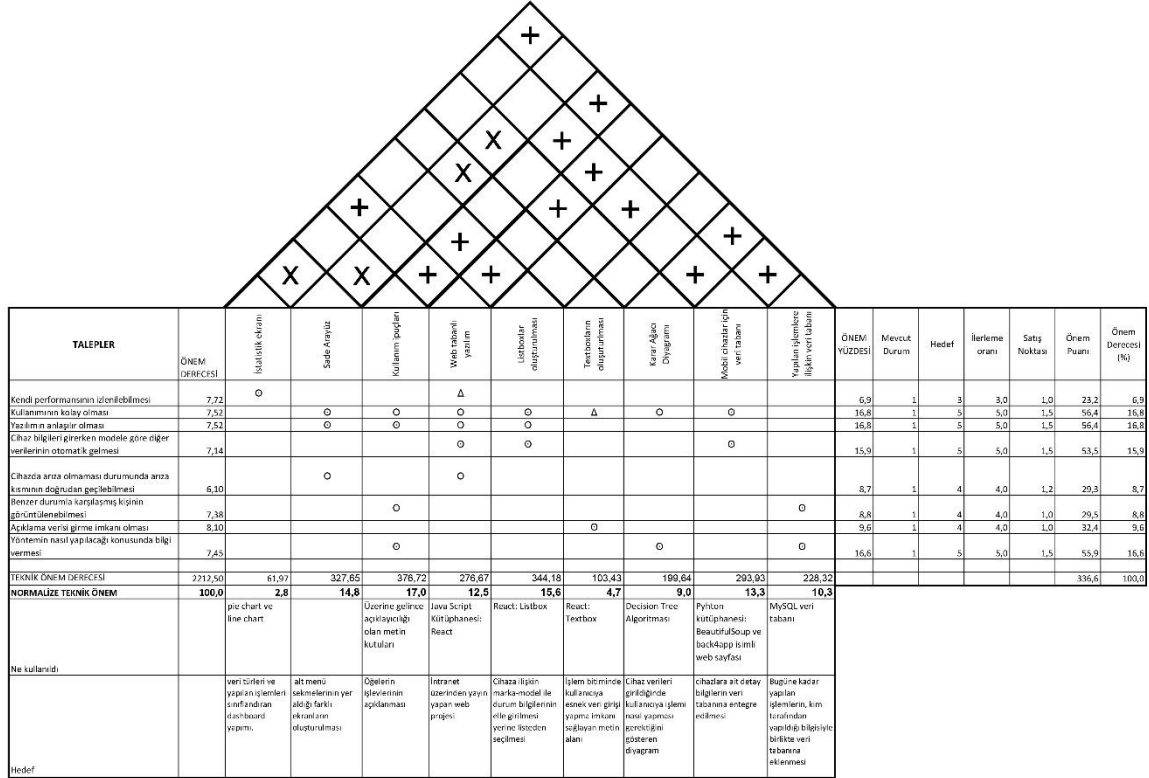
Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için kalite evi bileşenleri bir önceki bölümde tek tek ele alınmıştır. Bu bölümde ele alınan bileşenler ve oluşturulan tüm tablolar bir araya getirilerek kalite evi oluşturulmuş ve yazılımın oluşturulması aşamasında nelerin önemli olduğu, nasıl gerçekleştirileceği ve bunlar gerçekleştirilirken önceliklerin neler olduğu ortaya konulmuştur. Hazırlanan kalite evi Çizelge 6.7’de yer almaktadır (EK-6).

Gerçekleştirilmesi planlanan teknik gereksinimlerden, normalize teknik önem değeri 17,0 ile en yüksek olan kullanım ipuçlarının yer almasının en fazla önem verilmesi gereken özellik olduğu görülmektedir. Bununla birlikte normalize teknik önemi 15,6 olan listboxların oluşturulması, normalize teknik önemi 14,8 olan sade arayüz gereksinimi, normalize teknik önemi 13,3 olan mobil cihazlar için veri tabanı oluşturulması ile normalize teknik önemi 12,5 olan web tabanlı yazılım teknik gereksinimlerinin de yazılım için önem arz ettiği görülmektedir. Bunlardan sonra, normalize teknik önemi 10,3 olan yapılan işlemlere ilişkin veri tabanı ve normalize önem değeri 9,0 olan karar ağacı diyagramı da yapılması gerekli olan bir diğer gereksinim olarak karşımıza çıkmaktadır.

Teknik önemi daha düşük olan diğer özelliklerin daha geri planda kalabileceği değerlendirilmiştir. Özellikle istatistik ekranı özelliğinin en düşük puanda kaldığı gözlemlenmiştir. Her ne kadar textbox oluşturulması ve istatistik ekranı düşük öneme sahip

gibi gözükse de bu çalışma kapsamında tüm taleplerin yerine getirilmesi için çaba gösterilmiştir.

Çizelge 6.7. Yazılım için oluşturulan kalite evi



6.4. Karar Destek Sisteminin Oluşturulması

Karar destek sisteminin ihtiyaç, veriler, modeller, tasarım, uygulama ve geliştirme olarak altı farklı aşamadan oluştuğu önceki bölümlerde belirtilmişti. Bu çalışmanın problemini de oluşturan bu yazılımın ihtiyaç kısmı, mobil cihaz adlı bilişimi alanında karşılaşılan benzer problem bir adli bilişim personeli tarafından çözülebilenken, diğer personel tarafından çözülememektedir. Ayrıca cihazdan cihaza farklılık arz eden problemler karşısında doğru çözüme ulaşmak için deneme yanılma yöntemlerinin kullanılması sürecinde çokça iş gücü, zaman ve maliyet sarf edilmektedir. Oluşturulan karar destek sistemi yazılımı ile bu sorunların aşılması hedeflenmekte ve ayrıca mobil cihaz adli bilişime etki eden faktörler ve bunlara ilişkin stratejilerin tespit edilmesi beklenmektedir.

Veriler kısmında mobil cihaz adli bilişimine ilişkin yapılmış işlemlere dair toplanan veriler kullanılmıştır. Bu veriler cihaza ait bilgiler, cihazın durumuna ilişkin bilgiler ve cihaza

yapılan işlemlere ilişkin bilgiler olmak üzere toplam üç farklı kategoriden oluşmaktadır. Veriler üzerinde analiz çalışması yapılmış, eksik ve kirli veri vs. gibi değerler göz önünde bulundurularak temizleme işlemi yapılmış ve veri, eğitim ve test için hazır hale getirilmiştir.

Öznitelik değerlendirmesi yapılmış bu veriler altı farklı algoritma kullanılarak eğitilmiştir. WEKA yazılımında da yer alan bu algoritmalar, ayrıştırma için en az kova boyutu kullanan OneR, her düğümde belli sayıdaki özellikleri dikkate alan RandomTree, RandomTree topluluklarını paketleyen Random Forest, en yakın komşu bulma görevini hızlandırmaya çalışan IBk, olasılıksal sınıflandırıcı olan Naive Bayes ve kullanıcıya budama ve karar ağacı görselleştirme imkânı sunan J48 algoritmalarıdır (Aydemir, 2019:116-133).

Verinin eğitiminde çapraz doğrulama yöntemine başvurulmuştur. Eğitim sonunda gerçekleştirilen testlerde karar ağacı algoritması başarı oranı en yüksek algoritma çıkmıştır (Çizelge 6.8.).

Çizelge 6.8. Sınıflandırma algoritmaların başarı oranları

Algoritma	Başarı oranı
OneR	%91,2281
RandomForest	%96,7836
RandomTree	%96,4327
IBk	%96,4912
Naive Bayes	%92,6901
J48 (DecisionTree)	%97,076

Karar ağacı algoritması, tüm adımları görselleştirmektedir. Bu sayede karar ağacı algoritması, insanlar tarafından daha kolay anlaşılmaktadır (Kabari ve Nwachukwu, 2013). Bu sayede kullanıcı açısından anlaşılabilir bir ağaç yapısı sunularak, mobil cihazlarla ilgili karşılaşılan problemlerin çözümüne ilişkin önerilerin sunulması hedeflenmiştir. Karar ağacı algoritmasının karar destek sistemine uygulanması için RapidMiner araç olarak kullanılmıştır. RapidMiner kullanımında karar ağacı algoritması olarak sunduğu iki farklı operatör ID3 ve CHAID algoritmalarıyla test edilmiştir. RapidMiner ile bu veriler bu iki farklı algoritma ile test edildiğinde Çizelge 6.9.'daki sonuçlar elde edilmiştir. Görüldüğü üzere en yüksek başarı oranı ID3 ile elde edilmiştir.

Çizelge 6.9. RapidMiner karar ağacı algoritmalarının kıyası

Algoritma	Başarı Oranı
CHAID	%97,84
ID3	%98,83

Çıkan ağaç yapısında ağaçta derinlik ve boyut belirlenmiş ve budama işlemi gerçekleştirilmiştir. Bu sınıflandırma algoritması sonucunda mobil cihazlardan imaj alınmasında en önemli öznelikliğin cihazın şifreli olma durumu olduğu tespit edilmiştir. Özniteliklerin önem düzeylerine ilişkin tablo Çizelge 6.10’da gösterilmiştir.

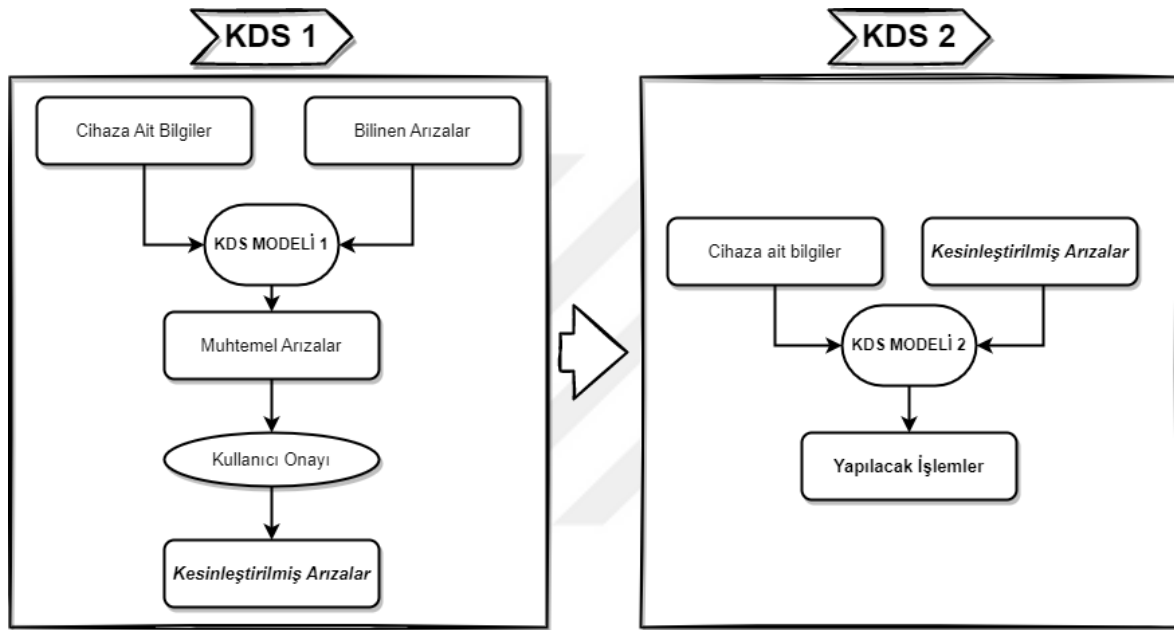
Çizelge 6.10. Özniteliklerin önem düzeyleri

ÖZNİTELİK	ÖNEM DÜZEYİ
Batarya değişimi	0,000
Basit tamir	0,002
XRY yazılımı kullanımı	0,003
Ekran değişimi	0,005
İşletim sistemi sürümü	0,006
Cihaz parçalanma durumu	0,008
Hafıza çipi markası	0,011
Port değişimi	0,013
Ekran arızası	0,015
Chip-off işlemi	0,017
Diğer adli bilişim yazılımlarının kullanımı	0,018
J-tag işlemi	0,020
Root işlemi	0,022
Cihazın markası	0,023
Root ihtiyacının tespiti	0,024
Port arızasının tespiti	0,029
Yazılımsal arızanın tespiti	0,033
UFED yazılımının kullanımı	0,035
Anakart arızasının tespiti	0,036
TWRP/CVM kurulumu	0,093
Şifre kırma işleminin uygulanması	0,173
Cihazın şifreli olma durumu	0,369

Karar destek sistemi modeli olarak, karar ağacı algoritmaları kullanılmıştır. Burada uygulanan algoritmadan ortaya çıkan ağaç yapısı modeli karar destek sistemi için temel niteliktedir. Sistemde iki farklı karar destek sistemi çalışmaktadır. Bunlardan ilki cihazın arızalarını tespit edilmesi için çalışan karar destek sistemidir. Bu sistemde cihaza ait bilgiler

girilerek, sistemin kullanıcıya önerdiği muhtemel arızalar ile sistem işlemektedir. Sistem, çıktı olarak ise mobil cihazda bulunan kesinleşmiş arızaları sunmaktadır.

İkinci karar destek sisteminde ilk karar destek sisteminde tespit edilen kesinleştirilmiş arızalar ile cihaza ait bilgiler girdi olarak kullanarak, bahse konu cihazın imajının alınması için yapılacak işlemlere ilişkin adımlar görsel olarak getirilmektedir. Her iki karar destek sistemine ilişkin model Şekil 6.7’de gösterilmiştir.



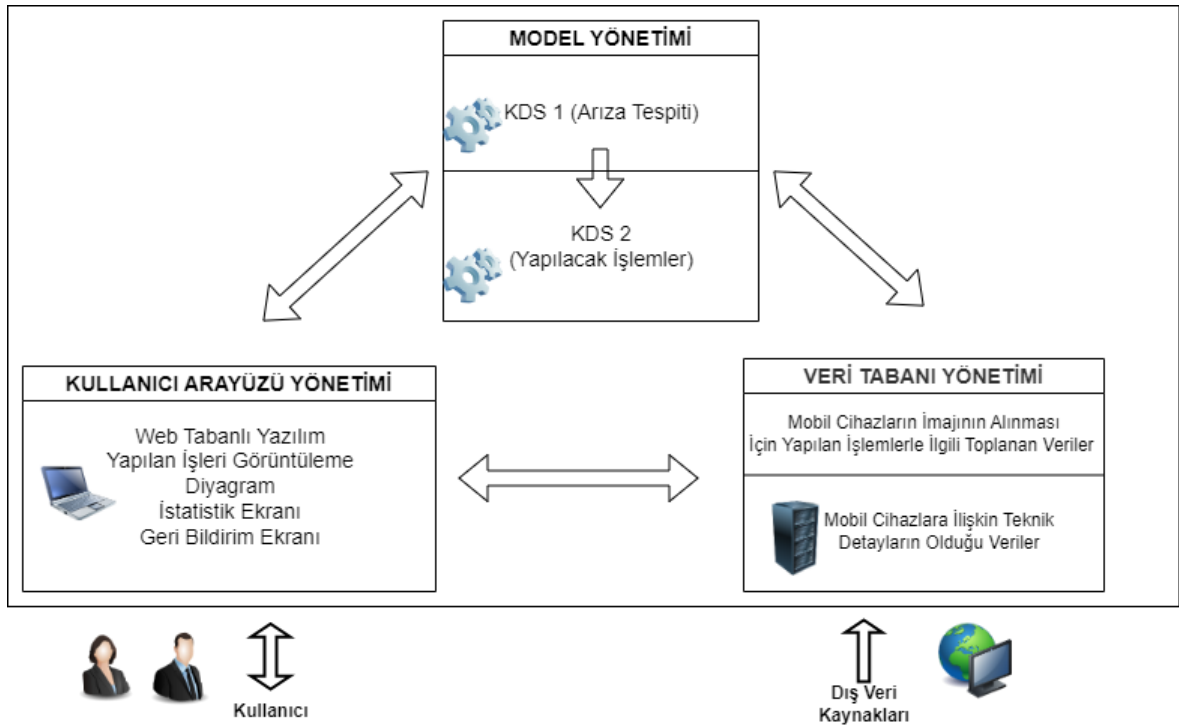
Şekil 6.7. Karar destek sistemi modeli

Tasarım aşamasında ise kalite fonksiyon göçerimi yöntemi kullanılmıştır. Gerçekleştirilen görüşmeler neticesinde yazılımı kullanması beklenen personelin talepleri dikkate alınmıştır. Bu taleplerin üstesinden gelinmesi için de teknik gereksinimler belirlenerek yazılıma uygulanmıştır.

Uygulama aşamasında ise, hazırlanan yazılımın mobil cihaz incelemesi yapan personele tarafından kullanılması gerçekleştirilmiştir. Ayrıca yazılımın başarısının da takip edildiği bu aşamada 29 personel tarafından yazılım kullanılmıştır. Kullanım sonucunda yazılımın kullanımının kolaylığı ve anlaşılabilirliğinin yanı sıra mobil cihaz adli bilişimi sürecine katkı sağlayacağı yönünde geri bildirimler alınmıştır.

Karar destek sistemi yazılımının geliştirme aşaması da oldukça önem arz etmektedir. Bu kapsamda, kullanım sırasında girilen yeni veriler toplanmakta ve veri tabanının geliştirilmesi planlanmaktadır. Bunun yanı sıra uygulayıcıların kullanımı sonucunda alınan geri bildirimler neticesinde yazılımın güncellenmesi konusu da değerlendirilmektedir.

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi oluşturulurken sayılan adımlar uygulanmıştır. Oluşturulan sistemin veri tabanı, model ve kullanıcı arayüzü yönetimine ilişkin bileşenleri Şekil 6.8.'de gösterilmiştir.



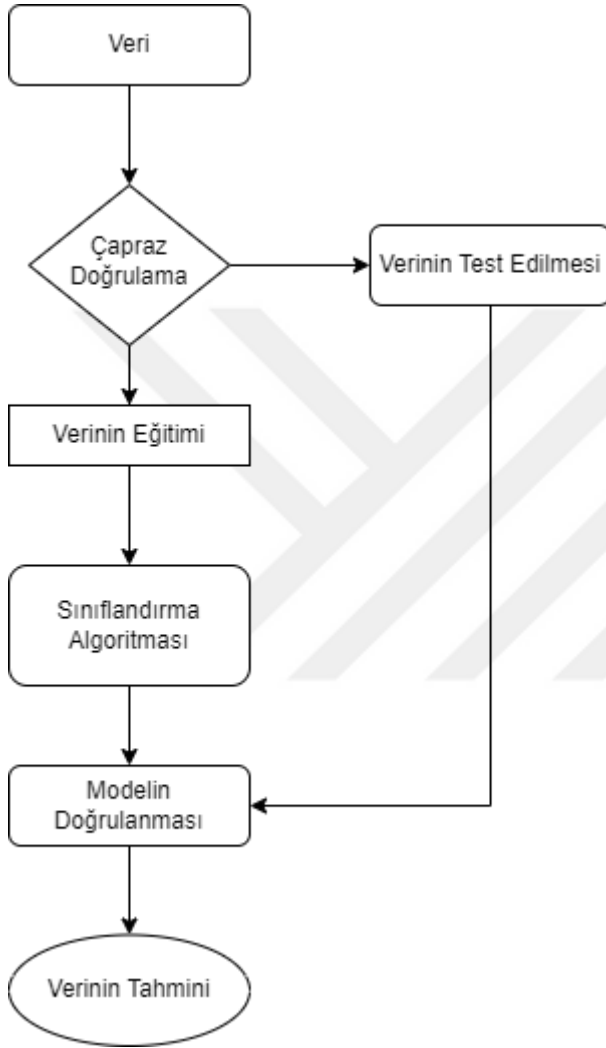
Şekil 6.8. Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi bileşenleri

6.5. Web Tabanlı Yazılımın Oluşturulması

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için öncelikle kullanılacak algoritma belirlenmiştir. En yüksek başarı oranına sahip bir karar ağacı algoritması olan ID3 algoritması kullanılmıştır.

Belirlenen karar ağacı algoritmasını yazılıma uygulama için RapidMiner aracından yararlanılmıştır. RapidMiner, makine öğrenmesi, veri madenciliği gibi operasyon için ortam sağlayan bir yazılım platformudur (Narayanan, 2020).

RapidMiner aracının yazılıma uygulanmasında veri, çapraz doğrulama sonrasında test edilmektedir. Daha sonrasında veriyi eğitmektedir ve seçilen sınıflandırma algoritmasına göre modeli doğrulamaktadır. RapidMiner aracının kullanımına ilişkin akış şeması Şekil 6.9.'da gösterilmiştir (Narayanan, 2020).



Şekil 6.9. RapidMiner İşleyişi Akış Şeması (Narayanan, 2020)

Kalite fonksiyon göçerimi yöntemiyle oluşturulan kalite evindeki isterler yerine getirilmiştir. İstatistik ekranı için hali hazırda veri tabanında sınıflandırılmış şekilde bulunan işlemlerin, veri türleri ve yapılan işlemleri sınıflandıran bir dashboard (gösterge paneli) şeklinde gösterilmesi için pie chart ve line chart gösterge seçenekleri kullanılmıştır.

Yazılımın web tabanlı olması için Java Script ve kütüphanesi React kullanılmıştır. Bu sayede personelin, bilgisayarlarındaki web tarayıcıları ile projeye erişmesi mümkün kılınmıştır.

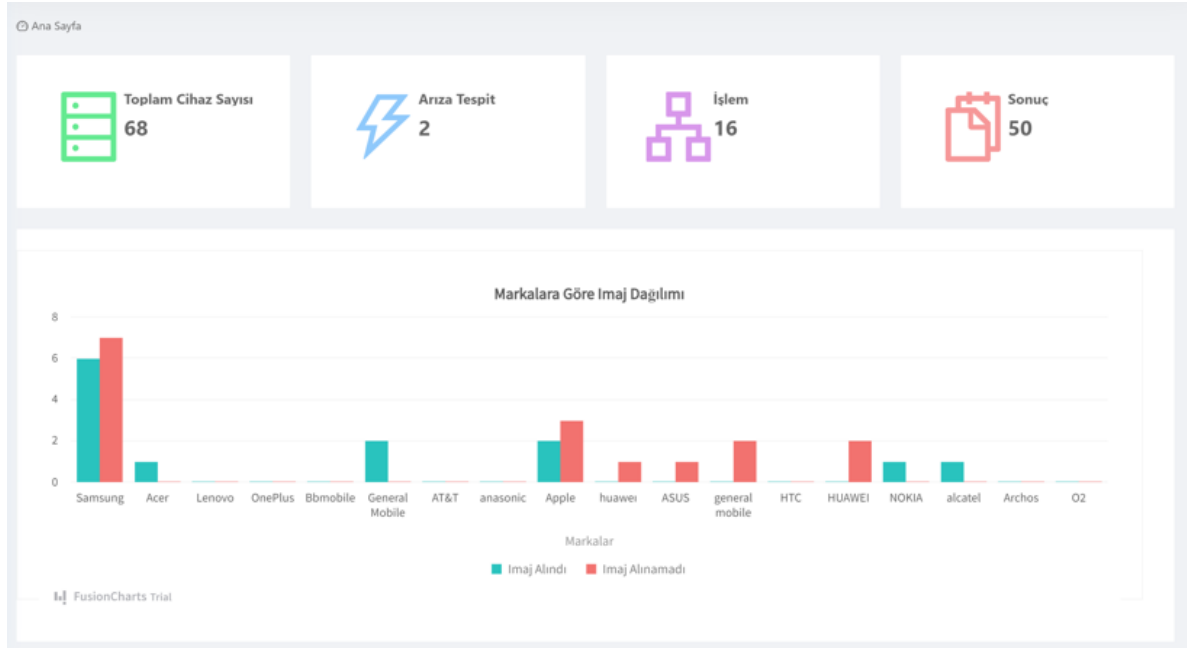
Ancak internet üzerinde değil, bilgisayarların bağlı olduğu intranet üzerinden yayın yapan bir proje gerçekleştirilmiştir. Intranet yapısıyla birlikte, web tarayıcıları ile iç ağdaki sunucuya ait IP'ye erişerek yazılıma erişilmesi sağlanmıştır.

Mobil cihaza ilişkin marka, model bilgilerinin yanı sıra durumuna ilişkin bilgilerin de elle girilmesi yerine listeden seçilmesi için React Kütüphanesinden listbox ögesi kullanılmıştır. İşlem bitiminde kullanıcıya esnek veri girişi yapma imkânı sağlanması için metin alanı React kütüphanesinden textbox ögesi ile sağlanmıştır.

Mobil cihazlara ait detay bilgileri veri tabanına bütünleştirilerek, personelin cihazı tanımak veya diğer bilgilerini girmek için ilave bir araştırma yapmasına gerek kalmaması için ilgili verilerin bulunduğu veri tabanı oluşturulmuştur. Bu veri tabanının oluşturulması için Python yazılımına ait BeautifulSoup Kütüphanesi ile back4app isimli internet sitesinden mobil cihazlara ilişkin veri setleri çekilmesi sağlanmıştır.

