T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MOBİL CİHAZLAR İÇİN EKRAN PARMAK İZLERİNDEN PAROLA TESPİTİ YAPILARAK YENİ BİR SÜREÇ TANIMLAMA MODELİNİN GELİŞTİRİLMESİ VE ADLİ BİLİŞİM İNCELEMESİ YAPILMASI

Ömer Faruk YAKUT

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

HAZİRAN 2020

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

MOBİL CİHAZLAR İÇİN EKRAN PARMAK İZLERİNDEN PAROLA TESPİTİ YAPILARAK YENİ BİR SÜREÇ TANIMLAMA MODELİNİN GELİŞTİRİLMESİ VE ADLİ BİLİŞİM İNCELEMESİ YAPILMASI

Tez Yazarı
Ömer Faruk YAKUT

Danışman
Dr. Öğr. Üyesi Fatih ERTAM

HAZİRAN 2020
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Mobil Cihazlar için Ekran Parmak İzlerinden Parola Tespiti Yapılarak Yeni Bir Süreç Tanımlama Modelinin Geliştirilmesi ve Adli Bilişim İncelemesi Yapılması
Yazarı:	Ömer Faruk YAKUT
İlk Teslim Tarihi:	15.05.2020
Savunma Tarihi:	15.06.2020

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

İmza

Danışman: Dr. Öğr. Üyesi Fatih ERTAM — Onayladım
Fırat Üniversitesi, Teknoloji Fakültesi

Başkan: Dr. Öğr. Üyesi Emrah AYDEMİR — Onayladım
Kırşehir Ahi Evran Üniversitesi, Mühendislik Fakültesi

Üye: Doç. Dr. Türker TUNCER — Onayladım
Fırat Üniversitesi, Teknoloji Fakültesi

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Soner ÖZGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Mobil Cihazlar için Ekran Parmak İzlerinden Parola Tespiti Yapılarak Yeni Bir Süreç Tanımlama Modelinin Geliştirilmesi ve Adli Bilişim İncelemesi Yapılması" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

15.06.2020

Ömer Faruk YAKUT

ÖNSÖZ

Tez çalışma aşamasında maddi manevi destek ve yardımlarını esirgemeyen kıymetli danışmanım Dr. Öğr. Üyesi Fatih ERTAM' a sonsuz teşekkürlerimi sunarım.

Desen tanıma bölümündeki görüntü işleme yöntemleri ile ilgili katkılarından dolayı Doç. Dr. Türker TUNCER' e ve çalışma sürecinde bölüm imkânlarını kullanıma açan değerli Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Öğretim elemanlarına teşekkürü bir borç bilirim.

Bu tez çalışması süresince her an destekçim ve umut vericim olan sevgili eşim Hilal YAKUT'a, sevgili oğullarım Eymen ve Uğur Mahir'e teşekkür ederim.

Bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **TEKF.20.06** protokol numaralı proje ile desteklenmiştir.

Ömer Faruk YAKUT
ELAZIĞ, 2020

İÇİNDEKİLER

Sayfa

ÖNSÖZ iv
İÇİNDEKİLER v
ÖZET vii
ABSTRACT viii
ŞEKİLLER LİSTESİ ix
TABLOLAR LİSTESİ xi
KISALTMALAR xii

1. GİRİŞ 1
1.1. Tezin Amacı 3
1.2. Tezin Yapısı 4

2. MOBİL CİHAZLARDA ADLİ BİLİŞİM 5
2.1. Mobil Cihazların Genel Yapısı 5
2.2. Mobil Cihaz Türleri 5
2.3. Mobil İşletim Sistemleri 6
2.4. Dijital Kanıtlar ve Adli Bilişimin Temel Aşamaları 13
2.5. Adli Bilişim Çeşitleri 15
2.6. Adli Kopya Alma Yöntemleri 16
2.7. Adli Bilişim Süreç Modelleri 19
2.8. Mobil Adli Bilişim Süreç Aşamaları 25

3. DERİN ÖĞRENME YAKLAŞIMLARI VE ÖZELLİK ÇIKARIMI YÖNTEMİ 28
3.1. Evrişimli Sinir Ağları (CNN) 28
3.1.1. MobileNet-V2 Mimarisi 30
3.1.2. SqueezeNet Mimarisi 31
3.2. Minimum İhtiyaç Maksimum Alaka (Minimum Redundancy Maximum Relevance) Özellik Seçimi 32

4. ÇALIŞMA METODOLOJİSİ 34
4.1. Desen Kilidi Tespit Yöntemi Ön Hazırlık Aşaması 34
4.2. Veri Seti Oluşturma Aşaması 37
4.3. Mobil Cihaz Analizi Hazırlık Aşaması 40

5. EKRAN İZLERİNDEN DESEN KİLİDİ TESPİT YÖNTEMİ 42
5.1. Desen Tanıma Yöntemi Basamakları 42

6. MOBİL CİHAZLARIN EKRAN İZLERİNDEN PAROLA TESPİT YÖNTEMİ İLE İLİŞKİLİ YENİ SÜREÇ TANIMLAMA MODELİ 48
6.1. Koruma Aşaması Süreç Modeli 49
6.2. Elde Etme Süreç Modeli 50
6.3. Analiz Aşaması Süreç Modeli 52
6.4. Raporlama aşaması süreç modeli 53

7. MOBİL CİHAZ ADLİ BİLİŞİM ANALİZ UYGULAMASI 54
7.1. Koruma Aşaması 54
7.2. Elde Etme Aşaması 54

7.3. Analiz Aşaması 60
7.4. Raporlama Aşaması 74
8. SONUÇLAR 76
ÖNERİLER 78
KAYNAKLAR 79
ÖZGEÇMİŞ

ÖZET

Mobil Cihazlar için Ekran Parmak İzlerinden Parola Tespiti Yapılarak Yeni Bir Süreç Tanımlama Modelinin Geliştirilmesi ve Adli Bilişim İncelemesi Yapılması

Ömer Faruk YAKUT

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Haziran 2020, Sayfa: xiii + 89

Hızla gelişen mobil cihaz teknolojisinin getirdiği yenilikler günlük işlemlerin mobil cihazlar ile rahatlıkla yürütülmesine imkân tanımıştır. Sosyal hayatın önemli bir kısmını oluşturan sosyal medya platformları ve anlık mesajlaşma uygulamaları yaygın bir şekilde mobil cihazlar üzerinden kullanılmaktadır. Bu özellikleri ile iş ve sosyal hayatın önemli bir parçası olan mobil cihazlar, farklı dijital suç ve kanıtların birincil kaynağını oluşturmakta ve kullanıcısıyla bütünleşmiş yapısı sayesinde suç soruşturmalarında başvurulan önemli delil kaynağı haline gelmiştir. Mobil cihazlar önemli kişisel verileri barındırmaktadır. Bu durum cihaz üreticilerinin verilerin güvenliği için farklı güvenlik uygulamaları ve şifreleme yöntemleri geliştirmesine neden olmuştur. Suç soruşturmalarında mobil cihazlardan kanıt elde etmek adli merciler için suçun aydınlatılmasında son derece önemli hale gelmiştir. Bu nedenle mobil cihazlardan kanıt elde etme yöntemleri, kullanılan güvenlik ve şifreleme yöntemleri ile paralel ilerlemeye mecburdur. Aksi halde suçun aydınlatılması için mobil cihazlardan kanıt elde edilemeyeceğinden adli mercilerin sağlıklı ve hızlı karar vermesi zorlaşacaktır. Adli bilişim alanında mobil cihazlardan kanıt elde etmek için öncelikle cihazın adli kopyası alınarak, kopya üzerinden işlemler yürütülmektedir.

Mobil cihazlarda ekran kilidinin kullanılması çoğu cihazın mantıksal kopyasının alınması önünde büyük engel teşkil etmektedir. Bu tez çalışmasında mobil cihaz adli bilişim süreçleri, adli kopya alma yöntemleri ve adli araç setleri irdelenmiş, cihaz ekranı üzerindeki parmak izlerinden desen kilidi tespit edilmesi ile ilgili yüksek sınıflandırma başarısına sahip yeni bir yöntem geliştirilmiştir. Ayrıca geliştirilen yöntemle ilişkili olarak yeni bir mobil cihaz inceleme süreç modeli önerilerek örnek mobil cihaz adli analizi yapılmıştır.

Anahtar Kelimeler: Adli soruşturma modelleri, Mobil adli bilişimi, Android cihazlar, Mobil ekran izleri, Parola tespiti.