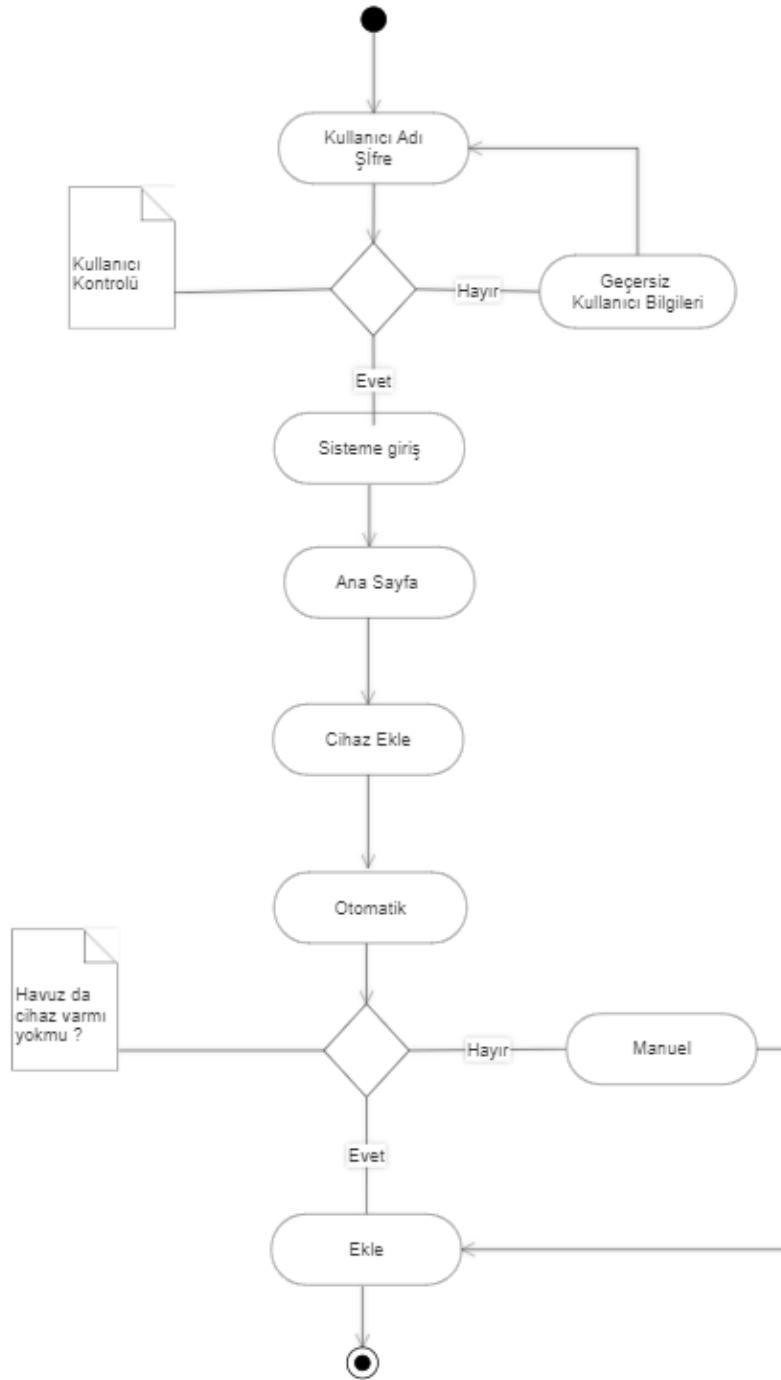
Yapılan işlemlere ilişkin veri tabanı oluşturularak, işlemlerin kim tarafından yapıldığı bilgisiyle birlikte yazılıma dâhil edilmesi hedeflenmiştir. Bu konuda hali hazırda toplanan verilerin MySQL veri tabanı sayesinde kullanılmasına karar verilmiştir. Yazılımın bileşenleri diyagram şeklinde EK-7'de gösterilmiştir.

Karar destek sistemi yazılımı tasarımı aşamasında öncelikle kullanıcının kullanıcı adı ve şifresiyle giriş yaparak yazılım üzerinde işlem yapmak için kimliğini doğrulaması (authentication) gerekmektedir. Başarılı giriş işlemi sonrasında karşısına istatistik takip ekranı (dashborad) gelmektedir (Resim 6.1.). Aktivite diyagramlarında eylemin gerçekleştiği aşama elips şekli, açıklama için dikdörtgen metin kutuları, seçim yapılması gereken aşamalar eşkenar dörtgen şekli kullanılmıştır.



Resim 6.1. İstatistik Takip Ekranı

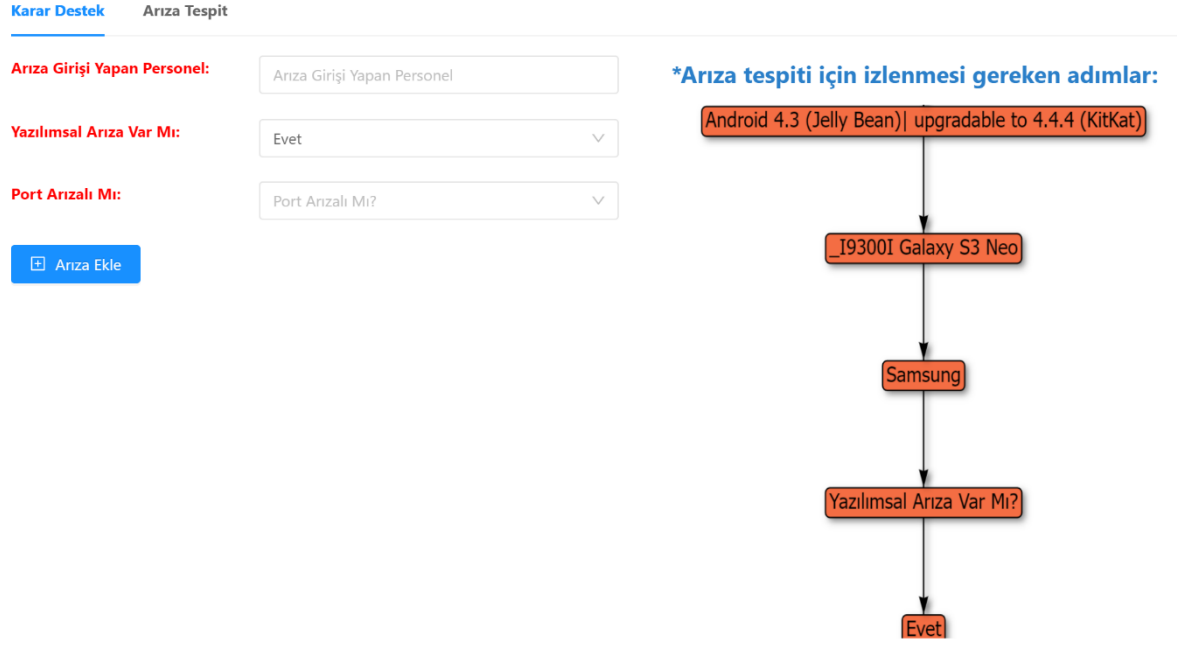
Daha sonrasında ise, işlem yapılacak mobil cihaz bilgileri girilmektedir. Kullanıcı girişi ve cihaz ekleme akışına ilişkin diyagram Şekil 6.10.'da gösterilmiştir.



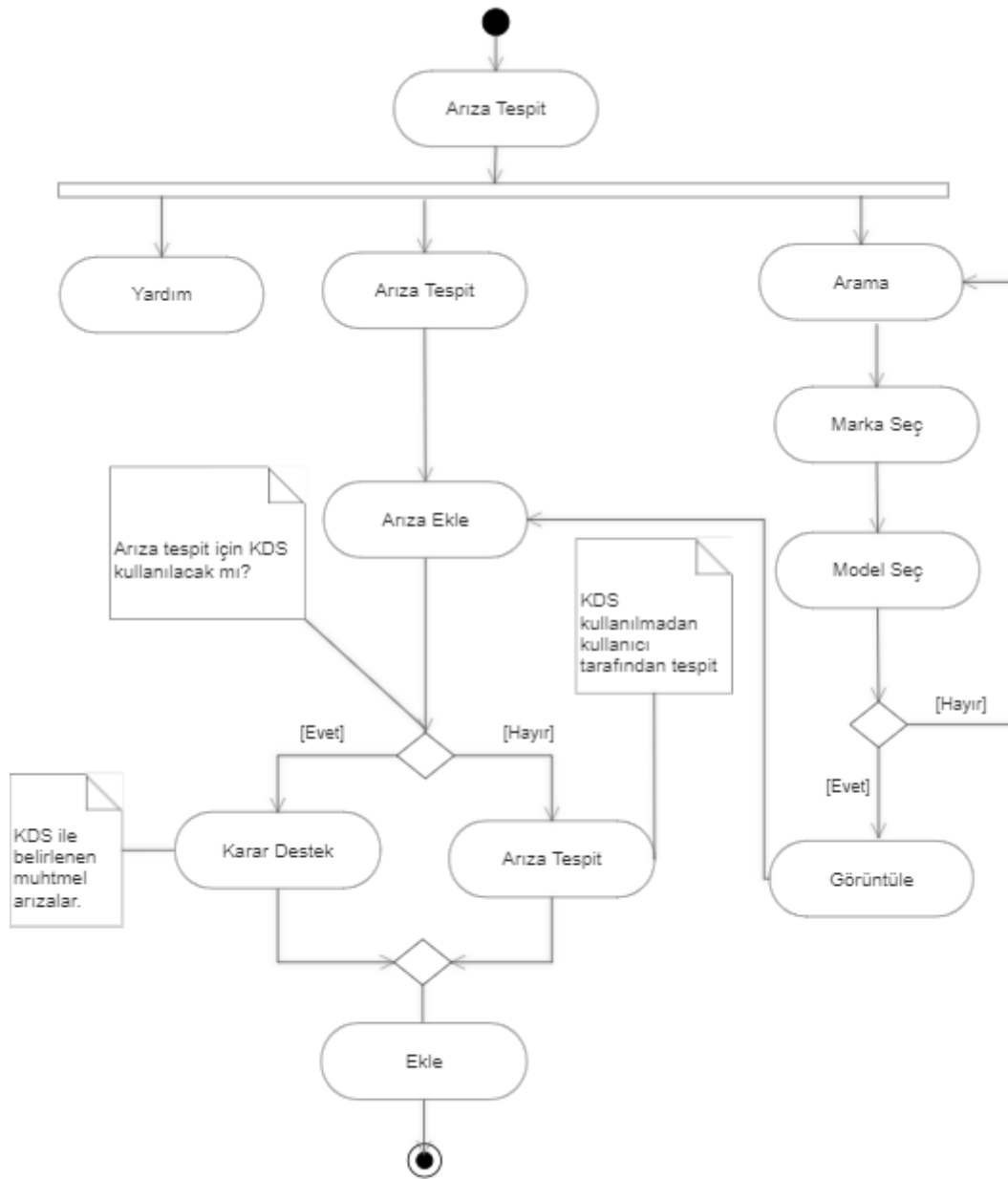
Şekil 6.10. Kullanıcı girişi ve cihaz eklemeye ilişkin aktivite diyagramı

Mobil cihaz bilgileri girildikten sonra arıza tespit işlemi için ilk karar destek sistemi çalışmaya başlamaktadır. Burada sistemin yönlendirmeleriyle muhtemel arızalar kullanıcıya sunulmaktadır. Ekran görüntüsü Resim 6.2.'de sunulmuştur. Bunun yanı sıra tecrübeli kullanıcılar için karar destek sistemine tabi olmaksızın da elle arıza tespit işlemlerinin

girilebileceği seçenek de mevcuttur. Bu akışa ilişkin aktivite diyagramı Şekil 6.11.'de gösterilmiştir.



Resim 6.2. Karar Destek Sistemiyle Arıza Tespit Ekranı (örnek)



Şekil 6.11. Arıza giriş aşamasına ilişkin aktivite diyagramı

Yazılımda arıza tespit işlemleri sonrasında ise mobil cihaz için veri tabanında kayıt oluşmaktadır. Bundan sonra kullanıcı karşısına arıza bilgisi ile buna benzer işlerin geçmişini görüntüleyebileceği bir ekran çıkmaktadır. Kullanıcı tarafından yapılan işlemleri görüntüleyebildiği ekranın görüntüsü Resim 6.3.'te gösterilmiştir.

Arıza Tespit

İşlemde

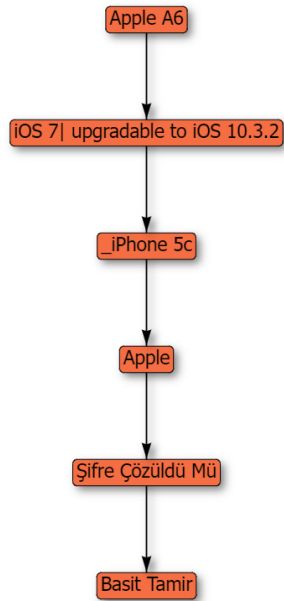
Sonuç

Marka	Model	İşletim Sistemi	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Arıza Sil
HTC	_One M8s	Android 5.0 (Lollipop)	... Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_I9500 Galaxy S4	Android 4.2.2 (Jelly Bean) upgradable to 5.0.1 (Lollipop)	... Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_Galaxy S5 LTE-A G906S	Android 4.4.2 (KitKat) upgradable to 6.0.1 (Marshmallow)	... Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_I9190 Galaxy S4 mini	Android 4.2.2 (Jelly Bean) upgradable to 4.4.2 (KitKat)	... Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil

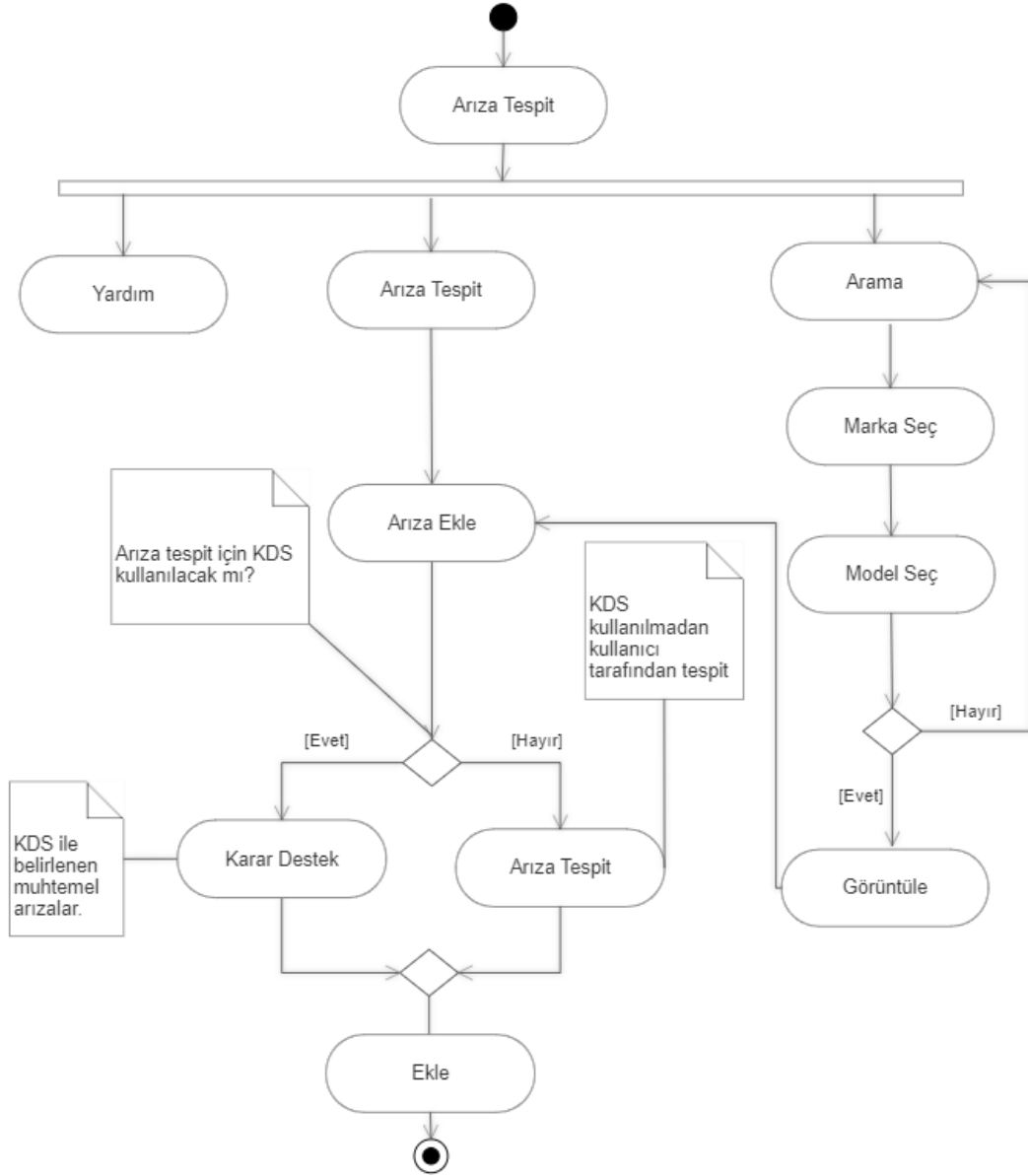
1

Resim 6.3. Kullanıcı tarafından yapılan işlemleri görüntüleyebildiği ekran

Bunların yanı sıra diğer karar destek sistemi olan yapılacak işlemlere ilişkin yol haritası da diyagram şeklinde kullanıcıya sunulmaktadır (Resim 6.4.). Kullanıcı imaj almak için gerçekleştirdiği işlemleri sisteme girmektedir. Bu sistemin yönlendirmesiyle veya kendisi tarafından olmakta bu veriyle birlikte işlemler neticesinde imaj alınıp alınmadığı bilgisini de sisteme girmektedir. Arıza tespiti sonrası işlemlere ilişkin aktivite diyagramı Şekil 9.12.'de gösterilmiştir.



Resim 6.4. Mobil cihazın imajının alınması için yapılacak işlem diyagramı (örnek)



Şekil 6.12. Yapılacak işlemlere ilişkin aktivite diyagramı

Tüm bu işlemler sonunda, kullanıcı şimdiye kadar yaptığı tüm işlemleri görebilmekte ve değerlendirme seçeneği ile hazırlanan karar destek sistemi yazılımına ilişkin geri bildirim verebilmektedir. Tüm yapılan işlemleri görüntüleyebildiği sonuç ekranı Resim 6.5.'te gösterilmiştir.

Arıza Tespit

İşlemede

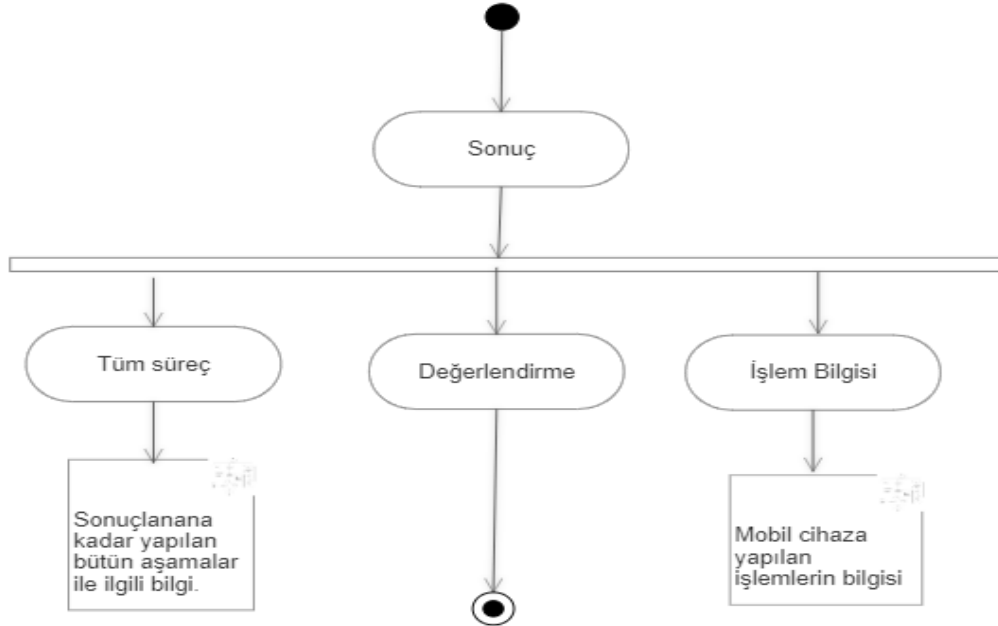
Sonuç

Tüm Değerlendirme Sonuçları

Marka	Model	İşletim Sistemi	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Arıza Sil
Samsung	_Galaxy Alpha	Android 4.4.4 (KitKat) upgradable to 5.0.2 (Lollipop)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Acer	_Iconia Tab 7 A1-713HD	Android 4.4.2 (KitKat)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Lenovo	_A2010	Android 5.1 (Lollipop)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
OnePlus	7pro	android	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Bbmobile	i1453	android	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Samsung	j810f	andorid	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Samsung	j810f	android 8.1	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil

Resim 6.5. Sonuç ekranı

Sonuç ekranında geri bildirimin yanında yaptığı her bir işleme ilişkin detayları ve o cihazla ilgili tüm süreci görüntüleyebilmektedir. Sonuç ekranına ilişkin aktivite diyagramı Şekil 6.13.'te gösterilmiştir.



Şekil 6.13. Sonuç ekranına ilişkin aktivite diyagramı

Yazılım, web tabanlı olarak hazırlanması sayesinde kullanımı, erişimi ve güncellemelerin uygulanması konusunda daha avantajlı hale gelmiştir. Kullanıcının mobil cihazlar ile ilgili vermesi gereken kararların kolaylaştırılması amaçlanmıştır. Böylelikle önceki kayıtlı veriler tecrübe niteliğinde kullanılmış ve bu tecrübe işleme girecek mobil cihaz için ilgili marka, ilgili model ve cihazın özellikleri göz önünde bulundurularak yapılması gereken işlemler konusunda kullanıcı sınırlanmadan yönlendirilme amaçlanmıştır.

Karar destek sistemi yazılımının son kullanıcı tarafından kullanılabilmesi için veri tabanları, yazılım ve arayüz hazırlanmıştır. Yazılımda personel mobil cihazın marka-model bilgilerini girmekte ve hafıza çipi, işletim sistemi gibi diğer özellikleri otomatik olarak gelmektedir. Bunun yanında cihazın arızası varsa ona ilişkin bilgileri de karar ağacı algoritmasına göre karşısına gelen sorularla belirlemektedir. Arıza tespitine ilişkin bu yöntemin özellikle yeni başlayan personel için faydalı olması beklenmektedir. Bunun yanı sıra personele kendisinin de el ile girebileceği bir alan mevcuttur. Tüm bu bilgileri girdiğinde ise karşısına belirlenen algoritmaya göre bir karar ağacı diyagramı çıkmaktadır. Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri EK-8’de gösterilmiştir.

6.6.Yazılımın Değerlendirilmesi İçin Soruların Belirlenmesi

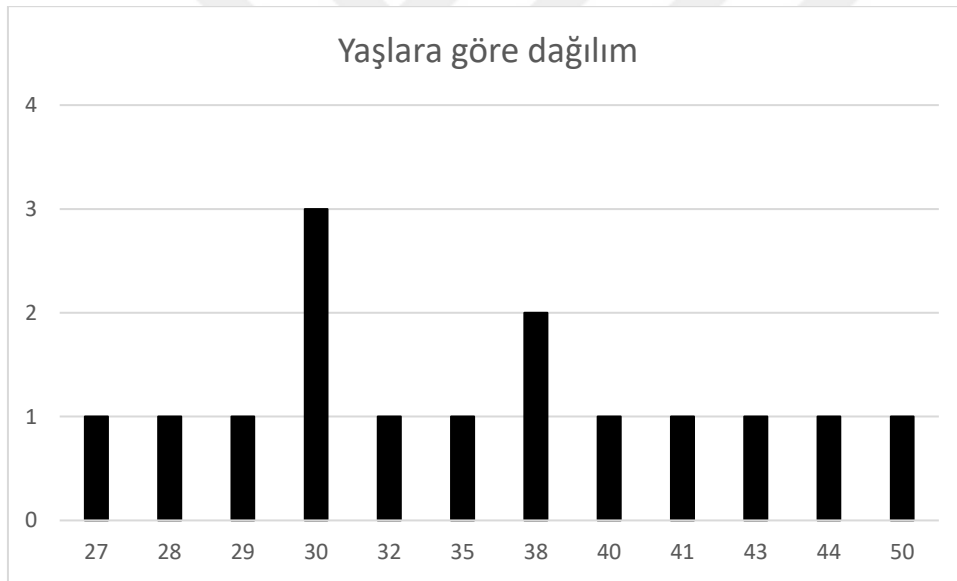
Yazılımın başarısının ölçülmesi için yazılımın kullanılması sonucunda kullanıcının karşısına bir geri bildirim ekranı tasarlanmasına karar verilmiştir. Geri bildirim ekranı için Sistem Kullanılabilirlik Ölçeği (System Usability Scale – SUS) ve uzman görüşlerinden yararlanılmasının uygun olacağı değerlendirilmiştir.

Brooke tarafından 1996 yılında geliştirilen Sistem Kullanılabilirlik Ölçeği, kullanıcılardan çabuk ve kolay bir değerlendirme elde edilmesi için kullanılmaktadır. Binlerce çalışmada uygulanan bu ölçek, 10 farklı soru içermektedir. Bu sorular (Bangor, Kortum ve Miller, 2008):

- “1. Bu sistemi sıklıkla kullanmak isteyeceğimi düşünmüyorum.
2. Sistemi gereksiz karmaşık buldum.
3. Sistemi, kullanımı kolay olarak düşündüm.
4. Sistemi kullanabilmek için teknik desteğe ihtiyacım olacağını düşünüyorum.
5. Sistemdeki çeşitli işlevlerin iyi entegre edildiğini fark ettim.

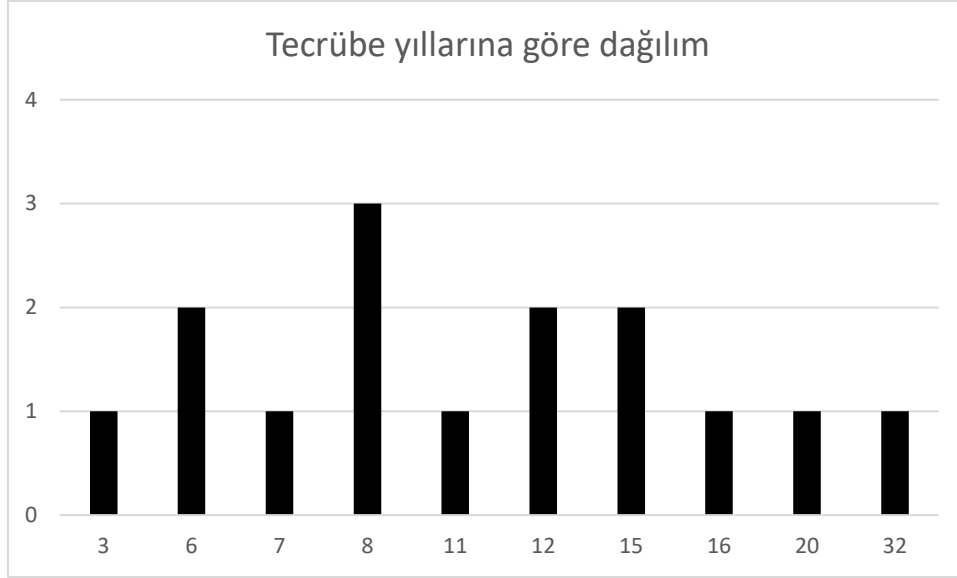
6. Bu sistemde çok fazla tutarsızlık olduğunu düşündüm.
7. Çoğu insanın bu sistemi kullanmayı çok çabuk öğreneceğini düşünüyorum.
8. Sistemi, kullanmak için çok hantal buldum.
9. Sistemi kullanırken kendime çok güveniyordum.
10. Bu sisteme geçmeden önce çok şey öğrenmem gerekti.” şeklindedir.

Bu soruların yanı sıra, geri bildirim ekranında hangi soruların cevaplanması gerektiği konusunda uzmanlardan talep edilmek üzere Türkçe ve yurtdışında yaşayanlar için İngilizce uzman görüş formu oluşturulmuştur (EK-9 ve EK-10). Almanya, Arnavutluk, Belçika, Hollanda, İsviçre, Kanada ve Romanya ülkelerinden birer uzman ve Türkiye’den bu alanda 8 uzman olmak üzere toplam 15 kişi ile görüşülmüştür. Bu uzmanların 14’ü erkek 1’i kadındır. Ayrıca yaş ortalaması 35,7 olup, yaşlara göre dağılımı Şekil 6.14’te gösterilmiştir.



Şekil 6.14. Uzmanların yaşlara göre dağılımı

Uzmanlıkları adli bilişim veya yazılım alanında olan bu uzmanların, uzmanlıklarındaki tecrübelerinin ortalaması 11,9 yıldır. Tecrübe yıllarına göre dağılımı Şekil 6.15.’te gösterilmiştir.



Şekil 6.15. Uzmanların tecrübe yıllarına göre dağılımı

Görüşülen uzmanların 3'ü özel sektörde faaliyet göstermekteyken; geriye kalan 12'si kamu sektöründe faaliyet göstermektedir. Bu uzmanların lisans, yüksek lisans veya doktora mezunu olduğu görülmüştür. Eğitim durumlarına göre dağılımı Şekil 6.16'da gösterilmiştir.



Şekil 6.16. Uzmanların eğitim durumlarına göre dağılımı

Uzmanlarla gerçekleştirilen görüşmeler neticesinde, Sistem Kullanılabilirlik Ölçeği de dikkate alınarak karar destek sistemi yazılımına ilişkin sorulması gereken sorular

belirlenmiştir. Bu sorular; kullanım kolaylığı, yazılımın anlaşılabilirliği ve sürece katkısını tespit etmeye yöneliktir.

Kullanım kolaylığına ilişkin olarak uzmanlarla görüşme neticesinde 5 farklı soru belirlenmiştir. Bunlar:

1. Yazılımın kullanımı kolay mıydı?
2. Yazılımın arayüzü basit ve kullanıcı dostu muydu?
3. Yazılımı teknik destek almadan kullanabildiniz mi?
4. Yazılımı rahatlıkla kullanabildiniz mi?
5. Programı kullanırken kaldığınız yerden devam, kayıt veya çıkış konularında sorun yaşadınız mı?

Yazılımın anlaşılabilirliği konusunda sorulması gereken sorularla ilgili olarak uzmanlarla gerçekleştirilen görüşmeler ve alınan dönüşler neticesinde 6 farklı soru belirlenmiştir. Bunlar:

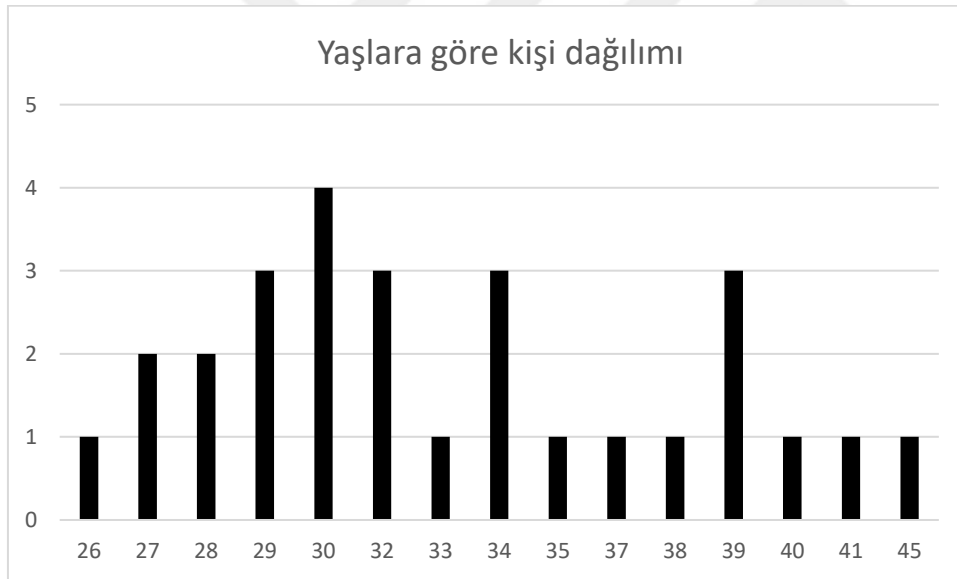
1. Yazılım gereksiz karmaşık mıydı?
2. Yazılımdaki işlevler bir bütün olarak anlaşılır mıydı?
3. Yazılımın kullanımına ilişkin başlık, yönlendirme, metinler gibi verilen bilgiler yeterli miydi?
4. Yazılımdaki metinlerde dilbilgisi ve anlam açısından bir sorunla karşılaştınız mı?
5. Yazılımın genel tasarımı (renk, renklerin uyumu, yazı tipi) ile ilgili bir sorun tespit ettiniz mi?
6. Kullanım kılavuzu ve ipuçları yeterli miydi?

Oluşturulan karar destek sistemi yazılımının mobil cihaz adli bilişimi sürecine olan katkısını ölçmek için nasıl bir soru sorulması gerektiği hakkında uzmanlarla görüşülmüştür. Bu görüşmeler neticesinde toplam 8 farklı soru tespit edilmiştir.

1. Yazılımın kullanılması sürecin hızlandırılmasına katkı sağladı mı?
2. Yazılımın kullanılması mobil cihaz imaj alma sürecine katkı sağladı mı?
3. Yazılımın kullanılması sırasında önerilen adımlar doğru ve tutarlı şekilde sizi yönlendirdi mi?
4. Yazılımın size katkıları göz önüne alındığında tekrar kullanır mısınız?

5. Yazılımın kullanılması sırasında önerilen adımlar mobil cihaz adli bilişimi sürecini kolaylaştırdı mı?
6. Yazılımda önerilen adımların nasıl yapılacağı konusunda öncesinde bir bilgilendirmeye ihtiyacınız var mıydı?
7. Bu yazılımın genel olarak iş yükünü hafifleteceğini düşünüyor musunuz?
8. Yeni başlayan personelin bu yazılımdan kolaylıkla faydalanabileceğini düşünüyor musunuz?

Belirlenen sorulardan sonra, Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğünde mobil cihaz incelemesi yapan personelden bu yazılımın kullanılması istenmiştir. Toplamda 28 farklı personel bu yazılımı kullanmıştır. Kullanan personelin 20'si erkek iken geriye kalan 8'i kadındır ve yaş ortalaması 33,1dir. Yaşlara göre kişi dağılımı Şekil 6.17.'de gösterilmiştir.



Şekil 6.17. Yaşlara göre kişi dağılımı



Şekil 6.18. Tecrübe yıllarına göre kişi sayısı

Yazılımı kullanan 28 kişinin 5'i yüksek lisans mezunu iken, 12'si lisans mezunudur. Geriye kalan 11 kişinin 9'u ön lisans ve 2'si lise mezunudur. Bu kişilerin adli bilişim alanındaki tecrübeleri çeşitlilik göstermektedir. En tecrübeli olan 11 yıllık tecrübeye sahip iken; en tecrübesiz olan 1 yıllık tecrübeye sahiptir. Bu 28 personelin tecrübelerinin ortalaması 5,4 yıldır. Tecrübeye göre dağılımı Şekil 6.18'de gösterilmiştir.



7. BULGULAR

7.1. Mobil Cihaz Adli Bilişimine Etki Eden Öznitelikler

Mobil cihazlar adli bilişim açısından diğer dijital materyal türlerine göre nicelik ve bulundurduğu veri açısından nitelik olarak ön plana çıkmaktadır. Bu çalışmada mobil cihaz adli bilişimi sürecinin en verimli ve etkili şekilde hızlandırması amacıyla bir karar destek sistemi tasarlanması hedeflenmektedir. Bu karar destek sisteminin veri kısmını oluşturmak için mobil cihazlarla ilgili olarak gerçekleştirilen adli bilişim işlemlerine ilişkin bazı verilerin toplanılması ihtiyacı doğmuştur. Hangi verilerin toplanacağını belirlemek için uzmanlarla görüşülmesine karar verilmiştir.

7.1.1. Mobil cihaz adli bilişimine etki eden öznitelikler konusunda uzman görüşleri

Mobil cihaza etki eden özniteliklerin tespiti amacıyla Türkiye’de ve diğer ülkelerde bu alandaki uzmanlarla görüşmeler gerçekleştirilmesi için hazırlanan Türkçe ve İngilizce uzman görüş formları kullanılmıştır (EK-1 ve EK-2). Almanya, Arnavutluk, Belçika, Kanada, Romanya ve İsviçre ülkelerindeki bulunan birer; Türkiye’den on beş uzman olmak üzere toplamda yirmi bir uzmanla görüşme gerçekleştirilmiştir.

Bu görüşmeler neticesinde mobil cihazlardan imaj alınmasına etki eden faktörlerin mobil cihaza ait bilgiler ve mobil cihazın durumuna ilişkin bilgiler olmak üzere iki kategori altında toplandığı görülmektedir. Cihaza ilişkin bilgiler; cihazın markası, modeli, işletim sistemi ve sürümü, hangi çip sete sahip olduğu gibi bilgilerden oluşmaktadır. Cihazın durumuna ilişkin bilgiler kısmında ise; cihazın şifreli olup olmadığı, ekran arızasının olup olmadığı, port arızasının olup olmadığı, anakart arızası olup olmadığı, cihazın parçalanıp parçalanmadığı, yazılımsal bir arızasının olup olmadığı bilgilerinden oluşmaktadır.

Uzmanlardan alınan görüşlerde cihaza ilişkin bilgilerden mobil cihazlardan imaj alınmasında mobil cihazın markasının önemli olduğunu %95,2’si; mobil cihazın modelinin önemli olduğunu ise %85,7’si belirtmiştir. Cihazın işletim sistemi ve hafıza çipi markasının önemli olduğunu ise görüşü alınan 21 uzmandan %90,5’ine denk gelen 19 uzman belirtmiştir.

Mobil cihazın durumuna ilişkin alınan uzman görüşleri, cihazın şifreli olma durumu için %90,5 iken; port arızası ve anakart arızası için %71,4'tür. Cihazda ekran arızası ve yazılımsal arıza bulunmasının imaj alınmasına etki ettiğini düşünen uzmanların oranı ise %66,7 iken; cihazın parçalanmış olmasının önemli olduğunu düşünen uzmanların oranı %76,2'dir.

7.1.2. Mobil cihaz adli bilişimine ilişkin toplanan verilerin analizi

Mobil cihaza ilişkin bilgiler, cihazın markası, modeli, işletim sistemi ve sürümü, hangi çip sete sahip olduğu bilgilerinden oluşmaktadır. Mobil cihazın elde edildiği ilk durumuna ilişkin bilgiler ise cihazın şifreli olup olmadığı, port arızasının olup olmadığı, anakart arızası olup olmadığı, cihazın parçalanıp parçalanmadığı ve yazılımsal bir arızasının olup olmadığı verilerinden oluşmaktadır.

Ayrıca karşılaşılan sorunların hangi yöntemle ile aşıldığının tespit edilmesi için cihaza yapılan işlemlerin de toplanması gerektiğine karar verilmiştir. Cihaza yapılan işlemler ise port değiştirilip değiştirilmediği, batarya değiştirilip değiştirilmediği, ekran değiştirilip değiştirilmediği, basit tamir işlemi yapılıp yapılmadığı, j-tag işlemi yapılıp yapılmadığı, chip-off işlemi yapılıp yapılmadığı, root işlemi yapılıp yapılmadığı, TWRP/CVM kurulumu yapılıp yapılmadığı ve kullanılan mobil cihaz adli bilişimi yazılımından oluşmaktadır. Bunlara ilave olarak hangi personel tarafından işlemin yapıldığı ve bu işlemlerin sonucunda imaj alınıp alınmadığı ait verileri de bu kategoride sayılmaktadır.

Üç temel kategoride belirlenen özniteliklere ilişkin verilerin toplanması için etik kurul başvurusu yapılmıştır. Gazi Üniversitesi Ölçme Değerlendirme Etik Alt Çalışma Grubu tarafından gerekli izinlerin alınması koşuluyla etik açıdan sakınca bulunmadığı kararı alınmıştır (EK-3). Gerekli izinler alınması talebiyle Emniyet Genel Müdürlüğünden yapılan başvuru olumlu sonuçlanmıştır (EK-4). Alınan izinler sonucunda mobil cihaz adli bilişimi faaliyeti gerçekleştiren EGM Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğü tarafından bir yıl süresince 1710 Adet akıllı telefon olan mobil cihaza ilişkin yapılan işlemlere ilişkin veriler toplanmıştır.

Bu çalışmada elde edilen veriler SPSS istatistik paket programı ile analiz edilmiş ve $p < 0,05$ anlamlı olarak kabul edilmiştir. İstatistiksel olarak veriler tanımlayıcı ve çıkarımsal istatistik bazında ele alınmıştır. Bu nedenle verilerin frekans dağılımları ele alınmış, anlamlı olan veriler değişik açılardan değerlendirilmeye tutulmuşlardır.

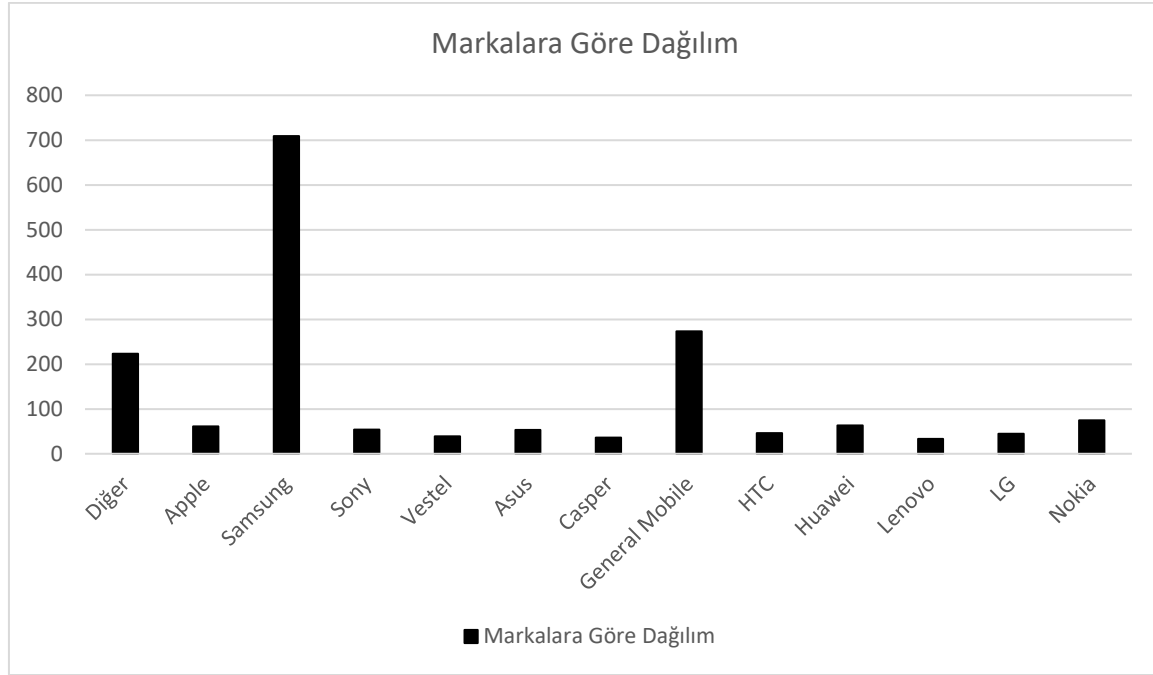
Tanımlayıcı istatistikler

Toplanan verilerin özetlenmesinden sonra, araştırma örneğinin tanıtılması veya daha iyi ifade edilmesi için hesaplanan değerlere tanıtıcı veya tanımlayıcı istatistikler denilmektedir. Tanımlayıcı istatistiklerin hesaplanmasıyla, çalışma konusu hakkında daha ayrıntılı bilgilere ulaşılmaktadır (Kocabaş, Özkan, ve Başpınar, 2013: 31). Tanımlayıcı istatistik analizi neticesinde veriler frekans (f) ve yüzdelik (%) olarak ifade edilmiştir. İstatiksel analiz için ise SPSS paket programı kullanılmıştır.

Çizelge 7.1. Cihaz markasına ilişkin frekans tablosu

Marka	f	%
Diğer	223	13,0
Apple	61	3,6
Samsung	709	41,5
Sony	54	3,2
Vestel	39	2,3
Asus	53	3,1
Casper	36	2,1
General Mobile	273	16,0
HTC	46	2,7
Huawei	63	3,7
Lenovo	33	1,9
LG	45	2,6
Nokia	75	4,4
Toplam	1710	100,0

Bu araştırmaya dâhil edilmiş 1710 cihazın markalarına ait frekans tablosu Çizelge 7.1.'de görüntülenmektedir. Görüldüğü üzere 61 adet Apple, 709 adet Samsung, 54 adet Sony, 39 adet Vestel, 53 adet Asus, 36 adet Casper, 273 adet General Mobile, 46 adet HTC, 63 adet Huawei, 33 adet Lenovo, 45 adet LG, 75 adet Nokia ve 223 adet diğer (Xiaomi, Oppo, Reeder, vb.) marka cihaz üzerinde inceleme yapılmıştır. Markaların sıklığı ise grafik olarak Şekil 7.1.'de gösterilmiştir.

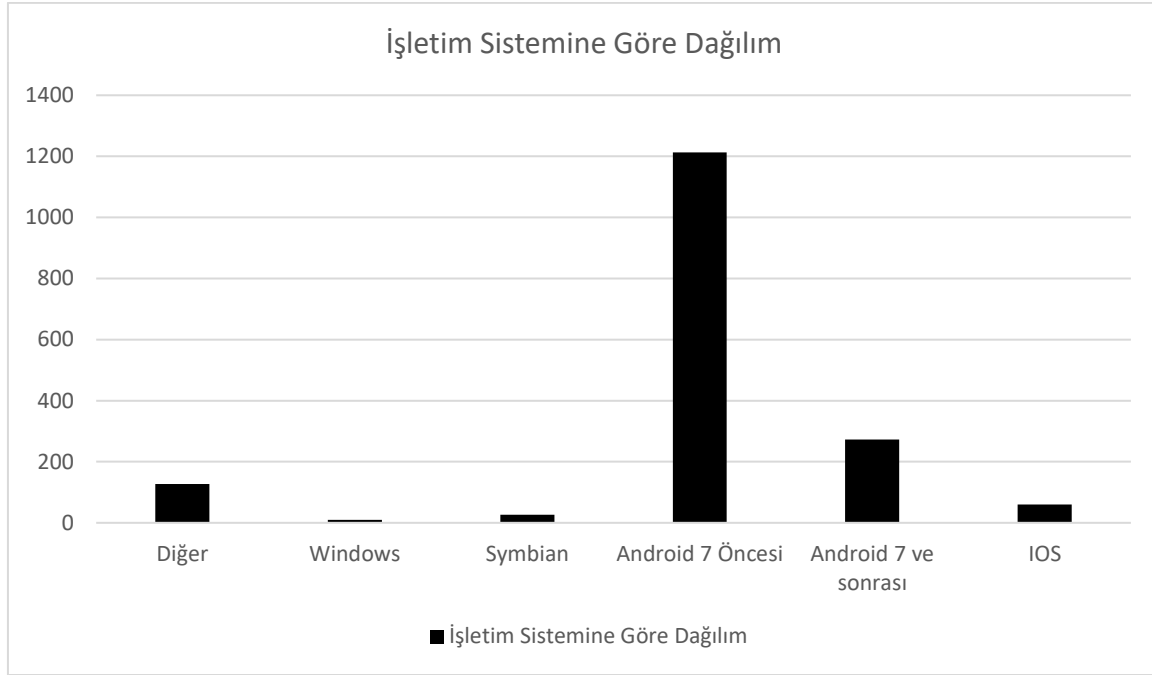


Şekil 7.1. Markaların sıklığına ilişkin grafik

Çizelge 7.2. İşletim sistemi sürümü frekans tablosu

İşletim sistemi	f	%
Diğer	127	7,4
Windows	10	0,6
Symbian	27	1,6
Android 7 Öncesi	1213	70,9
Android 7 ve sonrası	273	16,0
IOS	60	3,5
Toplam	1710	100,0

Çizelge 7.2.'de görüldüğü üzere incelenen cihazların %70,9'unun yani 1213 cihazın Android 7 öncesi versiyon işletim sistemine sahip olduğu görülmüştür. Bunu %16 ile Android 7 ve üstü versiyon işletim sistemine sahip cihazlar takip etmektedir. İşletim sistemi ve sürümüne ilişkin sıklık Şekli 7.2.'de gösterilmiştir.



Şekil 7.2. İşletim sistemi sıklık grafiği

Hafıza çipi markalarına ilişkin frekans tablosu Çizelge 7.3.'te gösterilmiştir. Buna göre en sık karşılaşılmış olan hafıza çipi markasının %27,7 ile Qualcomm olduğu; onu da %20,1 ile Exynos'un takip ettiği görülmüştür. Ayrıca incelenen cihazların 56 adedinin Apple marka hafıza çipine sahip olduğu, bunun tüm örnekleme %3,3 oranına sahip olduğu görülmüştür. 12 farklı değer ile ifade edilen hafıza çipi markalarının sıklığı Şekil 7.3.'te gösterilmiştir.

Çizelge 7.3. Hafıza çipi markası frekans tablosu

Hafıza çipi	f	%
Diğer	250	14,6
Apple	56	3,3
Spreadtrum	41	2,4
ARM Cortex	46	2,7
NovaThor	52	3,0
Qualcomm	474	27,7
Rockchip	39	2,3
Exynos	346	20,2
Kirin	35	2,0
Intel Atom	64	3,7
Marvell	37	2,2
MediaTek	270	15,8
Toplam	1710	100,0



Şekil 7.3. Hafıza çipi marka sıklığı

Bu 1710 cihazdan 260 adedinin şifreli olduğu görülmektedir. Bu sayı, araştırmaya dahil edilen materyalin %15,2'sini oluşturmaktadır. Çizelge 7.4.'te gösterilmiştir.