ABSTRACT

Developing a New Process Identification Model by Making Password Detection from latent fingerprint for Mobile Devices and Digital Forensics Analysis

Ömer Faruk YAKUT

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

June 2020, Pages: xiii + 89

The innovations brought by the rapidly developing mobile device technology allowed daily transactions to be carried out easily with mobile devices. Social media platforms and instant messaging applications, which form an important part of social life, are widely used with mobile devices. Social media platforms and instant messaging applications, which form an important part of social life, are widely used with mobile devices. Mobile devices, which are an important part of business and social life, are the primary source of digital crime and digital evidence. Thanks to its integrated structure with the user of mobile devices, it has become the most important source of evidence used in criminal investigations. The fact that mobile devices contain important personal data has caused device manufacturers to develop different security applications and encryption methods for the security of this data. In forensic investigations, obtaining evidence from mobile devices has become extremely important in the clarification of the investigation. Therefore, methods of obtaining evidence from mobile devices must proceed in parallel with the security and encryption methods used. Otherwise, it will be difficult for the judicial authorities to make a healthy and quick decision, since evidence cannot be obtained from mobile devices to clarify the crime. In order to obtain evidence from mobile devices in the field of forensic information, firstly a forensic copy of the device is taken and transactions are carried out over the copy.

Using screen locks on mobile devices is a major obstacle to making a logical copy of most devices. In this thesis, mobile device forensic processes, forensic copying methods and forensic tool sets are examined. A new method with high classification success has been developed for detecting pattern lock from fingerprints on the mobile device screen. In addition, a new mobile device review process model was proposed in relation to the developed method, and a sample forensic analysis was conducted.

Keywords: Forensic investigation models, Mobile forensic computing, Android devices, Mobile screen traces, Password detection.

ŞEKİLLER LİSTESİ

Sayfa

Şekil 2.1. Windows Mobile mimarisi 9

Şekil 2.2. Android mimarisi 12

Şekil 2.3. Mobil cihaz adli araç sınıflandırma sistemi 17

Şekil 2.4. Mobil cihazlarda adli bilişim aşamaları 25

Şekil 3.1. Genel CNN mimarisi 29

Şekil 3.2. MobileNetV2 Evrişimli Bloklar 30

Şekil 3.3. SqueezeNet mimari boyutları 32

Şekil 4.1. Dört farklı yüzeyin mobil cihaz ekranı üzerinde bıraktığı kaydırma ve baskı izi 34

Şekil 4.2. Ekran üzerindeki desen izlerinin belirginleştirme aşaması 35

Şekil 4.3. Farklı dalga boylarındaki ışık altında ekran izlerinin görünümü 36

Şekil 4.4. Örnek desen oluşturma şeması 37

Şekil 4.5. Veri seti için kullanılan 20 adet desen 38

Şekil 4.6. Önerilen yöntemin çalışma şeması 39

Şekil 4.7. Kullanılan donanımların konumlandırılması ile ilgili görseller 40

Şekil 5.1. Önerilen modelin grafiksel şeması 42

Şekil 5.2. Önerilen yöntemin sözde kodu 43

Şekil 5.3. TmRMR yinelemeli özellik seçim işlemi 47

Şekil 6.1. Koruma aşaması süreç şeması 49

Şekil 6.2. Elde etme aşaması süreç şeması 51

Şekil 6.3. İnceleme aşaması süreç şeması 52

Şekil 6.4. Raporlama aşaması süreç şeması 53

Şekil 7.1. XRY yazılımının Samsung SM-J530F modeline ait desteklenen adli kopya formatları 54

Şekil 7.2. Oxygen Forensic yazılımı tarafından desteklenen Samsung J serisi modeller 55

Şekil 7.3. UFED4PC yazılımının Samsung SM-J530F model cihaz için desteklediği adli kopya alma yöntemleri 56

Şekil 7.4. UFED4PC yazılımının desteklediği Samsung SM-J530F model mobil cihazın fiziksel adli kopya yöntemleri 57

Şekil 7.5. Önerilen yöntemle tespit edilen ekran desen şifresi 58

Şekil 7.6. Ekran izlerinin benzerlik gösterdiği desen şifresi 58

Şekil 7.7. Test cihazımız ile aynı yonga setine sahip muadil modelin UFED 4PC adli aracı tarafından desteklenen adli kopya yöntemleri 59

Şekil 7.8. Adli kopya ayıklama özeti 60

Şekil 7.9. Çağrı kayıtlarının tutulduğu calllog.db veri tabanı görünümü 61
Şekil 7.10. mmssms.db veri tabanı görünümü 62
Şekil 7.11. SMS kaydın hex görüntüsü 63
Şekil 7.12. Konum bilgileri açık olan resim dosyasına ait exif bilgileri 64
Şekil 7.13. Resim dosyasının tespit edilen konumunun harita gösterimi 65
Şekil 7.14. library.db dosyası içerisinde tutulan bazı kayıtlar 67
Şekil 7.15. package_verification.db dosyası içerisinde tutulan bazı kayıtlar 68
Şekil 7.16. suggestions.db dosyası içerisinde tutulan bazı kayıtlar 68
Şekil 7.17. Web Data içerisinde elde edilen otomatik doldurma kayıtları 72

TABLOLAR LİSTESİ

Sayfa

Tablo 2.1. ACPO ilkeleri 20

Tablo 3.1. MobileNetV2 Ana Mimarisi 31

Tablo 4.1. Kullanılan donanımlar. 39

Tablo 4.2. Örnek mobil adli bilişim analizinde kullanılacak yazılım ve donanımlar. 41

Tablo 5.1. LDA ile toplanan ekran kilidi desen görüntü veri kümesinde yöntemimizin sonuçları 46

Tablo 5.2. Önerilen derin hafif sıklet tümleşik özellik tabanlı yöntem ile yaygın olarak tercih edilen bazı derin ağların karşılaştırmaları. 47

Tablo 6.1. Android kilit deseninin kombinasyonları 48

Tablo 7.1. Cihaz temel bilgileri ve yolu 61

Tablo 7.2. localappstate.db dosyası içerindeki bazı tablo içerikleri ve açıklamaları 66

Tablo 7.3. Android cihazlarda çalışan bazı hizmet türleri ve grup yetkileri 69

Tablo 7.4. Paket adı ve uygulama adı uyuşan ve uyuşmayan uygulama örnekleri. 71

Tablo 7.5. Farklı adli kopya formatları içerisinde elde edilen verilerin karşılaştırması. 73

Tablo 7.6. Analiz edilen cihaza ait raporda belirtilecek temel bilgiler. 74

Tablo 7.7. Tespit edilen kanıt ile ilgili raporda belirtilmesi gereken öz nitelik bilgileri. 75

KISALTMALAR

ACC : Accuracy
ACPO : Association of Chief Police Officers
ADB : Android Debug Bridge
ADFM : Abstract Digital Forensic Model
AFC2 : Apple File Conduit 2
ANN : Artificial neural networks,
API : Application Programming Interface
APK : Android Package
APP : Application Store
ARM : Acorn Rischine
CD : Compact Disc
CFFTPM : Cyber Forensic Field Triage Process Model
CFTT : Computer Forensics Tool Testing Program
CNN : Convolution Neural Networks
CPU : Central Processing Unit
DFRWS : Digital Forensics Research Conference
DMR : Digital rights management
DVD : Digital Versatile (Video) Disc
EDIP : Enhanced Digital Investigation Process Model
EEPROM : Electronically Erasable Programmable Read-Only Memory
E-POSTA : Elektronik Posta
FN : False negatif
FP : False pozitif
GCFIPM : General Computer Forensic Investigation Process Model
GID : Group Identification Number
GM : Geometric mean
GNOME : GNU Network Object Model Environment
GNU : Graphical User Interface
GPS : Global Positioning System
HLR : Home Location Register
IDE : Integrated Development Environment
IDIP : Integrated Digital Investigation Process
IOT : Internet of Things
IPC : interproses communication
IrDA : Infrared Data Association
İos : iPhone/iPad OS
JTAG : Joint Test Action Group
LCD : Liquid Crystal Display
LDA : Linear Discriminant Analysis
LDD : Logical Device Driver
MDS : Mobile Data Servic
MMS : Multimedia Messaging Service
MP3 : MPEG-1 Audio Layer III
mRMR : Minimum Redundancy Maximum Relevance

MSC : Mobile Switching Center
MTD : Mobile Threat Defense
MTK : MediaTek
NFC : Near Field Comminucation
NIST : National Institute of Standarts and Technology
OHA : Open Handset Alliance
OS : Operating System
PCB : Printed Circuit Board
PDA : Personal Digital Assistant
PDD : Physical Device Driver
PIN : Personal identification number
RAM : Random Access Memory
ReLu : Rectified linear unit
RIM : Research in Motion
ROM : Read Only Memory
SD : Secure Digital
SIM : Subscriber Identity Module
SMS : Short Message Service
SQL : Structured Query Language
SSH : Secure Shell
TmRMR : Tekrarlanan Minimum Redundancy Maximum Relevance
TN : True negatif
TP : True pozitif
UID : User Identification Number
USB : Universal Serial Bus
USDOJ : United States Department of Justice
VLR : Visitor Recording locations
VM : Virtual Machines
WiFi : Wireless Fidelity
WM : Windows Mobile
WM : Windows Mobile
XML : Extensible Markup Language
YAFFS : Yet Another Flash File System

1. GİRİŞ

Başlangıçta dikkatsiz bir araştırmacı tarafından silinen bir veri tabanı üzerindeki bilgilerin kurtarılması için kullanılan adli teknikler olarak ortaya çıkan adli bilişim kavramı zamanla önem kazanmıştır. Adli bilişim kavramının kazandığı önem, aşağıda belirtilen durumların oluşması ile artmıştır [1].