Çizelge 7.7.4. Cihazın şifreli olma durumuna ilişkin frekans tablosu

	f	%
Hayır	1450	84,8
Evet	260	15,2
Toplam	1710	100,0

Çizelge 7.5. Ekran arıza durumuna ilişkin frekans tablosu

	f	%
Hayır	1511	88,4
Evet	199	11,6
Toplam	1710	100,0

Bu 1710 cihazdan 199 adedinde ekran arızası olduğu görülmektedir. Bu sayı, araştırmaya dâhil edilen materyalin %11,6'sını oluşturmaktadır. Çizelge 7.5.'te gösterilmiştir.

Çizelge 7.6. Port arıza durumuna ilişkin frekans tablosu

	f	%
Hayır	1387	81,1
Evet	323	18,9
Toplam	1710	100,0

Bu 1710 cihazın 323 adedinde port arızası olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %18,9'una denk gelmektedir. Çizelge 7.6.'da gösterilmiştir.

Çizelge 7.7. Anakart arıza durumuna ilişkin frekans tablosu

	f	%
Hayır	1658	97,0
Evet	52	3,0
Toplam	1710	100,0

Bu 1710 cihazın 52 adedinde anakart arızası olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %3'üne denk gelmektedir. Çizelge 7.7.'de gösterilmiştir.

Çizelge 7.8. Cihazın parçalanmış olma durumuna ilişkin frekans tablosu

	f	%
Hayır	1662	97,2
Evet	48	2,8
Toplam	1710	100,0

Bu 1710 cihazın 48 adedinin parçalanmış olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %2,8'ine denk gelmektedir. Çizelge 7.8.'de gösterilmiştir.

Çizelge 7.9. Yazılımsal arızalı olma durumuna ilişkin frekans tablosu

	f	%
Hayır	1607	94,0
Evet	103	6,0
Toplam	1710	100,0

Bu 1710 cihazın 103 adedinde yazılımsal arıza olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %6'sına denk gelmektedir. Çizelge 7.9.'da gösterilmiştir.

Çizelge 7.10. Root ihtiyacı olma durumuna ilişkin frekans tablosu

	f	%
Hayır	1630	95,3
Evet	80	4,7
Toplam	1710	100,0

Bu 1710 cihazın 80 adedinin root ihtiyacı olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %4,7'sine denk gelmektedir. Geriye kalan 1630'unda bu ihtiyaç tespit edilmemiştir. Çizelge 7.10.'da gösterilmiştir.

Çizelge 7.11. Port değişimi durumuma ilişkin frekans tablosu

	f	%
Hayır	1683	98,4
Evet	27	1,6
Toplam	1710	100,0

Bu 1710 cihazın 27 adedinin port değişim ihtiyacı olduğu görülmüştür. Bu sayı araştırmaya dâhil edilen materyalin %1,6'sına denk gelmektedir. Çizelge 7.11.'de gösterilmiştir.

Çizelge 7.12. Batarya değişim durumuna ilişkin frekans tablosu

	f	%
Hayır	1698	99,3
Evet	12	0,7
Toplam	1710	100,0

Bu 1710 cihazın 12 adedinin batarya deęişim ihtiyacı olduęu görölmüştür. Bu sayı araştırmaya dâhil edilen materyalin %0,7'sine denk gelmektedir. Çizelge 7.12.'de gösterilmiştir.

Çizelge 7.13. Ekran deęişimi işlemine ilişkin frekans tablosu

	f	%
Hayır	1696	99,2
Evet	14	0,8
Toplam	1710	100,0

Toplamda 1710 cihazın 14 adedine ekran deęişim işlemi uygulanmıştır. Bu sayı araştırmaya dahil edilen materyalin %0,8'üne tekabül etmektedir. Çizelge 7.13.'te gösterilmiştir.

Çizelge 7.14. Basit tamir işlemine ilişkin frekans tablosu

	f	%
Hayır	1671	97,7
Evet	39	2,3
Toplam	1710	100,0

1710 cihazın 39 tanesi için basit tamir işlemi uygulanmıştır. Bu toplam sayının %2,3'üne karşılık gelmektedir. Geriye kalan 1671 tanesi için basit tamir işlemi uygulanmamıştır. Çizelge 7.14.'de gösterilmiştir.

Çizelge 7.15. J-tag işlemine ilişkin frekans tablosu

	f	%
Hayır	1708	99,9
Evet	2	0,1
Toplam	1710	100,0

1710 cihazın sadece 2 tanesi için j-tag işlemi uygulanmıştır. Geriye kalan 1708 tanesi için bu işlemin uygulanmadığı görölmüştür. Çizelge 7.15.'te gösterilmiştir.

Çizelge 7.16. Chip-off işlemine ilişkin frekans tablosu

	f	%
Hayır	1460	85,3
Evet	250	14,6
Toplam	1710	100,0

1710 cihazdan 250 adedine chip-off yöntemi uygulanmıştır. Bu sayı toplam cihazların %14,6'sına denk gelmektedir. Çizelge 7.16.'da gösterilmiştir.

Çizelge 7.17. Root işlemine ilişkin frekans tablosu

	f	%
Hayır	1632	95,4
Evet	78	4,6
Toplam	1710	100,0

1710 cihazdan 78 adedi için root işlemi uygulandığı görülmüştür. Bu sayı toplam cihazların %4,6'sına denk gelmektedir. Çizelge 7.17.'de gösterilmiştir.

Çizelge 7.18. İmaj alma işlemi sonucuna ilişkin frekans tablosu

	f	%
Hayır	313	18,3
Evet	1397	81,7
Toplam	1710	100,0

Bu 1710 cihazdan marka, model, yazılım veya diğer değişkenleri gözetmeksizin 1397 adedinin imajının alınabildiği gözlemlenmiştir. Bu sayı araştırmaya dâhil edilen toplam materyalin %81,7'ine denk gelmektedir. Çizelge 7.18.'de görülmektedir.

Çıkarımsal istatistikler

Ki-kare (Chi-square) testi, uygulama kolaylığı sebebiyle istatistiksel araştırmalarda çokça başvurulan bir yöntemdir (Kalaycı, 2006: 85). Mobil cihazlardan adli kopya alma işlemi ile cihazın batarya değişimi, yazılımsal arızası olup olmadığı gibi durumlar arasında bir ilişki olup olmadığı ki-kare analizi ile araştırılmıştır.

Ki-kare analiz yöntemiyle ilişkilerin saptanmasının yanı sıra, değişkenlerin birbirinden farklılıkların tespiti için de kullanılması mümkündür. Ki-kare analizi, dağılımlar üzerinden çalışan bir analiz yöntemidir. Bu yöntemle yapılan testlerde iki değişkenin bağımsız olması,

aralarında bir ilişkinin yokluğunu ifade etmektedir. Değişkenlerin bağımsızlığını ölçmek için en sık kullanılan yöntemlerden birisi de Ki-kare testidir. Ki-kare analiz yönteminin özelliklerinden olan serbestlik derecesi artması, normal dağılıma benzemeyi ifade etmektedir. Bunun yanı sıra serbestlik derecesi Ki-kare değerini doğrudan etkilediğinden, gözlem sayısındaki artış Ki-kare değerini etkilemektedir. Bunun sonucunda farklılıkların anlamlı olup olmadığına ilişkin göstergelerin elde edilme ihtimali de artmaktadır. Ki-kare analiz yöntemi, iki değişken arasındaki ilişkinin bir sistem içerisinde mi sorusunu cevaplamayı sağlar. Sonuç olarak Ki-kare analiz yöntemi, bir çapraz tablodaki birden fazla değişkenin ilişkisinin istatistiksel açıdan anlamlı olup olmadığının test edilmesi için kullanılmaktadır (Kalaycı, 2006: 116).

Araştırma yapılan konuyla ilgili iddia edilen; ancak doğruluğu henüz ispatlanamamış olan görüşlere hipotez denilmektedir. Hipotezler üzerinde, doğruluğunu belirlemeye yönelik gerçekleştirilen testlere hipotez testi denilmektedir. Temel iddia, başlangıç hipotezi de olarak bilinen ve H_0 ile gösterilen sıfır, başlangıç veya farksızlık hipotezidir. Elde edilen sonuçlar da sıfır hipotezi sorgulanıyorsa, kıyas olarak öne sürülen hipotez ise Mevcut veriler sıfır hipotezinin doğruluğu hakkında şüphe uyandırdığında kıyas yapmak için ortaya sunulan ikinci hipotez H_A olarak da gösterilen alternatif hipotezdir. Elde edilen sonuçlara göre H_0 yanlış çıkarsa, bu durumda alternatif hipotez olan H_A 'nın kabulü anlamına gelir (Kalaycı, 2006: 65).

Bu bölümde mobil cihazlardan imaj alınmasına cihazın durumuyla birlikte arızaların etkisinin tespiti amaçlanmıştır. Kategorik değişkenler olan imaj alınmasının sonucuyla, cihazın markası, hafıza çipi markası, işletim sistemi ve şifreli olma durumu arasındaki ve anakart arızası, ekran arızası, port arızası, yazılımsal arıza ve cihazın parçalanmış olma durumu arasındaki ilişkileri araştırmak için Ki-kare testi kullanılmış ve güven düzeyi %95 olarak analizler yapılmıştır.

Çizelge 7.19. Anakart arızası ve sonuca ilişkin çapraz tablo

			Sonuç		Toplam
			Alınamadı	Alındı	
Arıza	Adet	Adet	1410	248	1658
		% Arıza durumunda	85,0%	15,0%	100,0%
	Adet	Adet	52	0	52
		% Arıza durumunda	100,0%	0,0%	100,0%
Toplam	Adet		1462	248	1710
	% Arıza durumunda		85,5%	14,5%	100,0%

Cihazlarda anakart arızası olup olmaması ve imaj alma işlemi sonucuna ait Çizelge 7.19. incelendiğinde, anakart arızası bulunan cihazların tamamından olumlu sonuç alınmadığı, anakart arızası bulunmayan cihazların ise %85'inden sonuç alındığı gözlemlenmiştir. Cihazlarda anakart arızası olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H_0 : Cihazlarda anakart arızası olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H_1 : Cihazlarda anakart arızası olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H_0 Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihazlarda anakart arızası olup olmamasına göre farklılık göstermektedir denilebilir.

Çizelge 7.20. Cihazın markası ve sonuca ilişkin çapraz tablo

			Sonuç		Toplam
			Alınamadı	Alındı	
Cihazın Markası	Diğer	Adet	61	162	223
		% Bu markada	27,4%	72,6%	100,0%
	Apple	Adet	28	33	61
		% Bu markada	45,9%	54,1%	100,0%
	Samsung	Adet	83	626	709
		% Bu markada	11,7%	88,3%	100,0%
	Sony	Adet	7	47	54
		% Bu markada	13,0%	87,0%	100,0%
	Vestel	Adet	8	31	39
		% Bu markada	20,5%	79,5%	100,0%
	Asus	Adet	7	46	53
		% Bu markada	13,2%	86,8%	100,0%
	Casper	Adet	12	24	36
		% Bu markada	33,3%	66,7%	100,0%
	General Mobile	Adet	61	212	273
		% Bu markada	22,3%	77,7%	100,0%
	HTC	Adet	13	33	46
		% Bu markada	28,3%	71,7%	100,0%
	Huawei	Adet	4	59	63
		% Bu markada	6,3%	93,7%	100,0%
	Lenovo	Adet	3	30	33
		% Bu markada	9,1%	90,9%	100,0%
	LG	Adet	6	39	45
		% Bu markada	13,3%	86,7%	100,0%
	Nokia	Adet	20	55	75
		% Bu markada	26,7%	73,3%	100,0%
Toplam		Adet	313	1397	1710
		% Toplam	18,3%	81,7%	100,0%

Cihazların markası ve imaj alma işlemine ait Çizelge 7.20.'deki çapraz tablo görüntülendiğinde, Samsung marka cihazların %88,3'ünden olumlu sonuç alındığı, Apple marka cihazların %.45,9'unda sonuç alınmadığı gözlemlenmiştir. En düşük başarılı imaj alma oranı %54,1 ile Apple marka cihazlardır. Çalışmaya dahil edilen cihazların %81,7 sinin imajının alındığı gözlemlenmiştir.

Cihazların markası ve imaj alma işlemi arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazın markası ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazın markası ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H₀ Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihaz markasına göre farklılık göstermektedir denilebilir.

Çizelge 7.21. Cihazın parçalanmış olma durumu ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
Arıza	Adet	Adet	302	1360	1662
		% Arıza durumunda	18,2%	81,8%	100,0%
	Adet	Adet	11	37	48
		% Arıza durumunda	22,9%	77,1%	100,0%
Toplam	Adet		313	1397	1710
	% Arıza durumunda		18,3%	81,7%	100,0%

Cihazların parçalanmış olup olmaması ve imaj alma işlemi sonucuna ait Çizelge 7.21.'deki çapraz tablo görüntülendiğinde, parçalanmış cihazların %77,1'inden imaj alınabildiği görülmüştür. Öte yandan parçalanmamış cihazların ise %81,8'inde olumlu sonuç alındığı gözlemlenmiştir. Cihazların parçalanmış olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazın parçalanmış olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazın parçalanmış olup olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten büyük olduğu için H₀ Hipotezi reddedilemez. Yani cihazların imaj alma işlem sonuçları cihazların parçalanmış olup olmamasına göre farklılık göstermemektedir denilebilir.

Çizelge 7.22. Cihazın şifreli olma durumu ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
Şifreli olma durumu	Hayır	Adet	232	1218	1662
		% Arıza durumunda	16,0%	84,0%	100,0%
	Evet	Adet	81	179	48
		% Arıza durumunda	31,2%	68,8%	100,0%
Toplam	Adet		313	1397	1710
	% Arıza durumunda		18,3%	81,7%	100,0%

Cihazların şifreli olup olmaması ve imaj alma işlemi sonucuna ait çapraz tablo görüntülendiğinde, şifreli cihazların %68,8 inden olumlu sonuç alındığı, şifresiz cihazların ise %.84,4'ünde sonuç alındığı gözlemlenmiştir. Çizelge 7.22.'de görülmektedir.

Cihazların şifreli olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazın şifreli olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazın şifreli olup olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H₀ Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihazların şifreli olup olmamasına göre farklılık göstermektedir denilebilir.

Çizelge 7.7.23. Cihazın ekran arızası olma durumu ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
Arıza	Hayır	Adet	240	1271	1662
		% Arıza durumunda	15,9%	84,1%	100,0%
	Evet	Adet	73	126	48
		% Arıza durumunda	36,7%	63,3%	100,0%
Toplam	Adet		313	1397	1710
	% Arıza durumunda		18,3%	81,7%	100,0%

Cihazlarda ekran arızası olup olmaması ve imaj alma işlemi sonucuna ait Çizelge 7.23'deki çapraz tablo görüntülendiğinde, ekran arızası bulunan cihazların %63,2'sinden olumlu sonuç

alındığı, ekran arızası bulunmayan cihazların ise %84,1'inden sonuç alındığı gözlemlenmiştir.

Cihazlarda ekran arızası olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H_0 : Cihazlarda ekran arızası olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H_1 : Cihazlarda ekran arızası olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H_0 Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihazlar da ekran arızası olup olmamasına göre farklılık göstermektedir denilebilir.

Çizelge 7.24. Hafıza çipi markası ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
Hafıza Çipi Markası	Diğer	Adet	82	168	250
		% Bu markada	32,8%	67,2%	100,0%
	Apple	Adet	25	31	56
		% Bu markada	44,6%	55,4%	100,0%
	Spreadtrum	Adet	4	37	41
		% Bu markada	9,8%	90,2%	100,0%
	ARM Cortex	Adet	25	21	46
		% Bu markada	54,3%	45,7%	100,0%
	NovaThor	Adet	2	50	52
		% Bu markada	3,8%	96,2%	100,0%
	Qualcomm	Adet	55	419	474
		% Bu markada	11,6%	88,4%	100,0%
	Rockchip	Adet	12	27	39
		% Bu markada	30,8%	69,2%	100,0%
Toplam	Exynos	Adet	40	306	346
		% Bu markada	11,6%	88,4%	100,0%
	Kirin	Adet	2	33	35
		% Bu markada	5,7%	94,3%	100,0%
	Intel Atom	Adet	20	44	64
		% Bu markada	31,3%	68,8%	100,0%
	Marvell	Adet	2	35	37
		% Bu markada	5,4%	94,6%	100,0%
	MediaTek	Adet	44	226	270
		% Bu markada	16,3%	83,7%	100,0%
		Adet	313	1397	1710
		% Toplam	18,3%	81,7%	100,0%

Cihazların hafıza çipi markası ve imaj alma işlemi sonuçlarına ait Çizelge 7.24.'teki çapraz tablo görüntülendiğinde, hafıza çipi markası bilinmeyen cihazların %67,2'sinden olumlu sonuç alındığı, yine MediaTek hafıza çipi markaya sahip cihazların %.83,7'sinde sonuç alındığı gözlemlenmiştir. En sık karşılaşın Qualcomm hafıza çiplerindeki başarılı imaj alma oranının %88,4 olduğu görülmüştür.

Cihazların hafıza çipi markası ve imaj alma işlemi arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazın hafıza çipi markası ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazın hafıza çipi markası ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. Değeri=0,004 yani 0,05'ten küçük olduğu için H₀ Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihaz hafıza çipi markasına göre farklılık göstermektedir denilebilir.

Çizelge 7.25. Cihazın işletim sistemi ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
İşletim Sistemi	Diğer	Adet	42	85	127
		% Bu işletim sisteminde	33,1%	66,9%	100,0%
	Windows	Adet	5	5	10
		% Bu işletim sisteminde	50,0%	50,0%	100,0%
	Symbian	Adet	8	19	27
		% Bu işletim sisteminde	29,6%	70,4%	100,0%
	Android 7 Öncesi	Adet	187	1026	1213
		% Bu işletim sisteminde	15,4%	84,6%	100,0%
	Android 7 ve sonrası	Adet	43	230	273
		% Bu işletim sisteminde	15,8%	84,2%	100,0%
IOS		Adet	28	32	60
		% Bu işletim sisteminde	46,7%	53,3%	100,0%
Toplam		Adet	313	1397	1710
		% Toplam	18,3%	81,7%	100,0%

Cihazların işletim sistemi ve imaj alma işlemi sonuçlarına ait çapraz tablo görüntülendiğinde, işletim sistemi Windows olan cihazların %50'sinden olumlu sonuç alındığı, iOS işletim sistemine sahip cihazların %.46,7'sinden sonuç alınmadığı gözlemlenmiştir. En sık karşılaşılan Android işletim sisteminde Android 7'ye kadar %84,6, Android 7'den sonra ise %84,2 oranında başarılı imaj alınmıştır. Çizelge 7.25.'te gösterilmiştir.

Cihazların işletim sistemi ve imaj alma işlemi arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazın işletim sistemi ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazın işletim sistemi ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H₀ Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları işletim sistemlerine göre farklılık göstermektedir denilebilir.

Çizelge 7.26. Cihazın port arızası olma durumu ve sonuca ilişkin çapraz tablo

			Sonuç		
			Alınamadı	Alındı	Toplam
Arıza	Hayır	Adet	216	1171	1387
		% Arıza durumunda	15,6%	84,4%	100,0%
	Evet	Adet	97	226	323
		% Arıza durumunda	30,0%	70,0%	100,0%
Toplam	Adet		313	1397	1710
	% Arıza durumunda		18,3%	81,7%	100,0%

Cihazlarda port arızası olup olmaması ve imaj alma işlemi sonucuna ait Çizelge 7.26.'da yer alan çapraz tablo görüntülendiğinde, port arızası bulunan cihazların %70'inden olumlu sonuç alındığı, port arızası bulunmayan cihazların ise %84,4'ünden olumlu sonuç alındığı gözlemlenmiştir.

Cihazlarda port arızası olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H₀: Cihazlarda port arızası olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H₁: Cihazlarda port arızası olup olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H₀ Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihazlarda port arızası olup olmamasına göre farklılık göstermektedir denilebilir.

Çizelge 7.27. Cihazın yazılımsal arıza durumu ve sonuca ilişkin çapraz tablo

			Sonuç		Toplam
			Alınamadı	Alındı	
Arıza	Hayır	Adet	262	1345	1607
		% Arıza durumunda	16,3%	83,7%	100,0%
	Evet	Adet	51	52	103
		% Arıza durumunda	49,5%	50,5%	100,0%
Toplam	Adet		313	1397	1710
	% Arıza durumunda		18,3%	81,7%	100,0%

Cihazların yazılımsal arızası olup olmaması ve imaj alma işlemi sonucuna ait Çizelge 7.27.'deki göre çapraz tablo görüntülendiğinde, yazılımsal arızası bulunan cihazların %50,5'inden olumlu sonuç alındığı, yazılımsal arızası bulunmayan cihazların ise %83,7'sinden sonuç alındığı gözlemlenmiştir.

Cihazlarda yazılımsal arızası olup olmaması ve imaj alma işlemi sonucu arasında anlamlı bir ilişki olup olmadığı araştırılmak istenmektedir. Çalışma sonuçları aşağıdaki gibidir.

H_0 : Cihazlarda yazılımsal arızası olup olmaması ve imaj alma işlemi sonuçları arasında fark yoktur.

H_1 : Cihazlarda yazılımsal arızası olmaması ve imaj alma işlemi sonuçları arasında fark vardır.

Tüm varsayımlar yerine getirildiğinden Pearson Chi-Square test sonucu değerlendirilir. Sig. değeri 0,05'ten küçük olduğu için H_0 Hipotezi kabul edilemez. Yani cihazların imaj alma işlem sonuçları cihazlarda yazılımsal arızası olup olmamasına göre farklılık göstermektedir denilebilir.

7.1.3. Mobil cihaz adli bilişimine etki eden özneliliklerin önemleri

Mobil cihaz adli bilişimine etki eden öznelilikler tespit edildikten sonra, veriler toplanmıştır. Bu veriler üzerinden en başarılı algoritmanın tespiti için bazı testlere tabi tutulmuştur. Gerçekleştirilen testler neticesinde en başarılı algoritmanın karar ağacı algoritması olduğu sonucuna ulaşılmıştır. Bunun üzerine yazılıma uygulanması sonucunda karar ağacı

algoritmalarından ID3 algoritması ile % 98,83'lük bir orana ulaşılmıştır. ID3 algortitması kullanımı sonucunda özniteliklerin önem düzeylerine ilişkin tablo Çizelge 7.28'de gösterilmiştir.

Çizelge 7.28. Özniteliklerin önem düzeyleri

ÖZNİTELİK	ÖNEM DÜZEYİ
Batarya değişimi	0,000
Basit tamir	0,002
XRY yazılımı kullanımı	0,003
Ekran değişimi	0,005
İşletim sistemi sürümü	0,006
Cihaz parçalanma durumu	0,008
Hafıza çipi markası	0,011
Port değişimi	0,013
Ekran arızası	0,015
Chip-off işlemi	0,017
Diğer adli bilişim yazılımlarının kullanımı	0,018
J-tag işlemi	0,020
Root işlemi	0,022
Cihazın markası	0,023
Root ihtiyacının tespiti	0,024
Port arızasının tespiti	0,029
Yazılımsal arızanın tespiti	0,033
UFED yazılımının kullanımı	0,035
Anakart arızasının tespiti	0,036
TWRP/CVM kurulumu	0,093
Şifre kırma işleminin uygulanması	0,173
Cihazın şifreli olma durumu	0,369

Bu sınıflandırma algoritması sonucunda mobil cihazların imajlarının alınmasında en önemli özneliliğin 0,369 değeriindeki önem düzeyi ile cihazın şifreli olma durumu olduğu tespit edilmiştir. Cihaza ait bilgilerden ise en önemli özneliliğin ise 0,023 değeriindeki önem düzeyi ile cihazın markası olduğu anlaşılmıştır.

7.2. Mobil Cihaz Adli Bilişimi Kapsamında İmaj Alma Sürecine İlişkin Karar Destek Sisteminden Beklentiler

7.2.1. Karar destek sistemi yazılımı için müşterinin sesi ve önem düzeyleri

Yazılımın tüketicisi olarak kabul edilen mobil cihaz adli bilişim personeliyle görüşmeler gerçekleştirilerek müşterinin sesine ulaşılması hedeflenmiştir. Bu yazılımı kullanması

beklenen 29 personel ile görüşme yapılmıştır. Bu personel ile “Müşterinin Sesi Tespiti İçin Görüşme Formu” (EK-5) kullanılarak yüz yüze görüşmeler gerçekleştirilmiştir.

Gerçekleştirilen görüşmeler neticesinde mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için sekiz farklı talepte bulunulmuştur. Bunlar yazılımın anlaşılır olması, kullanımının kolay olması, kendi performansının izlenilebilmesi, cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi, cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi, benzer durumla karşılaşmış kişinin görüntülenebilmesi, açıklama verisi girme imkânı olması ve yöntemin nasıl yapılacağı konusunda bilgi vermesidir.

Elde edilen talepler için 1-9 arasında önem düzeyleri belirlenmesi istenmiştir. Her bir talep için 29 kişiden alınan önem düzeylerinin ortalaması ile o talebin önem düzeyi belirlenmiştir. Talepler için belirlenen önem düzeyleri Çizelge 7.29.’daki gibidir.