- İncelenen sistemlerde depolama ortamlarının boyutunun küçük olması,
- Az sayıda dosya sistemi formatlarının varlığı,
- Şifreleme yöntemlerindeki başarısız denemeler olması,
- Birçok başarılı veri kurtarma yazılımlarının ortaya çıkmasıyla birlikte silinmiş olduğu düşünülen artık verilerin kurtarılmasında gösterilen başarı.

Bilgisayar ve ağ teknolojilerinde yaşanan gelişmeler ile birlikte suçlular, adli bilişim tekniklerinin daha fazla farkına varmakta ve suç işlemek için bilgisayar ve ağları daha karmaşık bir şekilde kullanmaktadır [2]. Bilgisayar aygıtları arasındaki farklı nitelikler nedeniyle adli bilişim kavramı: bilgisayar adli bilişimi, hafıza adli bilişimi, multimedya adli bilişimi, ağ adli bilişimi, küçük ölçekli cihaz adli bilişimi veya mobil cihaz adli bilişim olarak farklı alt alanlara ayrılmıştır [3]. Buna bağlı olarak her bir alt alanda dijital kanıt elde etmek için kullanılan yöntem ve araçlar farklılık gösterdiği gibi bu alanlarda karşılaşılan zorluklarda farklılaşmaktadır.

Bilgisayar teknolojisindeki hızlı gelişmelere paralel olarak gelişen mobil cihaz teknolojisi getirdiği birçok kolaylık ve yenilik ile hayatın vazgeçilmez bir parçası olmayı başarmıştır. Motorola firmasının 1983 yılında tanıttığı DynaTAC 8000X'den sonra dünya üzerinde cep telefonu kullanıcı sayısında meydana gelen artışa paralel olarak mobil cihaz teknolojisi büyük bir ivme kazanmıştır. 2007 yıllında Apple firması tarafından iphone 1 isimli ilk akıllı telefonun dünyaya tanıtılmasıyla yeni bir dönemin kapıları aralanmıştır. 2010 yılında Samsung firması Android işletim sistemine sahip ilk akıllı cep telefonunu piyasaya sürmesi ile birlikte, iphone'nin piyasadaki hâkimiyetine son vermeyi başarmıştır. "HootSuite" ve "We Are Social" in yayınladığı "Digital in 2019" raporlarına göre 5,112 milyar mobil cihaz kullanıcısı olduğu ve bu sayının toplam dünya nüfusunun %67 sini oluşturduğu belirtilmiştir [4].

Mobil cihaz teknolojisindeki devrim niteliğindeki donanım ve yazılım tabanlı gelişmeler bu cihazları sadece haberleşme aracı olmaktan çok öteye taşıyarak, kullanıcısının özel, kurumsal ve kamusal işlerinin büyük kısmını yürüttüğü ve takip ettiği taşınabilir bilgisayar haline gelmesine sebep olmuştur. Bu özellikleri ile kişisel bir bilgi kümesi barındıran mobil cihazlar siber saldırıların hedefi haline gelerek suç ile ilgili veri barındırma ihtimalleri taşımaları sebebiyle adli bilişimin konusu haline gelmiştir.

Cep telefonlarından veri toplanması son yıllarda daha önemli bir hale gelmiştir. Ancak akıllı cihaz teknolojisindeki gelişmeler ve güvenlik açıklarının kapatılmasıyla bu kazanımı elde etmek

gittikçe zor hale gelmiştir [5]. Giderek artan format uyumsuzlukları, şifreleme gibi karmaşıklık güvenlik mekanizmalarının kullanılması ve anti adli bilişim yöntemlerinin artması adli bilişim incelemelerindeki kazanımları azaltmıştır. Bu durum adli kopya oluşturma ve analiz aşamalarında geçen süreleri arttıracak, zor kazanılmış yeteneklerin de gelecek yıllarda kaybolmasına sebep olacaktır [1].

Mobil cihaz içerisindeki verileri depolama ortamından çıkarmak ve belgelemek için birden fazla araç ve yöntem kullanmak gerekebilir. Bazen bir soruşturma için yalnızca SMS içerikleri önemliyken, bazen dosya sisteminin veya fiziksel hafızasının tamamının çıkarılması gerekmektedir. Bu durumda manuel, mantıksal, dosya sistemi ve fiziksel adli kopya yöntemleri gibi farklı yöntemler uygulanabilir [6]. Bu yöntemlerden her biri, istenen miktarda veri çıkarmak için cihazın farklı niteliklerini kullanmaktadır.

Kullanılan işletim sistemleri ve yonga setlerinin çeşitliliği adli kopya alma yöntemlerini ve adli kopya içerisindeki verilerin analiz süreçlerini olumsuz şekilde etkilemeye devam etmektedir. Örneğin; Android 6 sürümüne sahip cihaz içerisindeki uygulama verilerinin kopyasının alınması için, uygulama sürümü düşürme yöntemi uygulanarak veriler başarılı şekilde alınırken, Android 7 ve üst sürümünü kullanan mobil cihaza bu yöntem uygulandığında veri kayıpları yaşanmasına neden olmaktadır.

Dijital materyallerin adli kopya alma ve analiz süreçleri adli araçlara tamamen bağımlı halde yürütülmektedir [7]. Kullanılan adli araçların genellikle ticari yazılım olmaları, bu alanda yapılan çalışmaların ortak paydada birleştirilmesi önünde en büyük engeldir. Mobil cihaz teknolojinin hızlı ilerleyişine karşılık adli bilişim alanında yapılan çalışmaların da en az aynı hızda ilerlemesi adli soruşturmaların aydınlatılması için büyük öneme sahiptir.

Adli araçların yeterlilikleri ile ilgili test işlemlerini gerçek ve tam anlamı ile gerçekleştirecek bir kurumun varlığı adli araç takımlarına duyulan güvene bir standart getirecektir. Bu konuda en dikkat çeken proje Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) Bilgisayar Adli Tıp Aleti Testi (CFTT) Projesi'dir. CFTT Projesi 2000 yılından bu yana faaliyettedir. Disk görüntüleme, medya hazırlığı, dosya oyma ve anahtar terim görevlerini kapsayan, adli bilişim araçları takım performansını potansiyel olarak doğrulamak ve değerlendirmek için sağlam test yöntemleri oluşturmaya çalışmaktadır [8]. Ancak bu çalışmalarda elde edilen test sonuçlarının açıklanması için geçen sürede, araçların test edilen versiyonları kullanılmaya devam edilecektir. Hatta ticari aracın bu süre zarfında yeni versiyona geçmiş olma ihtimalleri de olduğu düşünülürse CFTT testi tarafından herhangi bir olumsuzluk tespit edilse dahi bu araçların kullanımının önüne geçemediğinden tam işlevsellik gösteremeyecektir [7]. Bu nedenle adli bilişim alanında etkin bir işleyişin gerçekleşebilmesi için devletler, kanun uygulayıcılar, akademik personeller ve bu alanda hizmet veren ticari işletmelerin organik bir ilişki içinde çalışması gerekmektedir [9].