Çizelge 7.29. Talepler ve önem düzeyleri

Talepler	Önem Düzeyi
Kendi performansının izlenilebilmesi	7,72
Kullanımının kolay olması	7,52
Yazılımın anlaşılır olması	7,52
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	7,14
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	7,38
Açıklama verisi girme imkânı olması	8,10
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45

Kendi performansının izlenilebilmesi konusunda görüşülen 29 kişinin verdiği önemin ortalaması 7,72’dir. Kullanımının kolaylığı ve anlaşılabilirliği konusundaki önem düzeyi ise 7,52’dir. Cihaz bilgileri girilirken verilerin otomatik gelmesi için önem düzeyi 7,14 iken; cihazda herhangi bir arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesinin önem düzeyi 6,10’dur. Karşılaşılan cihaz ve arızasına benzer durumla karşılaşmış kişinin görüntülenebiliyor olması 7,38 iken, yöntemin nasıl yapılacağı konusunda bilgi vermesi 7,45’tir. Gerçekleştirilen görüşmeler neticesinden en fazla önem düzeyi 8,10 ile açıklama verisinin girilme imkanının olması talebinde olduğu görülmüştür.

7.2.2. Karar destek sistemi yazılımı için müşterinin sesi ve önem düzeylerinin karşılanması için teknik gereksinimler

Müşterinin sesine ulaşıldıktan sonra elde edilen sekiz talebin karşılanabilmesi için, dokuz farklı teknik gereksinime karar verilmiştir. Belirlenen teknik gereksinimler, Çizelge 7.30.'da gösterilmiştir.

Çizelge 7.30. Teknik Gereksinimler

Teknik Gereksinimler
İstatistik ekranı
Sade arayüz
Kullanım ipuçları
Web tabanlı yazılım
Listbox kullanılması
Textbox kullanılması
Karar ağacı diyagramı
Mobil cihazlar için veri tabanı
Yapılan işlemlere ilişkin veri tabanı

Bunlar sade arayüz, kullanım ipuçları, web tabanlı yazılım, veri girişi için listbox (veriyi el ile girmek yerine bir listeden seçilmesi) kullanılması, textbox (serbestçe metin girilebilecek alan) olması, karar ağacı diyagramı çıktı vermesi ve istatistik ekranı olarak belirlenmiştir. Ayrıca karar destek sistemine veri tabanı eklenmesi için mobil cihazlara ilişkin bazı verilerin bulunduğu “back4app” isimli internet sitesinden yararlanılmasına karar verilmiştir. Bu veri tabanı sayesinde mobil cihazlara ilişkin bilgilerin otomatik olarak gelmesi sağlanmıştır.

Toplanan verilerle yapılan işlemlere ilişkin de veri tabanı oluşmuştur. Bu sayede benzer işleri yapan personel bilgilerin de kullanıcıya sunulması mümkün hale getirilmiştir. Buna ilave olarak mobil cihaz adli bilişimi kapsamında imaj alma sürecine ilişkin karar destek sistemi kullanımı sırasında yapılan işlemler kayıt altına alınmakta ve bunun veri tabanını geliştirmesi hedeflenmektedir.

7.2.3. Karar destek yazılımının değerlendirilmesi

Yazılımın değerlendirilmesine ilişkin soruların belirlenmesinden sonra Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğünde mobil cihaz incelemesi yapan personelden bu yazılımın kullanılması istenmiştir. Toplamda 28 farklı personel bu yazılımı kullanmıştır. Yazılım kullanım kolaylığı, yazılımın

anlaşılabilirliği ve yazılımın mobil cihaz adli bilişimi sürecine katkısı olmak üzere üç farklı kategoride toplam 19 soru sorulmuştur.

Yazılımın kullanım kolaylığına ilişkin toplamda beş farklı soru sorulmuştur. Bu sorular yazılımı kullanımının kolaylığı ve rahatlığı, arayüzün basitliği, destek almadan kullanımı ile kullanım esnasındaki kaydetme ve çıkış konularına ilişkindir.

“Yazılımın kullanımı kolay mıydı?” sorusuna 28 kişiden 24’ü kolay olduğu yönünde cevap vermiştir. Bu toplam sayının %85,7’sine denk gelmektedir. Kolay olmadığını belirten 4 kişinin oranı ise %14,3’tür.

“Yazılımın arayüzü basit ve kullanıcı dostu muydu?” sorusuna 28 kişiden 27’si evet cevabını vermiştir. Toplam sayının %96,4’üne tekabül etmektedir. Sadece bir kişi yazılımın arayüzünün basit ve kullanıcı dostu olmadığını beyan etmiştir.

“Yazılımı teknik destek almadan kullanabildiniz mi?” sorusu karşısında 28 kişinin 18’i destek almadan kullanabildiğini beyan etmiştir. Bu toplam sayının %64,3’üne denk gelmektedir. %36,7’sine denk gelen 10 kişi ise yazılımı ancak teknik destek alarak kullandıklarını beyan etmiştir.

“Yazılımı rahatlıkla kullanabildiniz mi?” sorusuna 28 kişinin 22’si olumlu cevap vermiştir. Bu %78,6’lık bir orana denk gelmektedir. Geriye kalan 6 kişi rahatlıkla kullanamadığını beyan etmiştir.

“Programı kullanırken kaldığınız yerden devam, kayıt veya çıkış konularında sorun yaşadınız mı?” sorusuna 28 kişiden %17,9’una denk gelen 5 kişi sorun yaşadığını belirtmiştir. Geriye kalan 23 kişi sorun yaşamadan kullanabildiğini beyan etmiştir. Bu da toplam kullanıcıların %82,1’ine denk gelmektedir.

Yazılımın kullanım kolaylığına ilişkin sorulan sorulara alınan cevaplar neticesinde yazılımı kullanmanın kolay olduğu anlaşılmıştır. Sorulan 5 soruya alınan cevaplara ve oranlarına ilişkin tablo Çizelge 7.31’de gösterilmiştir.

Çizelge 7.31. Yazılımın kullanım kolaylığına ilişkin sorular ve cevaplar

		f	%
Yazılımın kullanımı kolay mıydı?	Hayır	4	14,3
	Evet	24	85,7
Yazılımın arayüzü basit ve kullanıcı dostu muydu?	Hayır	1	3,6
	Evet	27	96,4
Yazılımı teknik destek almadan kullanabildiniz mi?	Hayır	10	35,7
	Evet	18	64,3
Yazılımı rahatlıkla kullanabildiniz mi?	Hayır	6	21,4
	Evet	22	78,6
Programı kullanırken kaldığınız yerden devam, kayıt veya çıkış konularında sorun yaşadınız mı?	Hayır	23	82,1
	Evet	5	17,9
	Toplam	28	100,0

Yazılımın anlaşılabilirliği ile ilgili olarak toplam altı farklı soru kullanan personele yöneltilmiştir. Bu sorular karmaşıklığı, yazılımın işlevlerinin anlaşılması, kullanma kılavuzu ile yazılımdaki metinler, dilbilgisi ve tasarıma ilişkindir.

“Yazılımın gereksiz karmaşık mıydı?” sorusunu 28 kişi cevaplamıştır. Bunların 78,6%’sına denk gelen 22 kişi olumsuz cevap verirken; geriye kalan %21,4’üne denk gelen 6 kişi gereksiz karmaşık olduğu şeklinde geri bildirimde bulunmuştur.

“Yazılımdaki işlevler bir bütün olarak anlaşılır mıydı?” sorusunu cevaplayan 28 kişiden 25’i işlevleriyle bir bütün olarak anlaşılır olduğunu belirtmiştir. Anlaşılır olduğunu düşünen %89,3’lük kısma karşılık, %10,7’ye denk gelen 3 kişi yazılımın işlevlerini bir bütün olarak anlama konusunda sorun yaşadığını belirtmiştir.

“Yazılımın kullanımına ilişkin başlık, yönlendirme, metinler gibi verilen bilgiler yeterli miydi?” sorusuna 28 kişiden 25’i yeterli olduğunu belirtmiştir. Bu toplam sayının %89,3’üne denk gelmektedir. Geriye kalan %10,7’ye karşılık gelen 3 kişi ise yazılımda yer alan başlık, yönlendirme metin gibi bilgilerin yeterli olmadığını belirtmiştir.

“Yazılımdaki metinlerde dilbilgisi ve anlam açısından bir sorunla karşılaştınız mı?” sorusuna 28 kişiden 26’sı herhangi bir sorunla karşılaşmadığını belirtmiştir. Bu oran olarak %92,9’a denk gelmektedir. Yüzdelik olarak %7,1’e denk gelen 2 kişi ise dilbilgisi ve anlam açısından sorunla karşılaştığını belirtmiştir.

“Yazılımın genel tasarımı (renk, renklerin uyumu, yazı tipi) ile ilgili bir sorun tespit ettiniz mi?” sorusuna toplam 28 kişi cevap vermiştir. Bu soruya %82,1’e denk gelen 23 kişi sorunla karşılaşmadığını belirtmiştir. Geriye kalan 5 kişi ise bu soruya sorunla karşılaştım şeklinde cevap vermiştir.

“Kullanım kılavuzu ve ipuçları yeterli miydi?” sorusuna 28 kişinin %60’7’si yeterli olduğunu beyan etmiştir. Yeterli olduğunu beyan eden 17 kişiye karşılık, 11 kişi ise kullanım kılavuzu ve ipuçlarının yeterli olmadığını beyan etmiştir. Yeterli olmadığını düşünenlerin oranı ise %39,3’e karşılık gelmektedir.

Yazılımın anlaşılabilirliğine ilişkin sorulan sorulara alınan cevaplar neticesinde yazılımın anlaşılır olduğu sonucuna ulaşılmıştır. Sorulan 6 soruya alınan cevaplara ve oranlarına ilişkin tablo Çizelge 7.32’de gösterilmiştir.

Çizelge 7.32. Yazılımın anlaşılabilirliğine ilişkin sorular ve cevaplar

		f	%
Yazılım gereksiz karmaşık mıydı?	Hayır	22	21,4
	Evet	6	78,6
Yazılımdaki işlevler bir bütün olarak anlaşılır mıydı?	Hayır	3	10,7
	Evet	25	89,3
Yazılımın kullanımına ilişkin başlık, yönlendirme, metinler gibi verilen bilgiler yeterli miydi?	Hayır	3	10,7
	Evet	25	89,3
Yazılımdaki metinlerde dilbilgisi ve anlam açısından bir sorunla karşılaştınız mı?	Hayır	26	92,9
	Evet	2	7,1
Yazılımın genel tasarımı (renk, renklerin uyumu, yazı tipi) ile ilgili bir sorun tespit ettiniz mi?	Hayır	23	82,1
	Evet	5	17,9
Kullanım kılavuzu ve ipuçları yeterli miydi?	Hayır	11	39,3
	Evet	17	60,7
	Toplam	28	100,0

Yazılımın mobil adli bilişim süreçlerine katkısını tespit etmek için yazılımı kullanan 28 personele toplam sekiz farklı soru sorulmuştur. Bu sorular sürecin hızlanması ve katkısı, adımların yönlendirmesi, katkısı ve niteliği ile yeni personelin kullanımı hususlarını içermektedir.

“Yazılımın kullanılması sürecin hızlandırılmasına katkı sağladı mı?” sorusuna 20 kişi evet şeklinde cevap vermiştir. Bu toplam sayının %71,4’üne denk gelmekteyken; geriye kalan %28,6’sı sürecin hızlanması konusunda katkı sağlamadığını beyan etmiştir.

“Yazılımın kullanılması mobil cihaz imaj alma sürecine katkı sağladı mı?” sorusuna 28 kişi cevap vermiştir. %67,9’una denk gelen 19 kişi mobil cihaz imaj alma sürecine katkı sağladığını belirtmiştir. Geriye kalan 9 kişi ise bir katkısının olmadığını belirtmiş olup; bu sayı da toplam kişi sayısının %32,1’ine denk gelmektedir.

“Yazılımın kullanılması sırasında önerilen adımlar doğru ve tutarlı şekilde sizi yönlendirdi mi?” sorusuna cevap veren 28 kişiden 27’si adımların doğru ve tutarlı şekilde yönlendirdiğini belirtmiştir. Bu toplam katılımcıların %96,4’üne denk gelmektedir. Sadece %3,6’sına denk gelen 1 kişi doğru ve tutarlı yönlendirdi mi sorusuna olumsuz cevap vermiştir.

“Yazılımın size katkıları göz önüne alındığında tekrar kullanır mısınız?” sorusuna 28 kişiden %75’ine denk gelen 21’i adımların tekrar kullanabileceğini belirtmiştir. Geriye kalan 7 kişi ise olumsuz cevap vermiştir. Bu da %25’ine denk gelmektedir.

“Yazılımın kullanılması sırasında önerilen adımlar mobil cihaz adli bilişimi sürecini kolaylaştırdı mı?” 28 kişiden 18’i kolaylaştırdığını belirtmiştir. Bu toplam sayının %64,3’üne denk gelmekteyken; kolaylaştırmadığını beyan edenlerin oranı ise %35,7’dir.

“Yazılımda önerilen adımların nasıl yapılacağı konusunda bilgilendirmeye ihtiyacınız var mıydı?” sorusuna 28 kişi cevap vermiştir. Soruya cevap veren kişilerin %100’ü yazılımdaki adımların nasıl yapılacağını anlaşıldığını beyan etmiştir.

“Bu yazılımın genel olarak iş yükünü hafifleteceğini düşünüyor musunuz?” sorusuna 28 kişiden 18’i iş yükünü hafifleteceğini belirtmiştir. Bu toplam sayının %64,3’üne denk gelmekteyken; hafifletmeyeceğini beyan eden 10 kişinin oranı ise %35,7’dir.

“Yeni başlayan personelin bu yazılımdan kolaylıkla faydalanabileceğini düşünüyor musunuz?” sorusuna 28 kişi cevaplamıştır. Bu sayının %75’ine denk gelen 21 kişi yeni başlayan personelin de bu yazılımdan faydalanacağını düşündüğünü beyan etmiştir. Geriye kalan 7 kişi ise olumsuz cevap vermiştir.

Yazılımın mobil cihaz adli bilişimi sürecine katkısına ilişkin sorulara alınan cevaplar neticesinde yazılımın sürece katkı sağlayacağı anlaşılmıştır. Sorulan 8 soruya alınan cevaplara ve oranlarına ilişkin tablo Çizelge 10.33’de gösterilmiştir.

Çizelge 7.33. Yazılımın mobil cihaz adli bilişimi sürecine katkısına ilişkin sorular ve cevaplar

		Frekans	Yüzde
Yazılımın kullanılması sürecin hızlandırılmasına katkı sağladı mı?	Hayır	8	28,6
	Evet	20	71,4
Yazılımın kullanılması mobil cihaz imaj alma sürecine katkı sağladı mı?	Hayır	9	32,1
	Evet	19	67,9
Yazılımın kullanılması sırasında önerilen adımlar doğru ve tutarlı şekilde sizi yönlendirdi mi?	Hayır	1	3,6
	Evet	27	96,4
Yazılımın size katkıları göz önüne alındığında tekrar kullanır mısınız?	Hayır	7	25,0
	Evet	21	75,0
Yazılımın kullanılması sırasında önerilen adımlar mobil cihaz adli bilişimi sürecini kolaylaştırdı mı?	Hayır	10	35,7
	Evet	18	64,3
Yazılımda önerilen adımların nasıl yapılacağı konusunda bilgilendirmeye ihtiyacınız var mıydı?	Hayır	0	0,0
	Evet	28	100,0
Bu yazılımın genel olarak iş yükünü hafifleteceğini düşünüyor musunuz?	Hayır	10	35,7
	Evet	18	64,3
Yeni başlayan personelin bu yazılımdan kolaylıkla faydalanabileceğini düşünüyor musunuz?	Hayır	7	25,0
	Evet	21	75,0
	Toplam	28	100,0

Yazılımın değerlendirilmesine ilişkin olarak Sistem Kullanılabilirlik Ölçeği ve uzman görüşleri neticesinde toplam 19 soru sorulmuştur. Sorulan sorulara alınan cevaplar neticesinde yazılımın kullanımının kolay olduğu ve genel itibarıyla anlaşılır olduğu sonucuna ulaşılmıştır. Mobil cihaz adli bilişimi açısından ele alındığında sürece katkı sağlayacağı yönünde geri bildirimler alınmıştır. Mobil cihaz adli bilişimi sürecini hızlandırması beklenen bu yazılımın ayrıca bu süreci kolaylaştırması da beklenmektedir. Ayrıca adımların nasıl uygulanacağı konusundaki açıklık sorusuna verilen cevaplardaki fikir birliği dikkat çekmektedir. Doğru ve tutarlı bir şekilde kullanıcıyı yönlendiren bu yazılımın ayrıca iş yükünü de hafifletmesi beklenmektedir. Mobil cihaz adli bilişiminde çalışmaya başlayan yeni personelin de kolaylıkla bu yazılımı kullanabileceği değerlendirilmektedir.

8. SONUÇ VE ÖNERİLER

Teknolojinin yaygınlaşmasının olumsuz fonksiyonlarından biri de teknolojinin suçta kullanılmasıdır. “Bilginin her yerde olması, potansiyel delilin her yerde olması anlamına gelmektedir” (Collie, 2018). Suçla mücadelede özelde kolluk güçlerinin genelde devletin kendini geliştirmesi, kapasitesini genişletmesi, yeni yöntemler üretmesi ihtiyacı hasıl olmuştur. Bu açıdan verilerin elde edilmesi, toplanması, işlenmesi ve karar verme süreçleri açısından bilişim teknolojilerinin kullanılması sıklıkla görülmektedir. Teknolojinin suçta kullanımının yaygınlaşması gibi, suçla mücadelede kullanılması da kaçınılmaz bir hale gelmiştir. Bu sebeple suçla mücadele ve suçları aydınlatma açısından karar destek sistemlerine başvurulması da beklenen bir durumdur.

Dijital delillerin oluşturduğu yığınlar göz önüne alındığında, adli bilişim alanındaki bu problemin aşılması gerekmektedir. Bu çalışmada sürecin en verimli ve etkili şekilde hızlandırması amacıyla adli bilişim faaliyetlerine ilişkin bir çözüm önerisi sunulmuştur. Dünya genelinde 5 milyar üzerindeki kullanıcısı göz önüne alındığında ve diğer dijital materyal türlerine göre nicelik ve bulundurduğu veri açısından nitelik olarak daha ön plana çıkan mobil cihazların imaj alınması süreçlerine odaklanılmıştır. Bu kapsamda bir karar destek sistemi tasarlanmıştır. Karar destek sistemi için veri tabanı olarak, gerekli izinler alındıktan sonra EGM Siber Suçlarla Mücadele Daire Başkanlığı Adli Bilişim Şube Müdürlüğü tarafından mobil cihazlardan imaj alınmasına ilişkin veri toplanmıştır.

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı için kalite fonksiyon göçerimi yöntemine başvurulmuştur. Müşterinin sesine ulaşmak için, mobil cihaz adli bilişimi alanında görev yapan personelin böyle bir yazılımdan beklentilerinin tespiti için görüşmeler gerçekleştirilmiştir. Bu görüşmelerde müşterinin sesi olan talepler alınmıştır ve bu taleplerin onlar için önemleri de belirlenerek, KFG oluşturulması için tüketici talepleri oluşturulmuştur. Tüketici talep ve önem düzeylerinin yanı sıra korelasyonu, ilişkileri, planlama matrisi, teknik tanımlayıcılar, gerçek ve hedef değerlerin belirlenmesi gerçekleştirilmiştir. Tüm bu bileşenler ışığında kalite evi oluşturulmuş ve yazılımın oluşturulması aşamasında nelerin önemli olduğu, nasıl gerçekleştirileceği ve bunlar gerçekleştirilirken önceliklerin neler olduğu ortaya konulmuştur. Oluşturulan kalite evinde en fazla teknik önem düzeyine sahip teknik tanımlayıcının yazılımda listbox kullanılması olduğu görülmüştür.

Mobil cihaz adli bilişimi kapsamında imaj alma prosedürüne ilişkin karar destek sistemi yazılımı oluşturulması sırasında, karar ağacı yapısı için farklı algoritmalar denenmiştir. Toplanan verinin eğitiminde çapraz doğrulama yöntemi kullanılmıştır. Bu yöntemle eğitim sonunda %98,83 oranında başarı gösteren bir karar ağacı algoritması olan ID3 algoritması tercih edilmiştir. Müşterinin sesine dikkat edilerek, talepler önem düzeylerine göre önceliklendirilerek yerine getirilmiştir. Web tabanlı hazırlanan yazılım, ağ üzerinden yayınlanarak personelin kullanımına sunulmuştur.

Uygulama esnasında karar destek yazılımını kullanan 28 mobil cihaz adli bilişimi alanında çalışan personelden geri dönüşler alınmıştır. Gerçekleştirilen kullanım sonunda yazılımın kullanılmasının kolay olduğu ve yazılımın anlaşılır olduğu görülmüştür. Daha da önemlisi mobil cihaz adli bilişimi sürecine katkı sağlayacağı değerlendirilmektedir.

Tüm bu elde edilen veriler ve değerlendirmelerin neticesinde çalışmanın adli bilişim alanında bazı katkıları tespit edilmiştir. Bunlardan ilki mobil cihaz adli bilişiminde en önemli süreçlerden biri olan imaj alma sürecine en fazla etki eden faktörün tespit edilmesidir. En fazla etki eden faktörün mobil cihazın şifreli olup olmadığı durumu olduğu anlaşılmıştır.

Bu sistem sayesinde mobil cihazlardan imaj alınması işleminde doğru yönlendirmeler yapılacak ve yanlış yöntemler denenmeden hem hatayı hem de süreyi olumlu yönde etkilenecektir. Tüm işlemlerin sisteme kaydedilmesi ile birlikte tecrübelerin birleşimi olacak ve kurumsal hafıza oluşacaktır. Yeni başlayan personeli yönlendiren bu sistem sayesinde tecrübeli personele gelen soru sayısı azalacak ve iş yükünün azalmasıyla tecrübeli personel, daha kritik işlere odaklanabilecektir.

İstenirse personelin performansının da ölçülebileceği gibi, hangi personelin hangi konularda daha iyi olduğu veya hangi konularda desteğe ihtiyacı olduğu da tespit edilebilecektir. Geliştirmeye müsait olan bu sistemin yeni çıkan teknolojilere adaptasyon imkânı olup, yeni yöntemler ile revizyonu mümkündür. Ayrıca adli bilişimde imaj alma alanında böyle bir çalışma olmadığından, veri kurtarma gibi adli bilişimin diğer alt alanlarına uygulanabilme imkânı da bulunmaktadır.

Mobil cihaz adli bilişimi işlemini kurumsal olarak gerçekleştirilen yerlerde, ortaya çıkan karar ağacı diyagramı ile bu süreçlerin standardizasyonuna da katkı sağlanması

beklenmektedir. Ayrıca mobil cihaz adli bilişimine etki eden faktörlerin dinamik olarak tespiti ile bu alandaki yatırım, eğitim gibi stratejilerin daha doğru belirlenmesi ve buna ilişkin çözüm önerilerine de doğrudan katkısı olacağı değerlendirilmektedir. Bu çalışmada mobil cihaz adli bilişiminde imaj almaya etki eden en önemli faktörün mobil cihazın şifreli olup olmadığı durumu olduğu ortaya konmuştur. En önemli faktörün cihazın şifreli olup olmadığı durumu olduğunun tespit edilmesiyle, mobil cihazlarda kriptanaliz çalışmalarına ağırlık verilmesi gerekmektedir. Ayrıca bu alandaki şifreli veriyi okumaya ve şifreyi kırmaya veya atlamaya yönelik teknolojilerin üretilmesinin veya ithal edilmesinin gündeme gelmesi muhtemeldir.





KAYNAKLAR

- Abu-Assab, S. (2011). Quality Function Deployment in New Product Development. In S. Abu-Assab (Ed.), *Integration of Preference Analysis Methods into Quality Function Deployment: A Focus on Elderly People*. Cottbus, Germany: Springer Gabler. 47-69.
- Akalın, U. (2016). *Mobil Cihazlarda Adli Bilişim Çalışmalarına Yönelik Bir Model Önerisi*. Yayınlanmamış Yüksek Lisans Tezi: Gazi Üniversitesi Bilişim Enstitüsü, 45-128.
- Akıncı, K. S. (2006). *Bilişim Sistemlerinin Örgüt Yapılarına Etkileri*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 32-34.
- Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. and Gabban, F. M. (2021). Research Challenges and Opportunities in Drone Forensics Models. *Electronics*, 1-29.
- Alexouda, G. (2005). A User-Friendly Marketing Decision Support System for the Product Line Design Using Evolutionary Algorithms. *Decision Support Systems*, 495-509.
- Aliusta, C., ve Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Dergisi*, 35-42.
- Alpaydın, E. (2010). *Introduction to Machine Learning* (Second Edition b.). Massachusetts: The MIT Press, 173-196.
- Arslan, V., ve Yılmaz, G. (2010). Karar Destek Sistemlerinin Kullanımı İçin Uygun Bir Model Geliştirilmesi. *Havacılık ve Uzay Teknolojileri Dergisi*, 75-82.
- Atak, İ. (2003). *Karar Destek Sistemleri (DSS)*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Endüstri Mühendisliği, Gazi Üniversitesi, 4-16.
- Atalay, Ö. (1976). Hakem-Bilirkişi Kavram. *Ankara Barosu Dergisi*, 870-874.
- Avşar, M. (2015). *Lazer Epilasyon için Optik Görüntüleme ile Öznitelik Tabanlı Kıl Bölgesi Tespiti*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: TOBB Ekonomi ve Teknoloji Üniversitesi Fen Bilimleri Enstitüsü, 61-63.
- Ay, M. (2003). *Kalite Fonksiyon Göçerimi ve Uygulama Örneği*. Yayınlanmamış Yüksek Lisans Tezi, Denizli: Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü, 59-89.
- Aydemir, E. (2019). *Weka ile Yapay Zekâ* ((2. Baskı) b.). Ankara: Seçkin Yayıncılık, 116-133.