Başlangıçta mobil cihazlar radyo frekanslarını kullanan bir tür elektromanyetik alan oluşturan iki yönlü telsizler olarak tanımlanmıştır. Adli bilişim açısından cep telefonları içerisinden elde edilebilecek veriler; konum bilgisi, arama bilgileri ve cihaza yerel olarak kayıt edilmiş bilgiler olarak sınıflandırılmıştır [10]. Mobil cihaz teknolojisindeki gelişmeler ile birlikte sınırlı işlem ve bellek kaynaklarına sahip, farklı CPU mimarisi ile çeşitli işletim sistemi (OS) sürümlerine sahip mobil cihazların üretilmesi, bu cihazların adli kopya edinimi ve analizini zorlaştırmaktadır [11]. Mobil cihaz pazarındaki büyümenin devam etmesi, üretici ve model çeşitliliğine neden olmaktadır. Bu nedenle profesyonel bir araştırmacının, mobil cihazlardan dâhili verileri toplamak için en uygun adli araçları seçmesi gerekmektedir [12]. Örneğin Windows mobil akıllı telefonu için adli kanıt kurtarma tekniklerinin karşılaştırıldığı çalışmada mobil cihazda tutulan bilgilerin eksiksiz bir şekilde alınamadığı, ayrıca farklı araçlar ile elde edilen bilgilerin çelişkili olduğu belirtilmiştir [13]. Piyasada, adli bilişim uzmanlarının karşılaşacağı tüm mobil cihazların içerisindeki verileri toplamada yeterli olacak tek bir araç mevcut değildir. Bu nedenle uygun adli aracın seçiminde analizin amacı, analizcinin sahip olduğu kaynaklar, incelenecek mobil cihaz türü ve modeli gibi faktörlerin belirlenmesi gerekmektedir [14].

Adli kopyası alınamayan mobil cihazların analizi ve raporlanması genel olarak mümkün değildir. Bu nedenle adli kopya alma ve analiz aşaması mobil adli bilişim süreçlerinin en önemli kısmını oluşturmaktadır.

1.1. Tezin Amacı

Bu tezin amacı mobil cihazların ekran izlerinden desen kilidinin tespiti için derin öğrenme yöntemleri ile desteklenen otomatik bir yöntem geliştirmek ve buna bağlı olarak yeni bir mobil adli bilişimi süreç metodolojisi önermektir. Geliştirilen desen kilidi tespit yönteminin mobil cihaz analiz süreçlerinin tamamına etki edeceği değerlendirilmiştir. Tez çalışmasında geliştirilen desen kilidi tespit yöntemi ve önerilen mobil cihaz metodolojisi yaygın kullanımı nedeniyle Android işletim sistemine sahip mobil cihazlar temel alınarak geliştirilmiştir. Geliştirilen yöntem, ekran kilidi yöntemi olarak desen kullanan bütün işletim sistemine sahip mobil cihazlar içinde uygulanabilmektedir. Tez çalışmasında desen kilidi tespit yöntemi için derin öğrenme teknikleri kullanılarak sınıflandırma işlemi yapılmıştır. Geliştirilen yöntemin gelecek yıllarda yeni yapay zekâ modellemeleri ile daha başarılı sonuçlar alması ve yeni uygulama alanlarına ilham vermesi hedeflenmiştir. Desen kilidi tespit yöntemi ile elde edilen sonuçlar sayesinde, durmuş olan adli kopya alma süreçlerinin tekrar devam etmesi amaçlanmıştır. Ayrıca önerilen desen kilidi tespit yönteminin mobil cihaz süreçlerine dahil edilerek, mobil adli bilişim aşamalarında karşılaşılan aksaklık ve kayıpların önüne geçilmesi, çalışmanın ön görülen kazanımları arasındadır.

1.2. Tezin Yapısı

Bu tez çalışması Giriş Bölümü dahil 8 bölümden oluşmaktadır.

Bölüm 2'de Mobil Cihazlarda Adli Bilişim başlığı altında; Mobil cihazların genel yapısı, mobil cihaz türleri, mobil işletim sistemleri ve adli bilişim kavramı açıklanmış, adli bilişimin alt dallarına değinilerek, mobil adli bilişimin tanımı, mobil adli bilişim aşamaları, veri çıkarma yöntemleri ile mobil cihaz metodolojilerine yer verilmiştir.

Bölüm 3'de Derin öğrenme yöntemleri ile ilgili açıklamalar ve literatür bilgisine bu aşamada yer verilmiştir.

Bölüm 4'de çalışma metodolojisi anlatılarak, kullanılacak donanım ve yazılımlar ile yapılan ön hazırlıklara yer verilmiştir. Tez çalışmasında kullanılacak veri setinin oluşturulma süreci ve yöntemlerine yine bu kısımda değinilmiştir.

Bölüm 5'de Önerilen derin öğrenme yaklaşımına dayalı desen kilidi tespit yönteminin veri setine uygulama aşaması ele alınmış ve elde edilen sonuçların değerlendirilmesi yapılmıştır.

Bölüm 6'da Bölüm 5'de uygulanan desen kilidi tanıma yöntemi ile ilişkili olarak önerilen mobil cihaz süreç modelinin aşamaları ayrıntılı olarak ele alınmış ve sonuçları değerlendirilmiştir.

Bölüm 7'da önerilen desen kilidi tespit yöntemi ve mobil cihaz süreçleri ile ilişkili adli kopya alma ve analiz işlemlerinin uygulaması gerçekleştirilmiştir.

Bölüm 8'de ise elde edilen sonuçlar ile birlikte tez çalışmasının hedef kazanımlarının hangi oranda gerçekleştiği ile ilgili değerlendirilmeler yapılmıştır.

2. MOBİL CİHAZLARDA ADLİ BİLİŞİM

Mobil cihazlar, geliştirilen uygulamalar sayesinde basit bir bilgisayarın yapabileceği işleri yapabilen sınırlı hafıza ve işlem gücüne sahip, mobil altyapıları kullanabilen küçültülmüş bilgisayarlardır. Mobil cihazların çoklu işlem becerilerini gerçekleştirebilmek için Symbian, iOS, Android OS ve Windows Mobile vb. farklı işletim sistemleri geliştirilmiştir [15].

2.1. Mobil Cihazların Genel Yapısı

Çoğu mobil cihaz hareketlilik için tasarlanmış, kompakt, pille çalışan hafif ve temel çoklu işlem yeteneklerine sahiptir. İçerisinde mikro işlemci, salt okunur bellek (ROM), rastgele erişim belleği (RAM), radyo modülü, dijital sinyal işlemcisi, mikrofon, hoparlör, çeşitli donanımsal tuşlar, ara yüzler ve LCD ekran mevcuttur [16]. Ayrıca gereken destekleyici yongalar ile önemli miktarda dahili bellek kapasitesi bulunur. İşletim sistemi NAND ve NOR bellek içerisinde bulunurken, dahili (SD) hafıza kartı yuvaları sayesinde kapasite 64 GB ile 2 TB arasında değişen boyutlara çıkarılabilir. Kızılötesi (IrDA), Bluetooth, yakın alan iletişimi gibi kablosuz iletişim (NFC) ve kablosuz ağ (WiFi) ayrıca cihaza yerleştirilebilir ve senkronizasyon protokollerini destekleyebilir. Farklı mobil cihazlar boyut ağırlık, işlemci hızı, bellek kapasitesi gibi farklı teknik ve fiziksel özelliklere sahiptir. Ayrıca, mobil cihazlar kişisel bilgisayarların özelliklerinin yanında, taşınabilen GPS, kamera, MP3 çalar vb. farklı cihazların özelliklerini taşıyabilirler [17].

2.2. Mobil Cihaz Türleri

Mobil cihazlar dokunmatik veya dokunmatik olmayan bir ekranla, bazen de bir minik klavye ile birlikte kullanılan, internete bağlanabilen ve çoklu ortam uygulamalarını çalıştırabilen kolayca taşınan bilgisayarlardır [18]. Mobil cihazları çeşitlilikleri dolayısı ile kategoriye ayırmak zor olsa da genel olarak cep telefonları, kişisel dijital asistan (PDA), tablet bilgisayar ve akıllı telefonlar olarak sınıflandırılmıştır.

Cep Telefonu

Cep telefonları genel olarak bilgi iletmek için radyo frekans dalgalarını kullanan ahizeden gelen radyo sinyalini en yakın baz istasyonu anteni vasıtasıyla şebekeye ve hedefine ileten taşınabilir iki yönlü telsizlerdir [10]. Cep telefonları hızla gelişen mobil cihaz teknolojisi ile birlikte çoklu ve hızlı işlem kapasitesine ulaşmıştır. Çoklu ortam uygulama ve donanımları ile uyum içerisinde çalışan bu cihazlar, hücresel olmayan veri taşıma yöntemleri ile veri taşıyabilen, kablosuz bağlantılar ile internet üzerinden veri alışverişi yapabilen akıllı cihazlara dönüşmüştür.