- Aydoğan, H. (2009). *Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 7-36.
- Bangor, A., Kortum, P. T., and Miller, J. T. (2008). An Empirical Evaluation of the System Usability Scale. *Intl. Journal of Human-Computer Interaction*, 574-594.
- Bartra, M., and Agrawal, R. (2018). Comparative Analysis of Decision Tree Algorithms. In B. H. Panigrahi (Ed.), *Nature Inspired Computing. Advances in Intelligent Systems and Computing*, Singapore: Springer, 31-36.
- Başlar, Y. (2020). Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri. *Türkiye Barolar Birliği Dergisi*, 47-76.
- Bıçak, V. (2013). *Suç Muhakemesi Hukuku*. Ankara: Polis Akademisi Yayınları, 531-553
- Bilgen, B. (2011). *Kurumsallaşma Üzerine Bir Karar Destek Sistemi Oluşturulması-Türk İnşaat Sektöründe Örnek Uygulama (Kural Tabanlı KDS Modeli)*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Fen Bilimleri Enstitüsü, İstanbul Teknik Üniversitesi, 63-93.
- Bonnett, D. A. (1999, 30 September). Design for In-System Programming. *International Test Conference 1999*, Atlantic City, ABD: IEEE, 252-259.
- Bouchereau, V., and Rowlands, H. (2000). Methods and Techniques to Help Quality Function Deployment. *Benchmarking An International Journal*, 8-20.
- Casamen, R., Mata, M., and Mantilla, J. (2005, October). Using QFD in the Design Process of a Trailer Office . *11th International Symposium on Quality Function Deployment* Aydın, Kuşadası: Dokuz Eylül University, 191-200.
- Casey, E., and Turnbull, B. (2011). Digital Evidence on Mobil Devices. In E. Casey (Ed.), *Digital evidence and computer crime: Forensic science, computers, and the internet* (Üçüncü Baskı b.). Baltimore, ABD: Academic Press., 1-44.
- Chan, L.-K., and Wu, M.-L. (2002). Quality Function Deployment: A Comprehensive Review of Its Concepts and Methods. *Quality Engineering*, 23-35.
- Collie, J. (2018). Digital forensic evidence—Flaws in the criminal justice system. *Forensic Science International*, 154-155.
- Compton, W. D. (1999). *Mühendislik ve Teknoloji Yönetimi*. (Çev. G. E. Okudan) İstanbul: Beta Yayınları, 250-271.
- Çakır, H. (2014). Mobil Cihazların İncelenmesi. H. Çakır ve M. S. Kılıç (Editörler), *Adli Bilişim ve Elektronik Deliller*, Ankara: Seçkin Yayıncılık, 373-409.

- Çelik, L. (2006). *Karar Destek Sistemlerinin Karar Verme Sürecindeki Rolü*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Sosyal Bilimler Enstitüsü, Marmara Üniversitesi, 47-70.
- Çetin, H. (2007). *KOBİ Niteliğindeki İşletmelerde Kurumsal Kaynak Planlaması Yazılımlarının Etkin Kullanılması için Kalite Fonksiyon Göçerimi*. Yayınlanmamış Yüksek Lisans Tezi, Kırıkkale: Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü, 64-69.
- Çiçek, İ. (2008). *Ülkemizde Adli Bilişim Laboratuvarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları*. Yayınlanmamış Yüksek Lisans Tezi: Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 14-17.
- Çil, İ. (2002). Bilgi Tabanlı İmalat Karar Destek Sistemleri ve Bir Uygulama. *Türkiye Makine Mühendisleri Odası Endüstri Mühendisliği Dergisi*, 15-27.
- Çinpolat, S. (2007). *Kalite Fonksiyon Göçerimi ve Hizmet Sektöründe Uygulanması*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 26-57.
- Değirmenci, O. (2014). *Ceza Muhakemesinde Sayısal Delil*. Ankara: Seçkin Yayıncılık, 60-64.
- Demirci, N. (2012). *Karar Destek Sistemlerinin Bir Durum Çalışmasına Uygulanması*. Yayınlanmamış Yüksek Lisans Tezi, Edirne: Trakya Üniversitesi, Fen Bilimleri Enstitüsü, 3-10.
- Doğanay, H. A. (2019). *Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi Sağlık Bilimler Enstitüsü, 1-87.
- Doğanay, H. A. (2020). *Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri*. Ankara: Legem Yayıncılık, 56-93.
- Effiong, E. N. (2013, Temmuz). *Computer Forensics Investigation (Step by Step Guide)*. Baixardoc: <https://baixardoc.com/documents/computer-forensics-investigation-techniques-effiong-effiong--5c9d2edf8ef6d> adresinden alındı
- Emiroğlu, E. A. (2001). *Mamul Tasarımında Kalite Fonksiyon Açınımı Tekniği ve İnşaat Sektöründe Bir Uygulama Örneği*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, 42-44.
- Faheem, M., Kechadi, T., and Le-Khac, N. (2015). The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends. *International Journal of Digital Crime and Forensics*, 1-19.

- Gerst, R. M. (2004). QFD in Large-Scale Social System Redesign. *International Journal Quality&Reliability Management*, 959-972.
- Govindaraj, J., Verma, R., Mata, R., and Gupta, G. (2014, 18-21 May). *Poster: iSecureRing: Forensic Ready Secure iOS Apps for Jailbroken iPhones*. San Jose, ABD: 35th IEEE Symposium on Security and Privacy.
- Gökçen, H., Özkil, A., Yardımoğlu, H., ve Peker, D. (2010). *Kamuda Karar Destek Sistemlerinin Kullanımı ve Bir Model Önerisi*. Antalya: Türkiye Bilişim Derneği.
- Grigaliunas, S., Toldinas, J., Venckauskas, A., Morkevicius, N., and Damasevicius, R. (2021). Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensic Investigation. *IEEE Computer Society*, 39-48.
- Günel, C. (2012, 18 Şubat - 11 Mart). Adli Bilişim ve Delillerin Toplanması. *Özyeğin Üniversitesi Sertifika Programında Sunuldu*. İstanbul.
- Güvenç, E. (2018). *Zeki Karar Destek Sistemi Kullanılarak Muğla Sıtkı Koçman Üniversitesi Uzaktan Eğitim Öğrencilerinin Ders Performanslarının Değerlendirilmesi*. Yayınlanmamış Yüksek Lisans Tezi, Muğla: Fen Bilimleri Enstitüsü, Muğla Sıtkı Koçman Üniversitesi, 13.
- Han, S. B., Chen, S., Ebrahimpour, M., and Sodhi, M. S. (2001). A Conceptual QFD Planning model. *International Journal of Quality & Reliability Management*, 796-812.
- Henkoğlu, T. (2014). *Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi*. Ankara: Pusula, 1-5.
- Hoog, A., and Strzempka, K. (2011). *iPhone and iOS Forensic Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*. Waltham, ABD: Syngress, 55-77.
- Hopgood, A. A. (2016). *Intelligent Systems for Engineers and Scientist* (Third Edition b.). Florida: CRC Press, 3-10.
- Horsman, G. (2019). Formalising Investigative Decision Making in Digital Forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation*, 146-151.
- İçel, K. (2011). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 3-10.
- İnternet: ACELab. (2022). *Pc-3000 Mobile*. ACELab: <https://www.acelaboratory.com/pc-3000-mobile.php> adresinden 22 Haziran 2022 tarihinde alınmıştır.

İnternet: Aknar, A. (2019, Mayıs). *Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Hukuka Uygunluğu*. Cahit Cengizhan: <https://cahitcengizhan.com/adli-bilisim-forensics-dijital-delillerin-elde-edilmesi-ve-hukuka-uygunlugu/> adresinden 14 Ocak 2022 tarihinde alınmıştır.

İnternet: Altındağ, A. (2018, Ocak). *Dijital Delil*. Media Trend: <https://mediatrend.mediamarkt.com.tr/dijital-delil/> adresinden 2 Mart 2022 tarihinde alınmıştır.

İnternet: Cellebrite. (2022). *Cellebrite Physical Analyzer*. Cellebrite: <https://cellebrite.com/en/physical-analyzer/> adresinden 22 Haziran 2022 tarihinde alınmıştır.

İnternet: Cellebrite. (2022). *Cellebrite Physical Analyzer*. Cellebrite: <https://cellebrite.com/en/physical-analyzer/> adresinden 22 Haziran 2022 tarihinde alınmıştır.

İnternet: EGM. (2019). *Emniyet Genel Müdürlüğü*. Kriminal Daire Başkanlığı: <https://www.egm.gov.tr/kriminal/hakkimizda-28-11-2012> adresinden 7 Temmuz 2021 tarihinde alınmıştır.

İnternet: Ekizer, A. H. (2014, Şubat). *Adli Bilişim (Computer Foresnics)*. Ekizer.Net Adli Bilişim: <https://www.ekizer.net/adli-bilisim-computer-forensics/> adresinden 13 Şubat 2021 tarihinde alınmıştır.

İnternet: Exterro. (2022). *FTK Forensic Toolkit*. Exterro: <https://www.exterro.com/forensic-toolkit> adresinden 22 Haziran 2022 tarihinde alınmıştır.

İnternet: Hancom (2017). *Mobile Forensic Software*. HancomGMD: <http://www.hancomgmd.com/> adresinden 22 Haziran 2022 tarihinde alınmıştır.

İnternet: JGK. (2019). *Jandarma Genel Komutanlığı*. Kriminal Daire Başkanlığı: <https://www.jandarma.gov.tr/kriminal/hakkimizda> adresinden 7 Temmuz 2021 tarihinde alınmıştır.

İnternet: Kahney, L. (2010, Temmuz). *Apple's Official Response To DMCA Jailbreak Exemption: It Voids Your Warranty*. Cult of Mac: <https://www.cultofmac.com/52463/apples-official-response-to-dmca-jailbreak-exemption-it-voids-your-warranty/> adresinden 29 Kasım 2021 tarihinde alınmıştır.

İnternet: TBMM. (2012, Eylül). <https://www2.tbmm.gov.tr/d24/1/1-0676.pdf> adresinden 16 Ağustos 2022 tarihinde alınmıştır.

İnternet: Magnet Forensics. (2022). *Magnet Axion Mobile Capabilities*. Magnet Forensics: <https://www.magnetforensics.com/products/magnet-axion/mobile/> adresinden 23 Haziran 2022 tarihinde alınmıştır.

İnternet: MSAB. (2021). *XRY – Mobile Forensics and Data Recovery Software*. MSAB: <https://www.msab.com/product/xry-extract/> adresinden 23 Haziran 2022 tarihinde alınmıştır.

İnternet: Mulaj, F. (2019, Ağustos). *Delil Kavramı ve Delil Sistemleri*. Bol Gunal Hukuk: <http://www.bolgunalhukuk.com/article.php?aId=47> adresinden 3 Aralık 2021 tarihinde alınmıştır.

İnternet: National Institute of Justice. (2020). *Digital Evidence and Forensics*. 07 21, 2021 tarihinde nij.ojp.gov: <https://nij.ojp.gov/digital-evidence-and-forensics> adresinden 11 Nisan 2022 tarihinde alınmıştır.

İnternet: Oxygen Forensics. (2022). *Oxygen Forensic Detective*. Oxygen Forensics: <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective> adresinden 23 Haziran 2022 tarihinde alınmıştır.

İnternet: Power, D. J. (2007, Mart). *A Brief History of Decision Support Systems*. DSSResources.com: <http://dssresources.com/history/dsshhistory.html> adresinden 31 Aralık 2022 tarihinde alınmıştır.

İnternet: Silipo, R., and Melcher, K. (2019, Ağustos). *From a Single Decision Tree to a Random Forest*. Dataversity: <https://www.dataversity.net/from-a-single-decision-tree-to-a-random-forest/> adresinden 19 Eylül 2022 tarihinde alınmıştır.

İnternet: SWGDE. (2019, Eylül). *SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition*. Scientific Working Group on Digital Evidence: <https://www.swgde.org/documents/published> adresinden 12 Ekim 2021 tarihinde alınmıştır.

İnternet: Solmaz, A. N. (2008, Temmuz 11). *Olay Yerinden Alınan Dijital Delillerin Hukuki Kabul Edilebilirliğini Arttırmak*. Securify ID: <https://securifyid.com/2008/07/11/olay-yerinden-alinan-dijital-delillerin-hukuki-kabul-edilebilirligini-arttirmak/> adresinden 18 Ağustos 2022 tarihinde alınmıştır.

İnternet: Teel Technologies. (2012). *The Digital Investigator's Resource For Mobile Device Forensic Information/Products*. Mobile Forensics Central: http://www.mobileforensicscentral.com/mfc/products_software.asp#:~:text=The%20Cellebrite%20UFED%20and%20UFED,devices%20capable%20of%20being%20analyzed. adresinden 24 Haziran 2022 tarihinde alınmıştır.

İnternet: TÜİK. (2022, Ağustos). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması*, TÜİK: [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2022-45587](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587) adresinden 11 Aralık 2022 tarihinde alınmıştır.

- İnternet: Uyanık, B. (2016). *Karar Destek Sistemlerin Geliştirme Yaşam Döngüsü*. Dokumen.tips: <https://dokumen.tips/documents/karar-destek-sistemlerin-gelistirme-yasam-doenguesue.html> adresinden 17 Kasım 2021 tarihinde alınmıştır.
- James, I. J., Sosha, A. F., and Gladyshev, P. (2012). Digital Forensics Investigation and Cloud Computing. In K. Ruan (Ed.), *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, Pennsylvania, ABD: Information Science Reference, 1-41.
- Jansen, W., Ayers, R., and Brothers, S. (2014). *Guidelines on Mobile Device Forensics*. Springfield, ABD: NIST Special Publication, 15-50.
- Kabari, L. G., and Nwachukwu, E. (2013). Decision Support System Using Decision Tree and Neural Networks. *Computer Engineering and Intelligent Systems*, 8-19.
- Kalaycı, Ş. (2006). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri*. 2. Baskı, Ankara: Asil Yayın Dağıtım, 85-116.
- Kapanoğlu, M. (2019). Karar Destek Sistemleri: Temel Kavramlar. M. Kapanoğlu (Editör) içinde, *Karar Destek Sistemleri*. Eskişehir: Anadolu Üniversitesi, 2-23.
- Karegowda, A. G., Manjunath, A. S., and Jayaram, M. .. (2010). Comparative Study of Attribute Selection Using Gain Ratio and Correlation Based Feature Selection. *International Journal of Information Technology and Knowledge Management*, 271-277.
- Kathiravan, N., Devadasan, S. R., Michael, T. B., and Goyal, S. K. (2008). Total Quality Function Deployment in a Rubber Processing Company: A Sample Application Study. *Production Planning and Control*, 53-66.
- Kavzoğlu, T., ve Çölkesen, İ. (2010). Karar Ağaçları ile Uydu Görüntülerinin Sınıflandırılması: Kocaeli Örneği. *Harita Teknolojileri Elektronik Dergisi*, 36-45.
- Kıçeci, H. (2014). Bilgisayar Medyalarına İlk Müdahale. H. Çakır ve M. S. Kılıç (Editörler), *Adli Bilişim ve Elektronik Deliller* Ankara: Seçkin, 161-193.
- Kılıç, M. S. (2014). Elektronik Delillerin Yapısal Özellikleri. H. Çakır ve M. S. Kılıç (Editörler), *Adli Bilişim ve Elektronik Deliller*, Ankara: Seçkin, 139-157.
- Kocabaş, Z., Özkan, M. M., ve Başpınar, E. (2013). *Temel Biyometri*. Ankara: Ankara Üniversitesi Ziraat Fakültesi Yayınları, 31.
- Koç, E. (2013). *Yöntem ve Uygulama Açısından Klinik Karar Destek Sistemleri*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Fen Bilimleri Enstitüsü, Okan Üniversitesi, 14.

- Kuru, A. (1997). *Kalite Fonksiyonlarının Yayılımı ve Gelişimi*. Yayınlanmamış Yüksek Lisans Tezi, Bursa: Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, 17-60.
- Lillis, D., Becker, B. A., O'Sullivan, T., and Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *The 11th ADFSL Conference on Digital Forensics, Security and La*. Daytona Beach, FL, USA: CDFSL., 1-11.
- Lin, I.-L., Chao, H.-C., and Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *2011 International Conference on Broadband, Wireless Computing, Communication and Applications*, Barcelona, Spain: BWCCA 2011, 26-28.
- Liu, H., and Cocea, M. (2018). Induction of Classification Rules by Gini-Index Based Rule Generation. *Information Sciences*, 227-246.
- Marakas, G. M. (1999). *Decision Support Systems*. New Jersey: Prentice Hall, 7.
- Murthy, S. k. (1998). *Automatic Construction of Decision Trees from Data: A Multi-Disciplinary Survey*. Boston, ABD: Kluwer Academic Publishers.
- Murthy, S. K., Kasif, S., and Salzberg, S. (1994). A System for Induction of Oblique Decision Trees. *Journal of Artificial Intelligence Research*, 1-32.
- Mutawa, N. A., Franqueira, J. B., Marrington, A., and Read, J. C. (2018). Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes. *Digital Investigation*, 70-82.
- Narayanan, P. (2020). Assessment of Constructability and Financial Aspects of Risks in Construcion Industry Using Design Expert. *International Journal of Advanced Science and Technology*, 4329-4338.
- Noor, N. M., and Mohamed, R. (2010). New Architecture for Intelligent Multi-Agents Paradigm in Decision Support System. In C. S. Jao (Ed.), *Decision Support Systems*, Rijeka: INTECH, 25-33.
- Özdil, N., ve Dönmez, S. (2002, 17-19 Nisan). Örne Alanında Faaliyet Gösteren Bir Tekstil İşletmesinde Kalite Fonksiyon Göçeriminin Uygulanması. *I. Ulusal Kalite Fonksiyon Göçerimi Sempozyumu*. İzmir: Dokuz Eylül Üniversitesi Yayınları.
- Pal, M., and Mather, P. M. (2003). An Assessment of The Effectiveness of Decision Tree Methods for Land Cover Classification. *Remote Sensing of Environment*, 554-565.
- Power, D. J. (2002). *Decision Support Systems: Concepts and Resources for Managers*. Westport, Connecticut, USA: Quorum Books, 1-28.

- Prytherch, R. (2005). *Harrod's Librarians' Glossary*. Hampshire, UK: Ashgate, 199.
- Ramadhani, E., Wahyuni, E. G., and Pratama, H. R. (2020, 3-4 August). Design of Expert System for Tool Selection in Digital Forensics. *The 2nd Tarumanagara International Conference on the Applications of Technology and Engineering (TICATE)* (s. 1-10). Jakarta, Indonesia: IOP Science.
- Safavian, S. R., and Landgrebe, D. (1991). A Survey of Decision Tree Classifier Methodology. *IEEE Transactions on Systems Man and Cybernetics*, 660-674.
- Saraç, M. (2020). *Van Yüzüncü Yıl Üniversitesi Elektronik Belge Yönetim Sisteminin Kullanım Memnuniyetinin CART Karar Ağacı ile İncelenmesi*. Yayınlanmamış Yüksek Lisans Tezi, Van: Van Yüzüncü Yıl Üniversitesi, Sağlık Bilimleri Enstitüsü, 9-12.
- Sarsılmaz, M. (1999). *Kalite Fonksiyon Yayılımı ve Bir İşletmede Uygulama Denemesi*. Yayınlanmamış Yüksek Lisans Tezi, Balıkesir: Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü, 90.
- Savaş, H., ve Ay, M. (2005). Üniversite Kütüphanesi Tasarımında Kalite Fonksiyon Göçerimi Uygulaması. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 80-98.
- Scanlon, M., and Kechadi, M.-T. (2014). Digital Evidence Bag Selection for P2P Network Investigation. *In Proceedings of the 7th International Symposium on Digital Forensics and Information Security*. Gwangju, South Korea: Springer, 307-314.
- Shillito, L. M. (1994). *Advanced QFD, Linking Technology to Market and Company Needs*. New York, USA: Wiley Publishers, 2-146.
- Shouman, M., Turner, T., and Stocker, R. (2011). Using Decision Tree for Diagnosing Heart Disease Patients. *Proceedings of the Ninth Australasian Data Mining Conference* (s. 23-30). Ballarat, Australia: ACM Digital Library, 23-30.
- Sui, B. (2013). *Information Gain Feature Selection Based on Feature Interactions*. Yayınlanmamış Yüksek Lisans Tezi, Houston, ABD: University of Houston, the Faculty of the Department of Computer Science, 8-11.
- Sun, S., Cuadros, A., and Beznosov, K. (2015, 12 October). Android Rooting: Methods, Detection and Evasion. *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy on Smartphones and Mobile Devices* (s. 3-14). Denver, ABD: Association for Computing Machinery.
- Süder, E. (2003). *Müşteri Gereksinimlerini Karşılamada Kalite Fonksiyon Göçerimi (QFD) ve Tekstil Sanayinde Bir Uygulama*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 59.

- Tangirala, S. (2020). Evaluating the Impact of GINI Index and Information Gain on Classification Using Decision Tree Classifier Algorithm. *International Journal of Advanced Computer Science and Applications*, 612-619.
- Tekin, İ. (2009). *İşletmelerin Karar Verme Düzeylerinde Stratejik Planlamanın Yeri ve Ticari Bankalarda Uygulanırılığı Üzerine Bir Araştırma*. Yayınlanmamış Yüksek Lisans Tezi, Isparta: Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, 7-12.
- Tokaylı, M. A. (2005). *Zaman Pencere Arayış Problemi İçin Karar Destek Sistemi*. Yayınlanmamış Yüksek Lisans Tezi, Ankara: Fen Bilimleri Enstitüsü, Gazi Üniversitesi, 15-16.
- Turban, E. (1995). *Decision Support Systems and Expert Systems: Management Support Systems*. New York: Macmillan Publishing Company, 110.
- Vatis, M. A. (2010). The Council of Europe Convention on Cybercrime In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: The National Academic Press, 207-223.
- Vege, S. H. (2012). *Ensemble of Feature Selection Techniques for High Dimensional Data*. Kentucky, ABD: Western Kentucky University, The Faculty of the Department of Mathematics and Computer Science , 11-13.
- Wang, S. J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime. *Computer Standards & Interfaces*, 216-223.
- Wind, Y., and Saaty, T. L. (1980). Marketing Applications of the Analytic Hierarchy Process. *Management Science*, 641-658.
- Witten, I., Frank, E., and Hall, M. A. (2011). *Data Mining Practical Machine Learning Tools and Techniques*. Burlington, ABD: Morgan Kaufmann, 144.
- Yenginol, F. (2008). Neden Kalite Fonksiyon Göçerimi? *Dokuz Eylül Üniversitesi İşletme Fakültesi Dergisi*, 7-15.
- Yıldırım, H. (2002). *Kalite Fonksiyon Yayılımı ve Pazarlama Stratejisi Olarak Toplam Kalite Yönetiminde Uygulaması*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 78.
- Yıldız, M. S., ve Baran, Z. (2011). Kalite Fonksiyon Göçerimi ve Homojenize Yoğurt Üretiminde Uygulaması. *Ege Akademik Bakış*, 59-72.
- Yılmaz, F., ve Çakır, H. (2021). Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 1-11.

- Yılmaz, F., ve Güllüpınar, F. (2020). Türkiye’de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 5371-5409.
- Zairi, M., and Yousef, M. A. (1995). Quality Function Deployment: A Main Pillar for Successful Total Quality Management and Product Development. *International Journal of Quality & Reliability Management*, 9-23.
- Zareen, A., and Baig, S. (2010, 20 May). Mobile Phone Forensics Challenges, Analysis and Tool Clasification. *the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering* (s. 47-55). Oakland, ABD: IEEE Computer Society, 2010.
- Zhou, F., Yang, B., Li, L., and Chen, Z. (2008, 18-20 June). Overview of the New Types of Intelligent Decision Support System. *3rd International Conference on Innovative Computing Information and Control*. Dalian, China: IEEE.
- Zultner, R. E. (1993). TQM for Technical Teams. *Communications of th ACM*(36), 79-91.



EKLER

EK-1. Mobil cihazlarda imaj almaya etki eden faktörlere ilişkin uzman görüş formu

UZMAN GÖRÜŞ FORMU

Mobil cihazın imajının alınması için cihazla ilgili olarak, cihaza ilişkin bilgilerin ve cihazın durumuna ilişkin bilgilerin girilerek, o cihazla ilgili hangi adımların uygulanacağını kullanıcıya sunan bir karar destek yazılımı geliştirilmesi hedeflenmektedir.

Bu yazılım ile kullanıcı personel özelinde beklenen çıktıları ise şu şekildedir:

- Etkin şekilde kullanılması sonucunda mobil cihaz imaj alma süreçlerini yanlış yöntemler denenmeden hatanın ve sürenin azaltılması,
- Yeni personeli yönlendirebilecek bu sistem sayesinde tecrübeli personelin iş yükünün azaltılması,
- Karar ağacı algoritması sayesinde mobil cihaz adli bilişimi süreçlerinin standardizasyonunun sağlanmasıdır.

Mobil cihaz adli bilişimi alanındaki uzmanlığınızdans dolayı, mobil cihaz adli bilişimine etki eden faktörleri tespit etmek için değerli görüşlerinize ihtiyaç olmuştur. Bu kapsamda bu alandaki tecrübeleriniz ve uzmanlığınıza dayanarak, mobil cihaz adli bilişiminde imaj alma konusunda etki eden faktörleri belirtiniz:

Uzmanlık alanlarınız:				
Bu alandaki tecrübe yılınız:			Yaşınız:	
Eğitim düzeyiniz:	Ön lisans ☐	Lisans ☐	Y. Lisans ☐	Doktora ☐
Çalıştığınız sektör:	Kamu ☐		Özel ☐	

EK-2. Mobil cihazlarda imaj almaya etki eden faktörlere ilişkin uzman görüş formu
(İngilizce)

FORM OF EXPERT OPINION

In order to take the image of the mobile device, it is aimed to develop a decision support system software that provides the user with the actions to be taken about that device by entering the information about the device and the status of the device.

With this software, the expected outputs for user are as follows:

- As a result of effective use, reducing the error and time of mobile device acquisition processes without trying wrong methods,
- Reducing the workload of experienced personnel thanks to this system that can direct new personnel,
- Ensuring the standardization of mobile device forensics processes thanks to the decision tree algorithm.

Due to your expertise in digital forensics, your valuable input was needed to identify the factors affecting mobile device forensics. In this context, based on your experience and expertise in this field, specify the factors affecting image acquisition in mobile device forensics:

Information about your expertise:

Areas of expertise (multiple if needs)	Experience in the field (years)	Graduation degree	Sector worked
		☐ Associate,	☐ Private ☐ Public
	Age	☐ Bachelor's,	
		☐ Master of Science, ☐ PhD	

EK-3. Etik kurul onayı

Evrak Tarih ve Sayısı: 11.11.2019-E.141425



T.C.
GAZİ ÜNİVERSİTESİ
Ölçme Değerlendirme Etik Alt Çalışma Grubu



Sayı : 91610558-302.08.01-
Konu : Bilimsel ve Eğitim Amaçlı

BİLİŞİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 26.07.2019 tarih ve E.92975 sayılı yazı

İlgi yazınız ile göndermiş olduğunuz, Enstitünüz Adli Bilişim Anabilim Dalı **Doktora Öğrencisi Furkan YILMAZ'm, Dr.Öğr. Üyesi Hüseyin ÇAKIR'm** danışmanlığında yürüttüğü *"Uzman Sistem Yaklaşımı ile Adli Bilişim Laboratuvarı Yönetiminde Karar Destek Sisteminin Geliştirilmesi"* adlı tez çalışması ile ilgili konu Kurulumuzun 16.10.2019 tarih ve 10 sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. Mehtap ÇAKAN
Kurul Başkanı

Araştırma Kod No: 2019-340

Ek: 1 Liste



Ankara
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi :<http://etikkomisyon.gazi.edu.tr/>

Bilgi için :Burak Çitrak
Birim Evrak Sorumlusu
Telefon No:0312 229 78 00

Bu belge 5070 sayılı Elektronik İmza Kanununun 5. Maddesi gereğince güvenli elektronik imza ile imzalanmıştır.

EK-3. (devam) Etik kurul onayı

GAZİ ÜNİVERSİTESİ ÖLÇME DEĞERLENDİRME ETİK ALT ÇALIŞMA GRUBU KATILIM LİSTESİ	
TOPLANTI TARİHİ : 16/10/2019	TOPLANTI SAYISI : 10
ADI-SOYADI	İMZA
Prof. Dr. Mehtap ÇAKAN Başkan	
Doç.Dr.İsmail KARAKAYA Başkan Yrd.	
Prof.Dr.Galip YÜKSEL	
Prof.Dr.İsmet YÜKSEL	
Prof.Dr.Seçil ÖZKAN	
Prof.Dr.Cevriye TEMEL GENCER	
Prof.Dr. C. Haluk BODUR	
Prof.Dr.İbrahim DOĞAN	
Prof.Dr.Aymelek GÖNENÇ	
Doç.Dr.Zehra GÖÇMEN BAYKARA	
Doç.Dr.Nihan KAFA	
Doç.Dr.İlyas OKUR	
Doç.Dr.Necdet KARASU	

EK-3. (devam) Etik kurul onayı

Evrak Tarih ve Sayısı: 16.09.2022-E.456815



**T.C.
GAZİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Komisyonu**

Sayı : E-77082166-302.08.01-456815
Konu : Bilimsel ve Eğitim Amaçlı

16.09.2022

Dağıtım Yerlerine

Daha önce 11.11.2019 tarih ve E.141425 sayılı yazımız ile onay alan 2019-340 kod numaralı Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı Doktora Öğrencisi Furkan YILMAZ'ın, Doç. Dr. Hüseyin ÇAKIR'ın danışmanlığında yürüttüğü "*Uzman Sistem Yaklaşımı ile Adli Bilişim Laboratuvarı Yönetiminde Karar Destek Sisteminin Geliştirilmesi*" başlıklı tez çalışması ile ilgili ilgililerden alınan 01.09.2022 tarihli dilekçe Komisyonumuzun 13.09.2022 tarih ve 15 sayılı toplantısında görüşülmüş olup,

Çalışmanın başlığının "*Mobil Cihaz Adli Bilişimi Kapsamında İmaj Alma Sürecine İlişkin Karar Destek Sistemi Oluşturulması*" olarak değiştirilmesi ile ilgili talebin uygun olduğuna oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste
DAĞITIM
Gereği:
Sayın Doç. Dr. Hüseyin ÇAKIR

Bilgi:
Bilişim Enstitüsü Müdürlüğüne

Belge Doğrulama Kodu :BSAENJT6L3

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Takip Adresi : <https://www.turkiye.gov.tr/gazi-universitesi-ebys>

Emniyet Mahallesi Bandırma Caddesi No :6/1 06560 Yenimahalle/ANKARA
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi :<http://etikkomisyon.gazi.edu.tr/>
Kep Adresi: gaziuniversitesi@ks01.kep.tr

Bilgi için :Ayfer Çekmez
Genel Evrak Sorumlusu
Telefon No:202 38 81



Bu belge,güvenli elektronik imza ile imzalanmıştır.

EK-3. (devam) Etik kurul onayı

Evrak Tarihi ve Sayısı: 16.09.2022-E.456815	
GAZİ ÜNİVERSİTESİ	
ETİK KOMİSYONU KATILIM LİSTESİ	
TOPLANTI TARİHİ : 13.09.2022	TOPLANTI SAYISI : 15
ADI – SOYADI	İMZA
Prof. Dr. İsmail KARAKAYA BAŞKAN	
Prof.Dr.C.Haluk BODUR	
Prof.Dr.Seçil ÖZKAN	
Prof.Dr.Cevriye TEMEL GENCER	
Prof.Dr.İsmet YÜKSEL	
Prof.Dr.Aymelek GÖNENÇ	
Prof.Dr.Gülay BAYRAMOĞLU	
Prof.Dr.Makbule GEZMEN KARADAĞ	
Prof.Dr.Zehra GÖÇMEN BAYKARA	
Prof.Dr.İlyas OKUR	
Prof.Dr.Nihan KAFA	
Doç.Dr.Melek Gülşah ŞAHİN	

EK-4. Emniyet Genel Müdürlüğünden alınan izin

T.C.
İÇİŞLERİ BAKANLIĞI
Emniyet Genel Müdürlüğü

Sayı : 25984256-54684-(91244).
Konu : Akademik Araştırma Talebi İlk.

21/11/2019

GENEL MÜDÜRLÜK MAKAMINA

Başkanlığımız emrinde görevli 347018 sicil sayılı Başkomiser Furkan YILMAZ, Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalında devam ettiği "Uzman Sistem Yaklaşımı ile Adli Bilişim Laboratuvarı Yönetiminde Karar Destek Sisteminin Geliştirilmesi" adlı doktora tez çalışması kapsamında, ekteki ölçeğe göre veri toplamak için talepte bulunmuştur.

Konusu itibarıyla Başkanlığımız Adli Bilişim Şube Müdürlüğü ve bağlı taşra birimlerindeki işleme tutulan mobil cihazlarla ilgili herhangi soruşturma veya kovuşturma bilgisi ile kişisel veriden bağımsız olarak cihazın bilgileri, cihazın durumu, yapılan işlemler ve elde edilen sonuçlara ilişkin veriler toplanarak, hangi durumlarda hangi yöntemlerle başarılı sonuç alma ihtimaline ilişkin değerlendirmelerin bahse konu tez çalışmasında kullanılması hususunu;

Tensiplerinize arz ederim.

Siber Suçlarla Mücadele Daire Başkanı
1.Sınıf Emniyet Müdürü

Ek: Ölçek (1 Sayfa)

O L U R

21/11/2019

Genel Müdür a.
Emniyet Genel Müdür Yardımcısı
1.Sınıf Emniyet Müdürü

EK-5. Müşterinin sesi tespiti için görüşme formu

MÜŞTERİNİN SESİ TESPİTİ İÇİN GÖRÜŞME FORMU

Mobil cihazın imajının alınması için cihazla ilgili olarak, cihaza ilişkin bilgilerin ve cihazın durumuna ilişkin bilgilerin girilerek, o cihazla ilgili hangi adımların uygulanacağını kullanıcıya sunan bir karar destek yazılımı geliştirilmesi hedeflenmektedir. Sizin kullanımınıza sunulması hedeflenen yazılımdan beklentileriniz neler olduğuna ilişkin görüşmeler gerçekleştirilmiştir.

Gerçekleştirilen görüşmeler neticesinde yazılıma ilişkin bazı talepler tespit edilmiştir. Bu taleplerin sizin için önem düzeylerine ilişkin aşağıdaki tabloyu önem düzeyi 1’den 9’a kadar olacak şekilde (9, en önemli) doldurunuz:

Talepler	Önem Düzeyi
Kendi performansının izlenilebilmesi	
Kullanımının kolay olması	
Yazılımın anlaşılır olması	
Cihaz bilgileri girerken modele göre diğer verilerinin otomatik gelmesi	
Cihazda arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	
Benzer durumla karşılaşmış kişinin görüntülenebilmesi	
Açıklama verisi girme imkânı olması	
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	

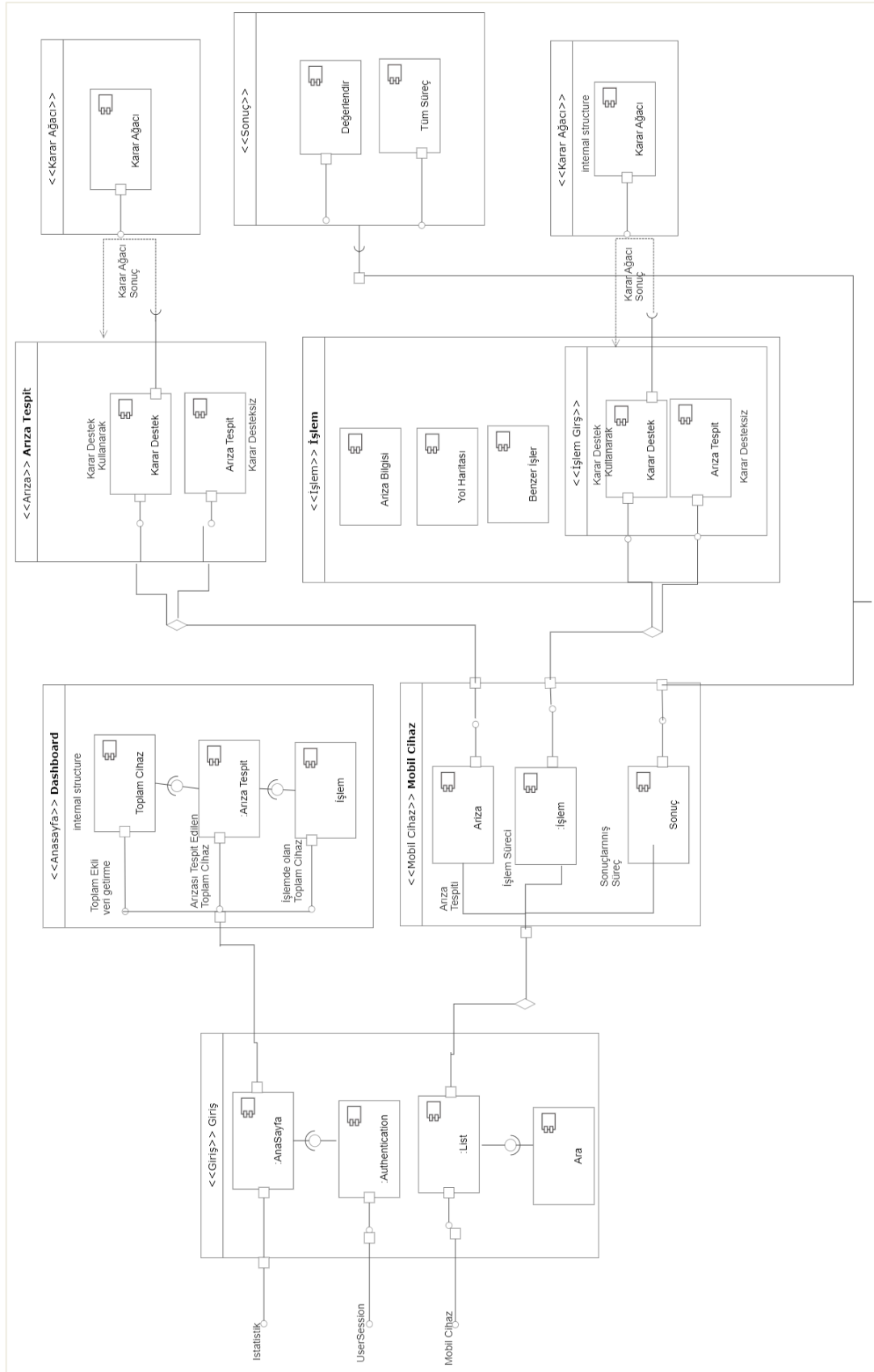
Uzmanlık alanlarınız:				
Bu alandaki tecrübe yılınız:	Yaşınız:			
Eğitim düzeyiniz:	Ön lisans ☐	Lisans ☐	Y. Lisans ☐	Doktora ☐
Çalıştığınız sektör:	Kamu ☐		Özel ☐	

EK-6. Oluşturulan kalite evi

TALEPLER	ÖNEM DERECE	İstatistik ekranı	Sade Arayüz	Kullanım ipuçları	Web tabanlı yazılım	Ustboksler oluşturulması	Tekstboksler oluşturulması	Karar Ağacı	Mobil cihazlar için veri tabanı	Yapılan işlemlere ilişkin veri tabanı	Önem Derecesi (%)
Kendi performansının izlenilebilmesi	7,72	0			Δ						6,9
Kullanımın kolay olması	7,52		0	0	0	0	Δ	0	0		16,8
Yazılımın anlaşılır olması	7,52		0	0	0	0	0				16,8
Çizim bilgileri gereken modele göre diğer verilerin otomatik gelmesi	7,14				0	0	0		0		15,9
Çizimde arıza olmaması durumunda arıza kısmının doğrudan geçilebilmesi	6,10		0		0						8,7
Benzer duruma karşılaşılmış kişinin görüntülenebilmesi	7,38			0						0	8,8
Açıklama verisi girme imkanı olması	8,10						0				9,6
Yöntemin nasıl yapılacağı konusunda bilgi vermesi	7,45			0				0		0	16,6
TEKNİK ÖNEM DERECE	2212,50	61,97	327,65	376,72	276,67	344,18	103,43	199,64	293,93	228,32	
NORMALİZE TEKNİK ÖNEM	100,0	2,8	14,8	17,0	12,5	15,6	4,7	9,0	13,3	10,3	
Ne kullanıldı		pie chart ve line chart		Üzerine gelince açılacaklı olan metin kutuları	Java Script Kütüphanesi: React	React: Listbox	React: Textbox	Decision Tree Algoritması	Python kütüphanesi: BeautifulSoup ve back4app isimli web sayfası	MySQL veri tabanı	
		alt menü verileri ve yapılan işlemleri sınıflandıran dashboard yapımı.	alt menü sekmelerinin yer aldığı farklı ekranlar oluşturulması	Öğelerin işlevlerinin açıklanması	Intranet üzerinden yayın yapan web projesi	Çizim ile ilgili marka-model ile durum bilgilerinin elle girilmesi yerine listeden seçilmesi	İşlem bitiminde kullanıcıya esnek veri girişi yapma imkanı sağlayan metin alanı	Çizim verileri gridiğinde kullanıcıya işlemi nasıl yapması gerektiğini gösteren diyagram	Çizimlere alt detay bilgilerin veri tabanına entegre edilmesi	Bugüne kadar yapılan işlemleri, kim tarafından yapıldığı bilgisiyle birlikte veri tabanına eklenmesi	
Hedef											336,6
											100,0

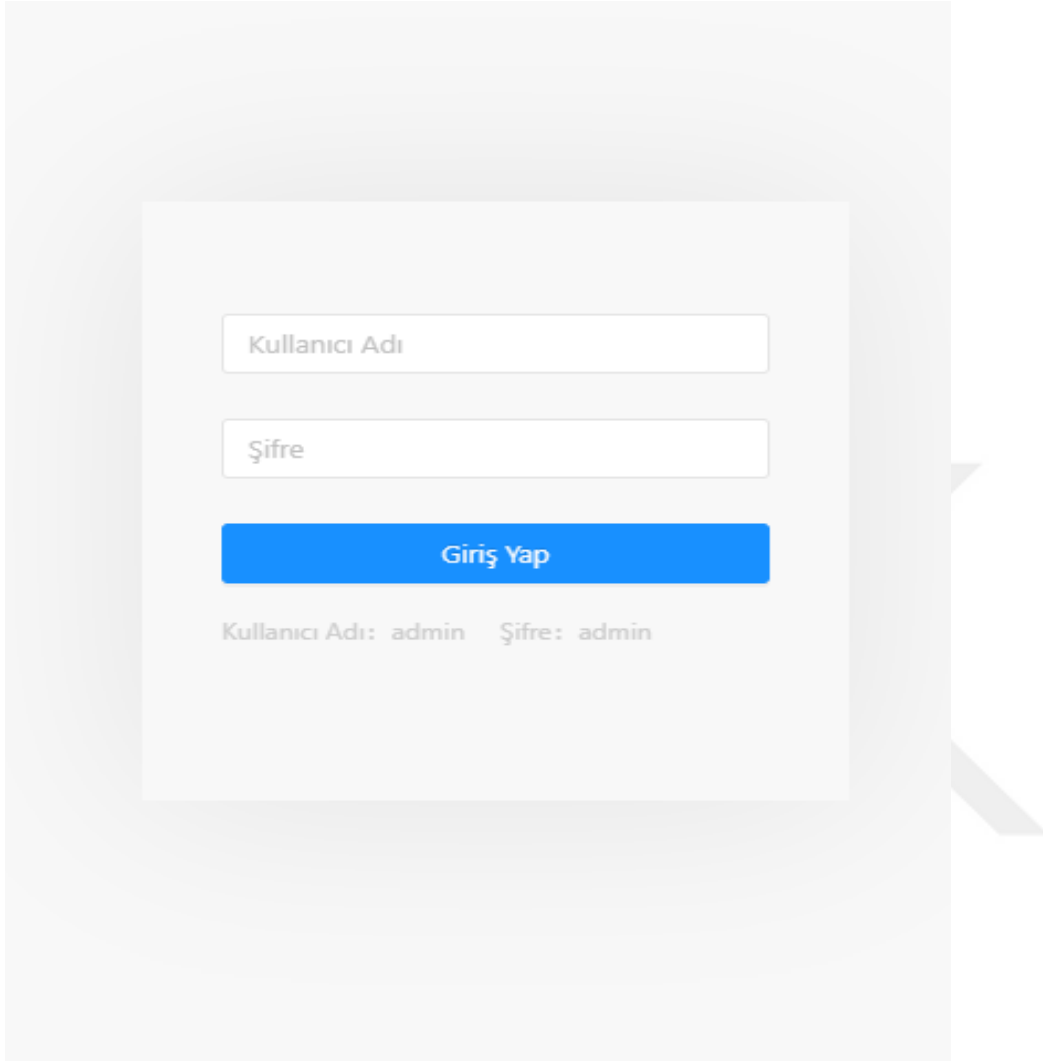
Çizelge 6.1. Oluşturulan kalite evi

EK-7. Yazılım bileşenleri diyagramı



Şekil 7.1. Yazılım bileşenleri diyagramı

EK-8. Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



Kullanıcı Adı

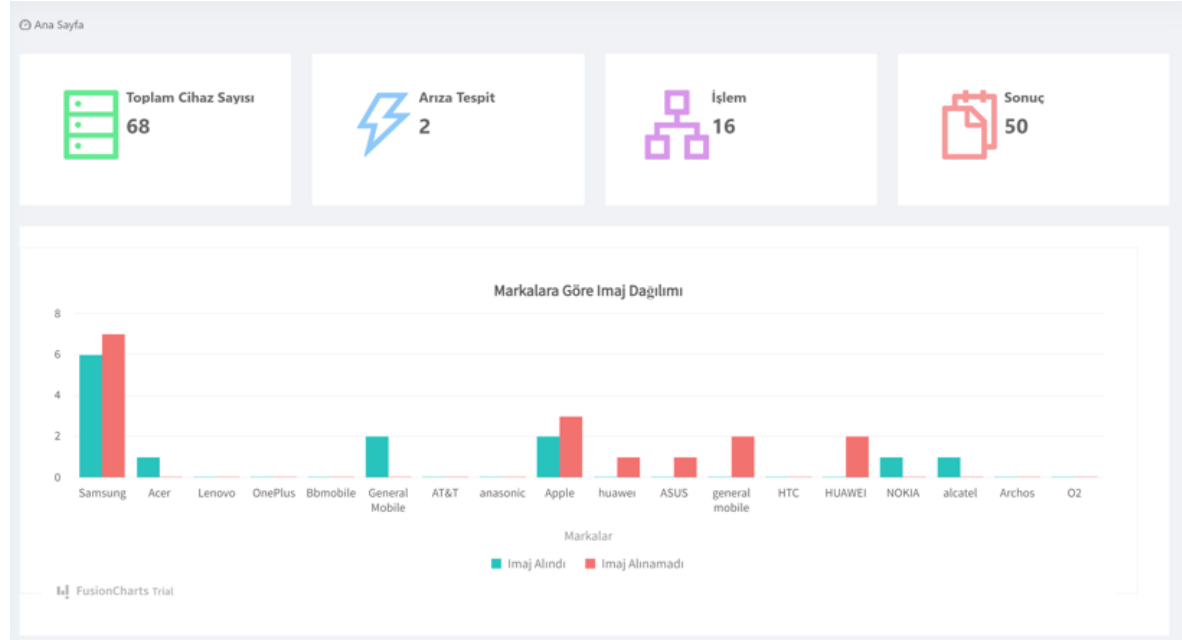
Şifre

Giriş Yap

Kullanıcı Adı: admin Şifre: admin

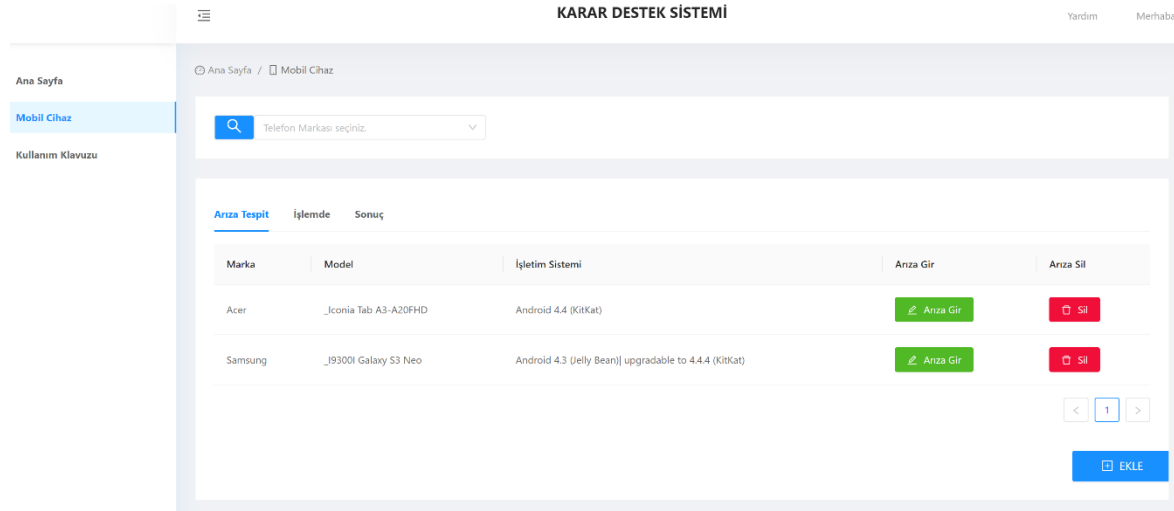
Resim 8.1. Giriş ekranı

EK-8. (devam) Mobil cihaz adlı bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



Resim 8.2. Ana sayfada yer alan dashboard ekranı

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



Resim 8.3. Cihazlara ilişkin listeleme ve arama ekranı

EK-8. (devam) Mobil cihaz adlı bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Seçenek Manuel

• Telefon Markası:		• Telefon Modeli:		• İşletim Sistemi:		• ChipSet:	
Battery:		Bluetooth:		AudioJack:		Cpu:	
Announced:		Dimension:		DisplayResolution:		DisplaySize:	
DisplayType:		Edge:		FourG:		Gprs:	
Gps:		Gpu:		InternalMemory:		LoudSpeaker:	
MemoryCard:		Nfc:		Network*:		NetworkSpeed:	
Announced:		PrimaryCamera:		Ram:		Radio:	
Sim*:		SecondaryCamera:		Sensor:		Status:	
ThreeG:		TwoG:		Usb:		Wlan:	

Kaydet

Resim 8.4. Cihaz ekleme ekranı

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Arıza Ekleme Alanı

Karar Destek

Arıza Tespit

Arıza Girişi Yapan Personel:

Arıza Girişi Yapan Personel

Cihaz Şifreli Mi:

Cihaz Şifreli Mi?