Cep Bilgisayarları

Cep bilgisayarları PDA (Personal Digital Assistant), kişisel dijital asistanlar avucunuzun içine sığabilecek kadar küçük, ağ bağlantısına sahip bilgisayarlardır. PDA'lar, Apple Newton ve Palm Pilot gibi birinci nesil cihazlardan başlayarak yıllar içinde geliştirildi. İlk dönemlerde PDA'lar, takvim ve not tutma gibi özellikler sunmuş, ancak hücresel veri ile internet bağlantısı gerçekleştirmesiyle masaüstü veya dizüstü bilgisayarın yerine yaygın olarak kullanılmaya başlanmıştır. Ancak bu cihazlar akıllı telefon teknolojisindeki yeniliklerin karşısında popülerliğini giderek yitirmiştir [19].

Tablet Bilgisayarlar

Mobil işletim sistemleri ile bilgisayarlar da kullanılan, farklı işletim sistemleri ile çalışabilen, çeşitli çoklu ortam uygulamalarını destekleyen, diz üstü bilgisayarlardan daha portatif ve esnek kullanım sağlayan mobil cihazlardır.

Akıllı Telefonlar

Normal haberleşme özelliği olan cep telefonlarına göre daha çok teknolojik fonksiyon ve işlevselliğe sahip cihazlardır [20]. Akıllı telefonların çoklu işlem becerileri, son teknoloji video, resim, ses vb. çoklu ortam uygulamalarını destekleyen yazılım ve donanımlarla entegre bir şekilde çalışabilmeleri tercih edilme sebeplerini arttırmaktadır [21]. Kullanıcılar bu cihazlar ile sosyal medya uygulamaları ve çevrim içi mesajlaşma uygulamalarını kullanabilmektedir. Ayrıca çeşitli uygulamalar ile dosya, fotoğraf vb. yükleyebilir, anlık mesajlaşma ve konuşmalar yapabilmektedir. Masaüstü bilgisayarlar ve dizüstü bilgisayarlar üzerinden web sitelerine erişmenin yanı sıra, aboneler bu hizmetlerden yararlanmak için akıllı telefonlarını kullanabilmektedirler [22]. "HootSuite" ve "We Are Social" tarafından yayınlanan "Digital in 2019" raporlarına göre; dünya üzerinde 5.11 milyar mobil cihaz kullanıcısının olduğu ve 2018 yılına göre mobil kullanıcı sayısında %2'lik bir artış meydana geldiği bildirilmiştir. Yine aynı rapora göre 3.484 milyar sosyal medya kullanıcısından 3.256 milyarının sosyal medya hesaplarına mobil cihazlar üzerinden eriştiği belirtilmiştir [4]. Her geçen gün artan akıllı telefon ve sosyal medya kullanımı yeni bağımlılıkları beraberinde getirerek fiziksel ve ruhsal problemlere yol açmaya başlamıştır. Bu özellikleri ile de psikoloji gibi farklı bilim dallarının konusu haline gelmiştir [23].

2.3. Mobil İşletim Sistemleri

İşletim sistemleri temel olarak bilgisayarın çalışması kontrol eden, giriş ve çıkış birimlerini yöneten ve programların işlevlerini yönlendiren, yazılımlardır [24]. Mobil cihazlar donanım ve uygulama yazılımlarının işlevlerini yerine getirmesini sağlayan işletim sistemlerine ihtiyaç duymaktadır. Bu işletim sistemleri pek çok erişim teknolojisini destekleyerek kullanıcıların her

senaryoda bağlantı kazanmalarını ve mobil saha ekipmanlarını verimli bir şekilde kullanmalarına olanak sağlar [25]. Mobil cihazlarda kullanılan donanım bileşenleri, uygulamalar, dosya formatları ve üreticiler arasındaki standartların çeşitliliği Blackberry OS, iOS, Palm WebOS, Windows Mobile, Symbian ve Android gibi farklı popüler işletim sistemlerinin geliştirilmesine neden olmuştur [26].

Blackberry OS

Research in Motion (RIM) şirketi tarafından tasarlan Blackberry OS dünyadaki farklı ülkeler ve gruplar arasında popülerliğe sahiptir. İşletim Sistemi'nin kendisi ve içeriği ile üretici tarafından yeterli dokümantasyon sağlamadığından resmi olarak çok az şey bilinmektedir. Ancak, tersine mühendislik yöntemleri ile elde edilen bilgilere göre: uygulamalar için özel bir Java ME tabanlı ve ağ işlevselliği için belirlenmiş bir MDS tabanlı iki ayrı çalışma zamanı ortamından oluştuğu bilinmektedir. İşletim sisteminin ilginç unsurlarından biri, çağrı günlükleri, SMS ve diğer kullanıcı verileri gibi bilgilerin depolandığı bir veri tabanı topluluğu olan etkileşimli çağrı yedekleme dosyası olmasıdır [6].

iOS

İlk olarak 2007'de piyasaya sürülen ve kısmen Mac OS X mimarisini izleyen UNIX tabanlı bir işletim sistemidir. iOS'u çalıştıran bir cep telefonunun ana depolama aygıtı iki bölüme ayrılmıştır. Birincisi işletim sistemi temel yapısını ve uygulamalarını, ikincisi ise kullanıcı tarafından manipüle edilen tüm verileri içerir. İlk katman core OS ve core servisleri tabakaları ikinci katman medya ve cocoa touch tabakaları şeklinde 4 tabaka bulundurmaktadır [27].

Core OS Tabakası: Bu veri katmanı temel düşük seviye özellikler, sistem yönetimi, hafıza yönetimi, genel güvenlik servisleri, şifreleme, ses, görüntü işleme ve donanım yönetimini işlemlerini gerçekleştirir [28].

Core Servisleri Tabakası: Farklı çerçevelerde alt bölümlere ayrılarak temel sistem hizmetleri sunar. Dosya erişimini sağlamak için genellikle C tabanlı temel ara yüzler içermektedir. Uygulama servisleri, ağ ve veri yönetimi, konum, takvim, etkinlikler, mağaza satın alma, SQLite ve XML gibi uygulamaların bulunduğu katmandır [28].

Medya Tabakası: Ses, grafik ve video kütüphaneleri ile uygulamalarının bulunduğu katmandır [28].

Cocoa Touch: Kullanıcıya en yakın olan katmandır. Kullanıcı ile görsel iletişimin sağlandığı dokunmatik girişlerin algılandığı, ara yüz görünümlerinin bulunduğu katmandır [28].

Ayrıca iOS işletim sisteminin yapısı, Apple App Store isimli uygulama marketi dışında hiçbir yerden uygulama yüklenmesine izin vermez.

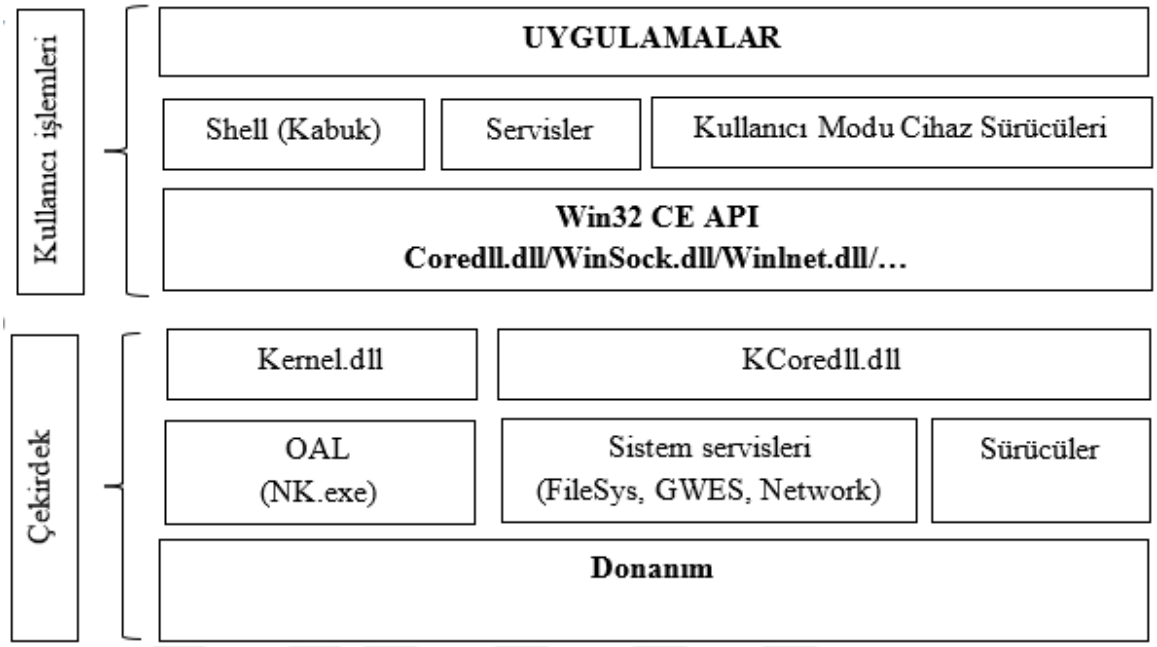
Palm WebOS

1992 yılında Jeff Hawkins ’in kurduğu Palm Computing, 1995'te US Robotics ile birleştikten sonra PDA cihazları için Palm OS'un geliştirilmesine öncülük etmiştir. 21. yüzyılın başlarında, Palm OS el bilgisayarı dünya pazarının yaklaşık %70'ine hâkim olmuştur. PDA pazarı Blackberry gibi akıllı telefonlara dönüşmesiyle Palm, işletim sistemini lisanslamak için Palm Source'nin bir alt kuruluşunu kurarak kablosuz mobil telefon teknolojisine odaklanmıştır [30]. Palm OS, Palm'ın tüm web tabanlı telefonlarını ve cihazlarını 2009'da WebOS tarafından kullanıcılara ulaştırmıştır. [29]. WebOS çalıştıran bir mobil cihaz, bir kullanıcı bölümüne ve sistem bölümüne sahiptir. Kullanıcı bölümü genellikle multimedya ve oyunları içermekle birlikte yapı bakımından oldukça basittir. Sistem bölümü yapı olarak daha karmaşıktır. Bölüm içerisinde metin mesajları, e-posta mesajları ve Web ‘de gezinme etkinlikleri ile ilgili verileri içeren veri tabanları bulunur. Ayrıca bu sistem bölümü genel kullanıcı erişimine kapalıdır [30].

Windows Mobile

Microsoft şirketi tarafından yaygın olarak PDA, tablet ve akıllı telefonlar gibi mobil cihazlarda kullanılmak üzere tasarlanmıştır. Windows Mobile işletim sistemi, C++ yazılımı ile yazılmış olup, Windows CE çekirdeği üzerine kurulmuştur. Windows Mobile ilk versiyonu olan Pocket PC 2000 19 Nisan 2000 yılında yayınlayarak sonrasında Pocket PC 2002, Windows Mobile 2003, Windows Mobile 5.0, Windows Mobile 6.0, Windows Mobile 6.1 ve Windows Mobile 6.5 versiyonlarını yayınlamıştır [31]. 2011 yılı mayıs ayında ek servis hazırlayanlara destek kesilmiş, yaklaşık 6 ay sonrada ekim ayı içerisinde My Phone hizmeti durdurulmuştur. Mayıs 2012 yılında sistem destek ve Windows Marketplace for Mobile durdurularak 8 Ocak 2013 tarihinden itibaren final versiyonuna destek kesilmiştir. Microsoft Firması, Windows Mobile sistemine son verdikten sonra yerine tamamen yeni işletim sistemi olan Windows Phone’ ye geçiş yapmıştır.

Windows Mobile 6.x ve Windows Phone 7 gibi işletim sistemi sürümleri modüler ve çok kanallı, gerçek zamanlı işletim sistemleridir. Bu işletim sistemleri çoklu görevleri destekleyerek birden fazla donanım mimarisi üzerinde çalışırlar. Şekil 2.1 ’de gösterildiği gibi ARM x86 ve SH4 (Pavlov ve Belevsky, 2008, Microsoft Corporation) işletim sistemi mimarisi iki katmandan oluşmaktadır. Birinci katman kullanıcı işlemleri, ikinci katman ise çekirdektir. Kullanıcı işlemleri katmanı kullanıcı uygulamalarını, uygulama programcı ara yüzlerini (API) ve kullanıcı modu cihaz sürücülerini içerir. Öte yandan, çekirdek katmanı NK.exe çekirdek işlemini, sistem servislerini (örneğin dosya sistemi, aygıt yöneticisi) ve çekirdek modu aygıt sürücülerini içerir. Ayrıca Bir WM OS ‘da üçüncü taraflarca geliştirilen bir aygıt sürücüsünü aygıtın EEPROM'daki dizin ya da SD kartındaki herhangi bir dizinden yüklemek mümkündür. WM OS 'un yaptığı tek şey, kullanıcıdan onay istemektir [32].



Şekil 2.1. Windows Mobile mimarisi [32]

Symbian

Symbian işletim sistemi modüler bir medya mimarisine sahiptir. Bu mimari, veri depolama giriş/çıkış işlemlerinden sorumludur. Symbian da dosya sistemlerini yönetmekten sorumlu olan hizmete dosya sunucusu adı verilir. Dosya sunucusu mimarisi aslında istemci uygulamasının ve dosya sunucusunun mesaj iletimi yoluyla iletişim kurduğu bir istemci-sunucu mimarisidir. Uygulamalar, EFSRV.DLL dosyasının API 'sini dosya sunucusuyla iletişim kurmak için kullanır. Dosya sunucusu, yeni dosya sistemi arabirimlerinin dinamik eklentisini destekleyen takılabilir bir mimariye sahiptir. Eklentiler, çekirdek düzeyindeki medya sürücüleri ile EUSER.DLL kullanıcı kitaplığındaki TBusLocalDrive sınıfı aracılığıyla iletişim kurar. Çekirdek tarafında, medya sürücüsü, mantıksal bir bölüm olan mantıksal aygıt sürücüsü (LDD) ve fiziksel bir bölüm olan fiziksel aygıt sürücüsünden (PDD) oluşur. Çekirdek işlemi, mantıksal aygıt sürücülerini dinamik olarak yükleyebilir. Yerel sürücüler için, LDD ELOCD.LDD'de bulunur ve kullanılan PDD gerçek cihaza bağlıdır (örn. NAND flaş veya SD çıkarılabilir medya) [33].

Maemo

Maemo Linux tabanlı, Debian tabanında ve GNOME görsel kullanıcı ara yüzü kütüphanesi üzerine kurulmuş açık kaynaklı bir işletim sistemidir. Her ne kadar yaygın olmasa ve gelişimi Ekim 2011'den beri dondurulmuş olsa da, kullanıcı verileri, işletim sistemi işlevleri ve takas alanlarının farklı bölümlerde yer alması gibi araştırmaya yönelik bazı ilginç özellikler vardır [34].

MeeGo

Intel ve Nokia şirketleri 15 Şubat 2010'da akıllı telefonlar, notebooklar, tabletler, bağlı TV'ler ve diğer bilgisayar cihazları için MeeGo isimli açık kaynaklı bir Linux tabanlı işletim sistemini geliştirmiştir. Maemo ve Moblin işletim sistemi projeleri MeeGo'nun öncüleridir. MeeGo hem ARM hem de Intel x86 işlemcileri gibi çeşitli donanım platformlarında çalışması amaçlanmıştır [35].

LiMo

LiMo OS Linux Mobile kısaltması olarak isimlendirilmiş, el bilgisayarları için LiMo Foundation tarafından geliştirilen açık kaynaklı bir Linux tabanlı işletim sistemidir. Eylül 2011'de proje Tizen olarak yeniden adlandırılan LiMo akıllı telefonlar için çok fazla tercih edilen bir işletim sistemi olamamıştır [36].

Tizen

Tizen OS, Linux Foundation tarafından desteklenen Linux tabanlı bir işletim sistemidir. Nokia ve Intel, Tizen işletim sistemini geliştirilmiştir. Ayrıca geliştiriciler topluluğu tarafından desteklenen açık kaynaklı ve esnek bir işletim sistemidir. Açık kaynak olduğundan, kullanmak isteyen tüm üyelere açıktır. Ayrıca, geliştiriciler kullanmakta ve geliştirmekte özgürdürler. Endüstrinin farklı gereksinimlerine hizmet eden çoklu profillere sahip bir çekirdek işletim sistemidir [37].