Cihaz Parçalanmış Mi:

Cihaz Parçalanmış Mi?

Port Arızalı Mi:

Port Arızalı Mi?

Ekran Arızası Var Mi:

Ekran Arızası Var Mi?

Root İhtiyacı Var Mi:

Root İhtiyacı Var Mi?

Anakart Arızası Var Mi:

Anakart Arızası Var Mi?

Yazılımsal Arıza Var Mi:

Yazılımsal Arıza Var Mi?

Arıza Ekle

Şekil 8.5. Arızanın elle girildiği ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Karar Destek
Arıza Tespit

Arıza Girişi Yapan Personel:

Yazılımsal Arıza Var Mı:

Port Arızalı Mı:

***Arıza tespiti için izlenmesi gereken adımlar:**

```

graph TD
    A["Android 4.3 (Jelly Bean) | upgradable to 4.4 (KitKat)"] --> B["I9300I Galaxy S3 Neo"]
    B --> C["Samsung"]
    C --> D["Yazılımsal Arıza Var Mı?"]
    D --> E["Evet"]
        
```

Şekil 8.6. Karar Destek Sistemiyle Arıza Giriş Ekranı

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Arıza TespitİşlemdeSonuç

Marka	Model	İşletim Sistemi	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Arıza Sil
HTC	_One M8s	Android 5.0 (Lollipop)	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_I9500 Galaxy S4	Android 4.2.2 (Jelly Bean) upgradable to 5.0.1 (Lollipop)	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_Galaxy S5 LTE-A G906S	Android 4.4.2 (KitKat) upgradable to 6.0.1 (Marshmallow)	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil
Samsung	_I9190 Galaxy S4 mini	Android 4.2.2 (Jelly Bean) upgradable to 4.4.2 (KitKat)	Arıza Bilgisi	Yol Haritası	Benzer İşler	İşlem Gir	Sil

<

1

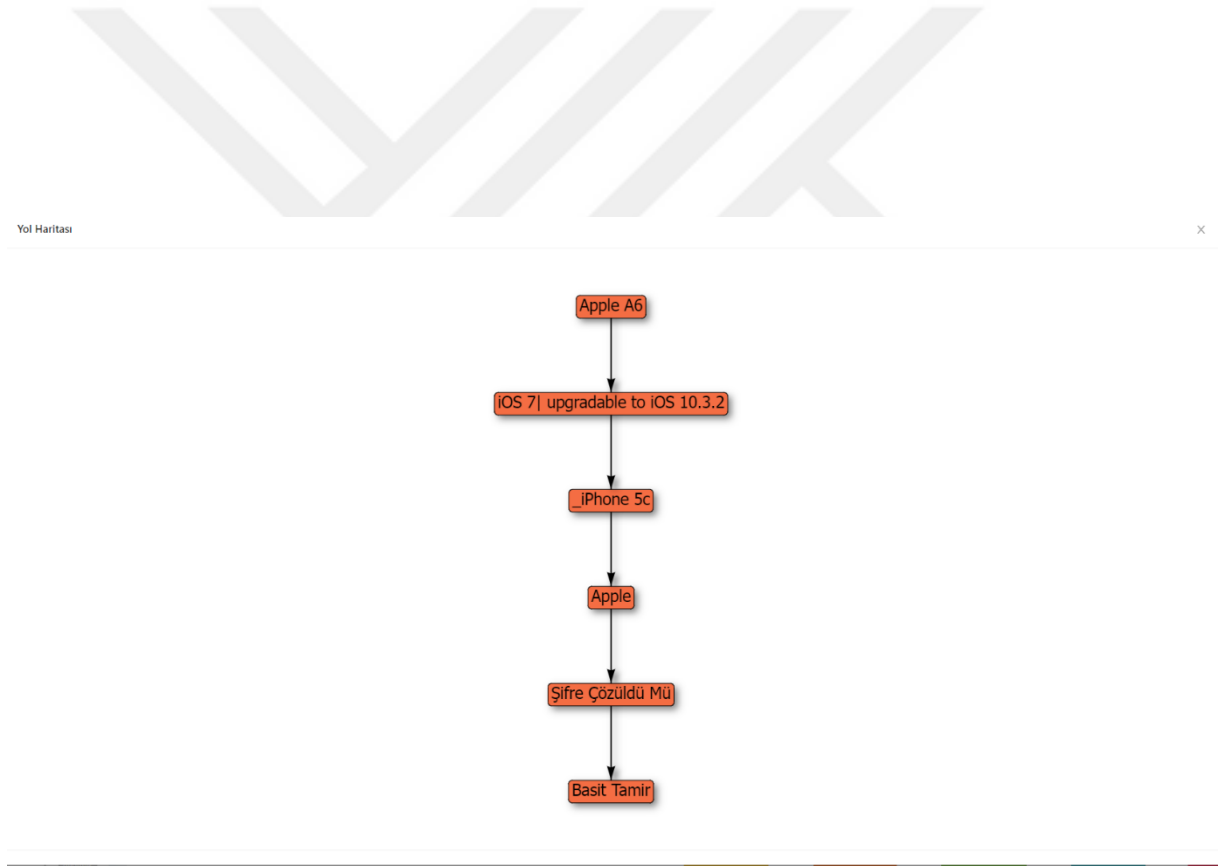
>

Şekil 8.7. İşlemde olan cihazların görüntülendiği ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Arıza Bilgisi								
ŞİFRELİ Mİ	TAMAMEN PARÇALANMIŞ	ANAKART ARIZASI	PORT ARIZASI	EKRAN ARIZASI	YAZILIM ARIZASI	ROOT İHTİYACI	ARIZA GİREN PERSONEL	ARIZA GİRİŞ ZAMANI
Var	Yok	Yok	Yok	Var	Yok	Yok	942913	13-05-2022 00:00:00

Şekil 8.8. Arıza bilgisinin kontrol edilebildiği ekran



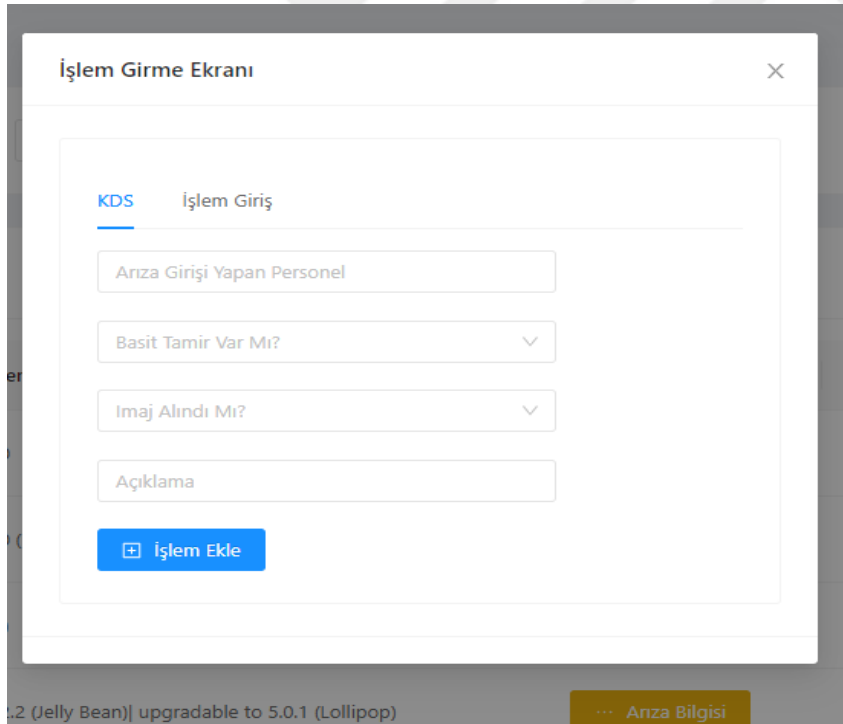
Şekil 8.9. Yapılacak işlemlere ilişkin belirlenen yol haritasının sunulduğu ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



MARKA	MODEL	YAPAN PERSONEL	BİTİRME SÜRESİ	SONUÇ	İŞLETİM SİSTEMİ SÜRÜMÜ	HAFIZA ÇİPİ MARKASI	CİHAZ ŞİFRELİMİ	EKRAN ARIZASI VAR MI	PORT ARIZASI VAR MI	ANAKART ARIZASI VAR MI	CİHAZ PARÇALANMIŞ MI	YAZILIMSAL ARIZA VAR MI	ROOT İHTİYACI VAR MI	PORT DEĞİŞİMİ	BATARYA DEĞİŞİMİ	EP Dİ
Samsung	GT-I8200Q	AHI	25	Fiziksel imaj alındı	4.2.2		x						x			

Şekil 8.10. Mobil cihaza benzer nitelikte yapılan işlemlerin listelendiği ekran



İşlem Girme Ekranı

KDS

İşlem Giriş

Arıza Girişi Yapan Personel

Basit Tamir Var Mı?

İmaj Alındı Mı?

Açıklama

İşlem Ekle

Şekil 8.11. Karar destek sistemiyle yapılan işlemlerin girişinin yapıldığı ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

The screenshot displays a web-based interface titled "İşlem Girme Ekranı" (Operation Entry Screen). At the top, there are two tabs: "KDS" and "İşlem Giriş", with "İşlem Giriş" being the active tab. Below the tabs, there is a list of operations to be performed, each in a separate row with a dropdown arrow on the right. The operations listed are:

- İşlem Yapan Personel
- Ekran Değişimi Var Mı?
- Port Değişimi Var Mı?
- Şifre Çözüldü Mü?
- Batarya Değişimi Var Mı?
- Basit Tamir
- jTag
- Chip-Off
- Root
- TWRP/CVM Kurulumu
- XRY
- UFED Var Mı?
- Oxygen
- Imaj Alındı Mı?
- Açıklama

At the bottom of the screen, there is a blue button with a plus icon and the text "İşlem Ekle" (Add Operation).

Şekil 8.12. Elle Yapılan İşlemlerin Girişinin Yapıldığı Ekran

EK-8. (devam) Mobil cihaz adlı bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Arıza Tespit İşlemde **Sonuç**

Tüm Değerlendirme Sonuçları

Marka	Model	İşletim Sistemi	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Arıza Sil
Samsung	_Galaxy Alpha	Android 4.4.4 (KitKat) upgradable to 5.0.2 (Lollipop)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Acer	_Iconia Tab 7 A1-713HD	Android 4.4.2 (KitKat)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Lenovo	_A2010	Android 5.1 (Lollipop)	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
OnePlus	7pro	android	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Bbmobile	i1453	android	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Samsung	j810f	andorid	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil
Samsung	j810f	android 8.1	İşlem Bilgisi	Değerlendir	Değerlendirme Sonucu	Tüm Süreç	Sil

Şekil 8.13. Sonuçların listelendiği ekran

İşlem Bilgisi

EKRAN DEĞİŞİMİ	PORT DEĞİŞİMİ	BATARYA DEĞİŞİMİ	BASİT TAMİR	JTAG	CHIPOFF	ROOT	TWRP	XRY	UFED	OXYGEN	AÇIKLAMA	XRY AÇIKLAMA	UFED AÇIKLAMA	OXYGEN AÇIKLAMA	İMAJ	İŞLEM GİREN PERSONEL	İŞLEM GİRİŞ ZAMANI
-	Var	-	Var	-	-	-	-	-	-	-	İmaj alındı				Fiziksel İmaj Alındı	Murat	12-05-2022 00:00:00

< 1 >

Şekil 8.14. Mobil cihaza ait işlemlerin listelendiği ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Tüm Süreç Ekranı

Değerlendirme Sonucu

Arıza Bilgisi

ŞİFRELE Mİ	TAMAMEN PARÇALANMIŞ	ANAKART ARIZASI	PORT ARIZASI	EKRAN ARIZASI	YAZILIM ARIZASI	ROOT İHTİVACI	ARIZA GİREN PERSONEL	ARIZA GİRİŞ ZAMANI
Yok	Yok	Var	Var	Yok	Var	Yok		21-06-2022 00:00:00

< 1 >

İşlem Bilgisi

EKRAN DEĞİŞİMİ	PORT DEĞİŞİMİ	BATARYA DEĞİŞİMİ	BASİT TAMİR	JTAG	CHİPOFF	ROOT	TWRP	XRY	UFED	OXYGEN	AÇIKLAMA	XRY AÇIKLAMA	UFED AÇIKLAMA	OXYGEN AÇIKLAMA
-	Var	-	Var	-	-	-	-	-	-	-				

< 1 >

Şekil 8.15. Mobil cihaza ait tüm süreç verilerinin sunulduğu ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Değerlendirme X

1 KULLANIM KOLAYLIĞI

2 YAZILIMIN ANLAŞILIRLIĞI

3 SÜRECE OLAN KATKISI

KULLANIM KOLAYLIĞI

1.Yazılımın kullanımı kolay mı? ☐ Evet ☐ Hayır

2.Yazılımın ara yüzü basit ve kullanıcı dostu muydu? ☐ Evet ☐ Hayır

3.Yazılımı teknik destek almadan kullanabildiniz mi? ☐ Evet ☐ Hayır

4.Yazılımı rahatlıkla kullanabildiniz mi? ☐ Evet ☐ Hayır

5.Programı kullanırken kaldığınız yerden devam, kayıt veya çıkış konularında sorun yaşadınız mı? ☐ Evet ☐ Hayır

İleri

Şekil 8.16. Karar Destek Sistemi Yazılımının Kullanım Kolaylığına İlişkin Geri Bildirim Ekranı

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

Değerlendirme X

✓ KULLANIM KOLAYLIĞI

2 YAZILIMIN ANLAŞILIRLIĞI

3 SÜRECE OLAN KATKISI

YAZILIMIN ANLAŞILIRLIĞI

1.Yazılım gereksiz karmaşık mıydı? ☐ Evet ☐ Hayır

2.Yazılımdaki işlevler bir bütün olarak anlaşılır mıydı? ☐ Evet ☐ Hayır

3.Yazılımın kullanımına ilişkin başlık, yönlendirme, metinler gibi verilen bilgiler yeterli miydi? ☐ Evet ☐ Hayır

4.Yazılımdaki metinlerde dilbilgisi ve anlam açısından bir sorunla karşılaştınız mı? ☐ Evet ☐ Hayır

5.Yazılımın genel tasarımı (renk, renklerin uyumu, yazı tipi) ile ilgili bir sorun tespit ettiniz mi? ☐ Evet ☐ Hayır

6.Kullanım kılavuzu ve ipuçları yeterli miydi? ☐ Evet ☐ Hayır

İleri Geri

Şekil 8.17. Karar Destek Sistemi Yazılımının Anlaşılabilirliğine İlişkin Geri Bildirim Ekranı

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri

✓ KULLANIM KOLAYLIĞI

✓ YAZILIMIN ANLAŞILIRLIĞI

3 SÜRECE OLAN KATKISI

SÜRECE OLAN KATKISI

1.Yazılımın kullanılması sürecin hızlandırılmasına katkı sağladı mı?

☐ Evet ☐ Hayır

2.Yazılımın kullanılması mobil cihaz imaj alma sürecine katkı sağladı mı?

☐ Evet ☐ Hayır

3.Yazılımın kullanılması sırasında önerilen adımlar doğru ve tutarlı şekilde sizi yönlendirdi mi?

☐ Evet ☐ Hayır

4.Yazılımın size katkıları göz önüne alındığında tekrar kullanır mısınız?

☐ Evet ☐ Hayır

5.Yazılımın kullanılması sırasında önerilen adımlar mobil cihaz adli bilişimi sürecini kolaylaştırdı mı?

☐ Evet ☐ Hayır

6.Yazılımda önerilen adımların nasıl yapılacağı konusunda öncesinde bir bilgilendirmeye ihtiyacınız var mıydı?

☐ Evet ☐ Hayır

7.Bu yazılımın genel olarak iş yükünü hafifleteceğini düşünüyor musunuz?

☐ Evet ☐ Hayır

8.Yeni başlayan personelin bu yazılımdan kolaylıkla faydalanabileceğini düşünüyor musunuz?

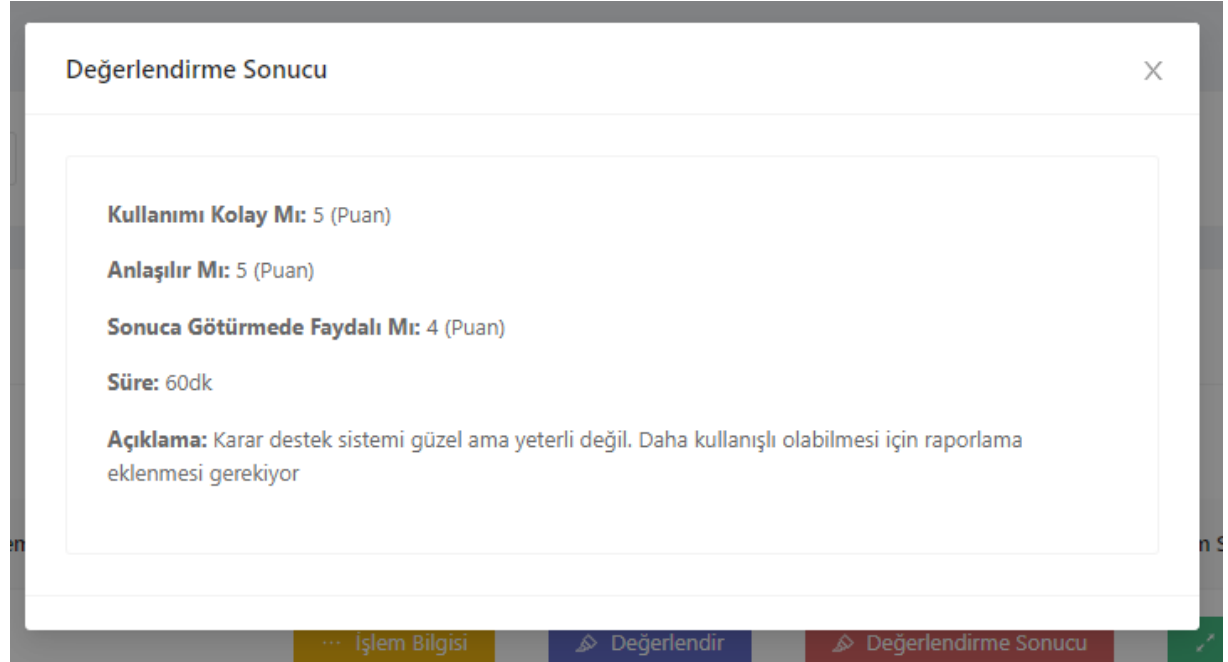
☐ Evet ☐ Hayır

Tamamla

Geri

Şekil 8.18. Karar Destek Sistemi Yazılımının Mobil Cihaz Adli Bilişimi Sürecine Katkısına İlişkin Geri Bildirim Ekranı

EK-8. (devam) Mobil cihaz adlı bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



Şekil 8.19 Yazılıma İlişkin Geri Bildirim Sonuçlarının Gösterildiği Ekran

EK-8. (devam) Mobil cihaz adli bilişiminde imaj alma sürecine ilişkin karar destek sistemi yazılımına ilişkin ekran görüntüleri



Şekil 8.20. Yardım menülerinin olduğu ekran

EK-9. Geri Bildirim Ekranı İçin Uzman Görüş Formu

UZMAN GÖRÜŞÜ FORMU

Mobil cihazın imajının alınması için cihazla ilgili olarak, cihaza ilişkin bilgilerin ve cihazın durumuna ilişkin bilgilerin girilerek, o cihazla ilgili hangi adımların uygulanacağını kullanıcıya sunan bir karar destek yazılımı geliştirilmiştir.

Bu yazılım ile kullanıcı personel özelinde beklenen çıktıları ise şu şekildedir:

- Etkin şekilde kullanılması sonucunda mobil cihaz imaj alma süreçlerini yanlış yöntemler denenmeden hatanın ve sürenin azaltılması,
- Yeni personeli yönlendirebilecek bu sistem sayesinde tecrübeli personelin iş yükünün azaltılması,
- Karar ağacı algoritması sayesinde mobil cihaz adli bilişimi süreçlerinin standardizasyonunun sağlanmasıdır.

Bu yazılımın başarısını ölçmek için **mobil cihaz adli bilişim incelemesi yapan personelin kullanımı** ile ilgili geri dönüşler alınması için bir ölçek geliştirilmesi hedeflenmektedir. Bu sebeple **yazılımın amacına uygunluğundaki başarısını ölçmek** için kullanımı, anlaşılabilirliği ve faydası konularında hangi soruların sorulması gerektiği konusunda değerli katkılarınıza ihtiyaç duyulmaktadır.

Bu kapsamda konuyla ilgili olarak yazılımı kullanan personele sorulmasını uygun gördüğünüz soruları aşağıdaki tabloya işlemeniz beklenmektedir.

	SORU
1	Yazılımın kullanımının kolaylığına ilişkin nasıl bir soru sorulmalıdır?
2	Yazılımın anlaşılabilirliği konusunda nasıl bir soru sorulmalıdır?
3	Sürece olan katkısını ölçmek için nasıl bir soru sorulmalıdır?
4	Konuyla ilgili fayda gördüğünüz diğer sorular varsa belirtiniz.

Uzmanlık alanlarınız:				
Bu alandaki tecrübe yılınız:	Yaşınız:			
Eğitim düzeyiniz:	Ön lisans ☐	Lisans ☐	Y. Lisans ☐	Doktora ☐
Çalıştığınız sektör:	Kamu ☐		Özel ☐	

EK-10. Geri Bildirim Ekranı İçin Uzman Görüş Formu (İngilizce)

FORM OF EXPERT OPINION

In order to get acquisition of the mobile device, a decision support software has been developed that provides the user with which action to take regarding that device by entering the information about the device and the status of the device.

With this software, the expected outputs for user are as follows:

- As a result of effective use, reducing the error and time of mobile device acquisition processes without trying wrong methods,
- Reducing the workload of experienced personnel thanks to this system that can direct new personnel,
- Ensuring the standardization of mobile device forensics processes thanks to the decision tree algorithm.

In order to measure the success of this software, it is aimed to develop a scale to receive feedback on the use of mobile device forensics personnel. For this reason, your valuable contributions are needed on what questions should be asked about the **use, clarity and usefulness of the software** in order to measure the success of the software.

In this context, you are expected to write down the questions you deem appropriate to be asked to the personnel using the software in the table below.

	QUESTIONS
1	What question should be asked about the ease of use of the software?
2	What kind of question should be asked about the comprehensibility of the software?
3	What kind of question should be asked to measure its contribution to the process?
4	If there are other questions that you find useful on the subject, please specify.

Information about your expertise:

Areas of expertise (multiple if needs)	Experience in the field (years)	Graduation degree	Sector worked
		☐ Associate,	☐ Private
	Age	☐ Bachelor's,	☐ Public
		☐ Master of Science,	
		☐ PhD	

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : YILMAZ, Furkan

Uyruğu : T.C.

Doğum tarihi ve yeri :

Medeni hali : Evli

Telefon :

E-posta :

Eğitim

<u>Derecesi</u>	<u>Okul</u>	<u>Mezuniyet</u>
Doktora	Gazi Üniversitesi/Adli Bilişim ABD	2023
Yüksek Lisans	Anadolu Üniversitesi/Sosyoloji ABD	2015
Lisans	Ankara Üniversitesi/Hukuk	2022
Lisans	Polis Akademisi/Güvenlik Bilimleri	2011

İş Deneyimi

2011-2014 Eskişehir Emniyet Müdürlüğü

2014- ... Emniyet Genel Müdürlüğü/Siber Suçlarla Mücadele Daire Başkanlığı

Yabancı Dil

İngilizce, Fransızca

Yayınlar

Yılmaz, F. ve Güllüpnar, F. (2020). Türkiye’de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 15(1), 5371-5409.

Yılmaz, F. ve Çakır, H. (2021). Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7 (1), 25-46.

Yılmaz, F. ve Karataş, S. (2022). Karar Destek Sistemi, *Yapay Zekâ Kuramdan Uygulamaya*, (1), 355-382.



GAZİLİ OLMAK AYRICALIKTIR.