Sailfish OS

Sailfish OS, çeşitli mobil cihazların bağımsız tasarımcısı, geliştiricisi ve satıcısı Jolla'nın geliştirdiği işletim sistemidir. Sailfish OS, kapsamlı bir lisanslama modeli sunan, inovasyonu teşvik eden bağımsız Linux tabanlı bir işletim sistemidir. Ayrıca, farklı cihaz türlerinde genel amaçlı bir Linux OS olarak kullanılabilir. Bununla birlikte, iOS, Android ve Windows gibi tasarım prensibine sahip değildir. Bu işletim sistemi, şu anda çalışan uygulamaların ızgara stili bir ara yüzde gösterildiği çoklu görev uygulamasına sahiptir. Bu işletim sisteminde, hareketler yalnızca yukarıdan aşağı doğru kaydırarak ekranlar arasında geçiş yapılmasına izin vermektedir. Bir web tarayıcısı içerisindeki diğer sekmelere erişmek soldan sağa kaydırarak mümkündür. Bildirim menüsünü açmak için ekranın altından hızlıca kaydırılması yeterlidir [38].

Firefox OS

Web'in gücünü insanların elinde tutmaya adanmış misyon tabanlı kuruluş olan Mozilla, Firefox OS'u 1 Temmuz 2013 da duyurmuştur. Firefox OS akıllı telefonlar, tamamen Web teknolojileri tarafından desteklenen ilk cihazlardır ve bir akıllı telefondan beklenen birçok özelliği sunmaktadır. Firefox OS, akıllı telefonlar için yepyeni bir kavrama sahiptir. Telefona herhangi bir

uygulama indirmeye gerek kalmadan, her an kullanıcı ihtiyaçlarını karşılayacak şekilde dönüşebilen, uyarlanabilir bir uygulama araması kullanır. Ayrıca Firefox OS'un market uygulaması olan Firefox Marketplace dünyanın en büyük uygulama mağazası olma potansiyeline sahiptir [39].

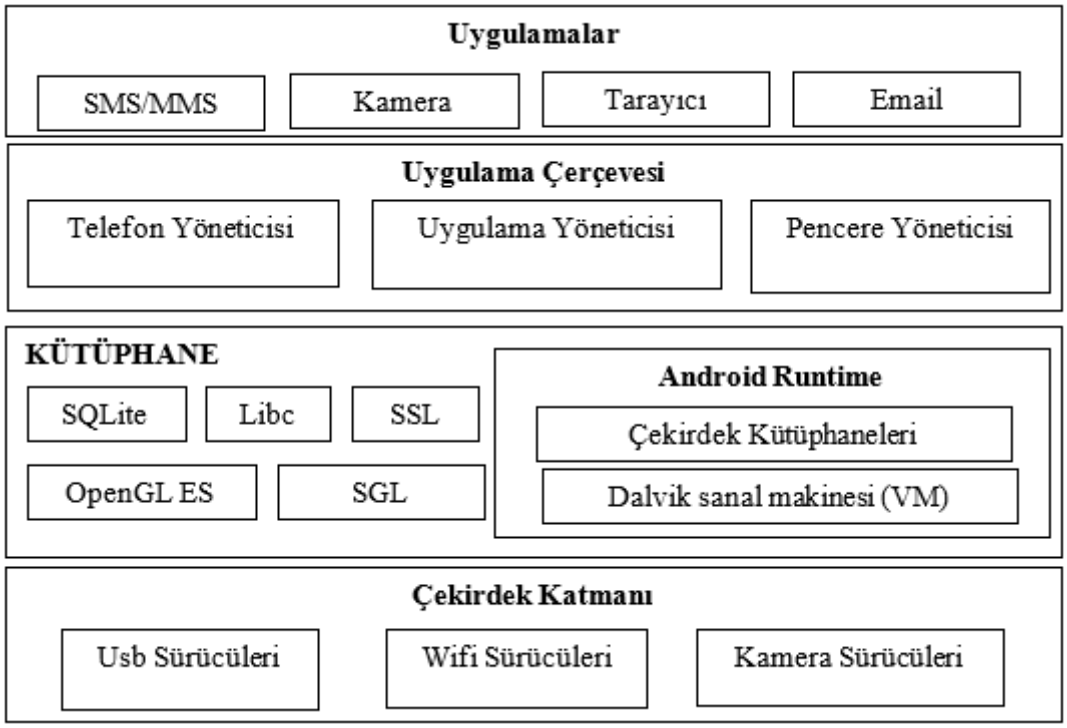
Bada

Samsung Electronics 'in akıllı telefonlar için tasarladığı mobil işletim sistemi olan Bada, web hizmetlerini kullanan uygulamalar alanında geliştirici dostu ortamlardan biridir. Bada harita kontrolü uygulamalarda haritalama için kullanılabilir. Eclipse ve GNU takım zinciri de geliştirme amacıyla IDE olarak kullanılabilir. Bada hareket sensörünü ve yüz algılamayı destekler. Ayrıca sensör tabanlı ve bağlama duyarlı uygulamalar geliştirmek için mekanizma sağlar. Geliştiriciler, kullanıcı profillerini yönetmek için sosyal ağ uygulamaları, haritalama için konum uygulamaları vb. gibi servis odaklı uygulamalar oluşturabilirler [40].

Android

Android, Google liderliğindeki Özgür Yazılım Topluluğu (Open Handset Alliance) OHA, olarak bilinen bir grup şirket tarafından açık kaynak kodları ile oluşturulan mobil platformdur. Her ne kadar açık kaynak kodları ile yazılmış olsa da kodların küçük ve önemli kısımları Google tarafından saklı tutulmaktadır [41, 28]. Android ilk olarak 2007 yılında piyasaya sürüldü ve beş yıldan daha az bir sürede mobil telefon pazarında baskın işletim sistemi olma başarısı elde etti [6]. IDC tarafından yapılan araştırma sonuçlarına göre 2019 yılı verilerine göre Android işletim sisteminin pazar payı %86,1 seviyesine ulaşmıştır [42].

Android İşletim sistemi, aygıt sürücüleri, ağ altyapısı ve güç yönetimi gibi temel işlevleri desteklemeye yarayan Linux 2.6 tabanlı bir çekirdek üzerinde çalışır ve Şekil 2.2 'de gösterildiği üzere Linux çekirdeği, yerel kütüphaneler, dalvik sanal makinesi (VM) , uygulama çerçevesi ve uygulamalar gibi katmanlardan oluşur [43,6].



Şekil 2.2. Android mimarisi [44]

Linux çekirdeği: Aygıt donanımı arasında bir soyutlama seviyesi sağlar, kamera, tuş takımı, ekran vb. tüm temel donanım sürücülerini içerir. Ayrıca, çekirdek, ağ oluşturma ve çok çeşitli aygıt sürücüleri içerir.

Kütüphaneler: Ara yüz ve grafik kütüphaneleri, Web tarayıcı kütüphaneleri, veri tabanı kütüphanelerini içerir.

Android Çalışma Zamanı: Bu, mimarinin üçüncü bölümüdür ve alttan ikinci katmanda bulunur. Bu bölüm, Android için özel olarak tasarlanmış ve optimize edilmiş bir tür Java sanal makinesi olan dalvik sanal makinesi isimli önemli bir bileşen sunar. Dalvik sanal makinesi, Java diline gerçek olan bellek yönetimi ve çoklu iş parçacığı gibi Linux temel özelliklerini kullanır.

Uygulama çerçevesi: Uygulama geliştiricilerin uygulamalarında bu hizmetleri kullanmasına izin vererek uygulamalara java sınıfları şeklinde birçok üst düzey hizmet sunar.

Uygulamalar: java dili ile programlanmış Android uygulamalarının bulunduğu katmandır. Rehber, tarayıcı, oyunlar vb. bu tür uygulamalara örnek olarak verilebilir [44] [45].

Android Dosya Sistemi: Android'in bir başka ilginç unsuru ise yerel olarak desteklenen YAFFS2 dosya sistemidir. YAFFS 'ın yayınlanan birinci versiyonu YAFFS1; 512 bayt artı 16 bayt yedek alana sahip eski NAND yongaları için tasarlanmıştır; İkinci versiyon YAFFS2 ise 2048 bayt artı 64 bayt yedek alana sahip yeni yongaları barındırmak için YAFFS1'den geliştirilmiştir [45].

Android güvenlik mimarisi: Android, süreçler ve kullanıcılar yönetimi için standart Linux olanaklarına dayanan çok işlemli bir platformdur. Android, varsayılan olarak, herhangi bir

uygulamanın, diğer herhangi bir uygulamayı ya da işletim sistemini engellemek amacıyla işlem yapma yeteneğini reddeder. Dolayısıyla, bu tasarım nedeniyle, uygulamalar için, son kullanıcı özel verileri (örneğin, rehber, mesajlar) üzerinde herhangi bir işlem yapmak, başka bir uygulamanın dosyalarına erişmek, ağ erişimlerini gerçekleştirmek, cihaz durumunu yönetmek, mümkün değildir. Android, çalışan herhangi bir uygulamayı, sandbox tarafından istenen özelliklere erişmek için gereken izinlerin açıkça bildirilmesi dışında, diğer uygulamalarla karışmayan güvenli bir sandbox'a bağlar. Bir uygulama tarafından tutulan izinler kümesi, statik bir şekilde tanımlanır, kurulum sırasında doğrulanır ve uygulamanın ömrü boyunca değişemez. Herhangi bir Android uygulamasının, uygulamalar arasındaki ilişkileri kurmak ve yönetmek için geliştirici tarafından düzenlenen bir sertifika ile imzalanması gerekir.

Android işletim sistemi varsayılan olarak yüklü olan her uygulamayı farklı bir Linux kullanıcısı olarak yönetir. Aslında kurulum sırasında, herhangi bir uygulamanın kendine özgü Linux kullanıcı kimliği ile sağlanır. Belirli bir uygulama tarafından depolanan tüm veriler, uygulamanın kullanıcı kimliğini de alır, diğer uygulamalara bu verilere herhangi bir erişim izni vermek için, diğer kullanıcı grubundan erişimi sağlamak gerekir. Varsayılan olarak, temel bir Android uygulamasının ilişkili izinleri yoktur. Dalvik sanal makinası varsayılan yeteneklerini kullanarak ortaya çıkabilecek sınırlamaların üstesinden gelmek ve uygulamalar arasında hizmet sunumuna izin vermek için başka izinler beyan etmek zorundadır. İhtiyaç duyulan izinlerin beyanı geliştirme zamanında yapılır. Uygulamanın Android manifest.xml dosyasına *<uses-permission>* etiketlerinin eklenmesiyle, yükleme sırasında, uygulamanın gerektirdiği izinler paket yükleyici modülü tarafından verilir. İzin verme politikası hem uygulamaların imzalarından hem de son kullanıcı ile etkileşimlerinden yararlanabilmektedir [45].

2.4. Dijital Kanıtlar ve Adli Bilişimin Temel Aşamaları

Günümüzde iş başvurularından, alışverişe, hastane randevu işlemlerinden bankacılık işlemlerine kadar hemen hemen her tür işlem bir noktada dijitalleşmektedir. Dijital cihazlar ise bu işlemler ile ilgili bir tür elektronik kayıt oluşturmaktadır [41]. Adli bilişim günlük faaliyetler sonucu isteyerek ya da istemeyerek oluşturulan bu elektronik verilerin herhangi bir suç soruşturmasında kanıt olma ihtimali ile ilgilenmektedir. Bu nedenle adli bilişim kavramı olayların yeniden yapılandırılmasını kolaylaştırmak veya ilerletmek amacıyla dijital kaynaklardan elde edilen kanıtların korunması, toplanması, doğrulanması, tanımlanması, analizi, yorumlanması, belgelenmesi ve sunulmasına yönelik bilimsel olarak türetilmiş yöntemler bütünü olarak tanımlanmaktadır [42].

Dijital kanıt terimi hem dijital cihazları hem de cihazlarda bulunan ilgili bilgi parçalarını (verileri) kapsar. Dizüstü bilgisayar veya akıllı telefon gibi dijital cihaz dan elde edilen veriler sıklıkla tek başına kanıt olarak kabul edilir [43]. Adli bilişimin yukarıda verilen tanımı mahkeme

salonunun dışındaki kapsamı genişleterek araştırmacıların çok daha geniş bir yelpazedeki kriterleri değerlendirmelerini sağlamıştır [44].

Bir verinin dijital kanıt haline gelmesi için, hukuki veya cezai bir eylem ışığında saklandığı depolama aygıtları içerisinden erişilerek işlenmesi gerekmektedir. Bu nedenle adli bilişim işlemlerini yürütürken tanımlama, koruma, toplama, analiz ve raporlama aşamasından oluşan beş temel aşamanın dikkatli takip edilmesi gerekir. Adli bilişim yalnızca bir suç veya olayla ilgili verileri toplama, koruma, analiz etme ve raporlama süreçleriyle ilgili değildir. Bir adli bilişim insanı, her şeyden önce bir bilim insanı olmalı ve bu nedenle dijital adli tekniklerle ilgili en son araştırmalara ayak uydurmalıdır [46].

- **Tanımlama**

İlk aşama, sorunların ve verilerin yerinin yanı sıra ilgili kanıt / bilgi potansiyel kaynaklarını tanımlama sürecidir. Bu aşama potansiyel dijital delil kaynaklarının belirlenmesiyle ve toplanmasıyla başlar. En çok bilinen dijital veri kaynakları içerisinde bilgisayarlara takılı sabit diskler, CD/DVD, disket, USB, cep telefonunu, tablet vb. araçları sayabilir. Bunların yanında veri tabanları, web siteleri, kart kopyalama cihazları, dron ve IoT cihazları kaynak olabilir [47].

- **Koruma**

Olay mahallini korunması, olay yerinin görüntülerinin alınması, kanıtların nasıl elde edildiğiyle ilgili tüm bilgilerin belgelenmesi ve elektronik olarak saklanan bilgilerin koruması sürecidir [46].

- **Toplama**

Soruşturma konusu ile ilgili olabilecek dijital bilgilerin toplanması, elektronik cihazların olay yerinden alınarak laboratuvar ortamına taşınması ve ardından cihaz içeriğinin kopyalanması süreçlerini içerir [46].

- **Analiz**

Adli olayla ilgili derinlemesine ve sistematik bir kanıt araştırmasının yapıldığı, sistem ve kullanıcı tarafından oluşturulan dosyaların analiz edilerek, bulunan kanıtlardan sonuçlar çıkarmayı amaçlayan süreçtir [48].

- **Raporlama**

Analiz aşamasında tespit edilen kanıt olma potansiyeline sahip verileri kanıtlanmış teknikler ve metodolojilere uygun olarak adli makamların anlayacağı yalın ve arındırılmış bir dille ifade etme sürecidir [49].

2.5. Adli Bilişim Çeşitleri

Adli bilişim birçok alt disipline sahip, sürekli gelişen bilimsel bir alandır. Bu gelişime bağlı olarak artan cihaz çeşitliliği ve özellik kapasitesi adli bilişimin alt alanlara ayrılmasına sebep olmuştur [6].

- **Bilgisayar Adli Bilişimi**

Soruşturmalar ve yasal işlemlerin desteklenmesi amacıyla bilgisayarlarda, dizüstü bilgisayarlarda ve depolama ortamlarında bulunan kanıtlarla ilgili tanımlama, koruma, toplama, analiz ve raporlama süreçlerini içeren adli bilişimin en eski disiplinidir. Adli bilişimin alt dallarının bir çoğu zamanla bu disiplinden ayrılarak farklı bir alt disiplin oluşturmuşlardır [50].

- **Ağ Adli Bilişimi**

Bazı dijital kanıtlar fiziksel olmaktan ziyade çevrimiçi olabilmektedir. Bu tür delillerin korunmasına ilişkin web sitelerini içeren suçlarda bulunabilir. Ağ adli bilişimi: güvenlik saldırıları, izinsiz girişler, kötü amaçlı yazılım saldırılarının, anormal ağ trafiğinin ve güvenlik ihlallerinin kaynağını bulmak için ağ etkinliklerinin veya olaylarının izlenmesi, yakalanması, saklanması ve analizi süreçlerini içermektedir [51].

- **Dijital Görüntü, Video ve Ses Adli Bilişimi**

Bu alan dijital olarak elde edilen fotoğraf görüntülerin çıkarılması ve bu görüntülerin analiz edilerek, orijinalliklerinin teyit edilmesi süreçlerini içermektedir. [52] .

- **Bellek Adli Bilişimi**

Çalışan bir bilgisayarın Rasgele Erişim Belleğinden (RAM) kanıtların toplanması, aynı zamanda canlı kazanım olarak da bilinir. RAM içeriğinden, şifreleme anahtarları gibi adli olarak çok önemli bilgiler elde edilebilmektedir. Ayrıca bilgisayarlar yürüttükleri işlemler ile ilgili geçici bilgileri RAM içerisinde saklamaktadır. Bu nedenle RAM içerisinde kanıt olabilecek birçok kritik veriye ulaşılabilir [53].

- **Mobil Cihaz Adli Bilişimi**

Mobil cihaz adli bilişimi cep telefon, akıllı telefon, SIM kart, PDA, GPS, tablet, oyun konsolları vb. elektronik cihazlardan kanıtların kurtarılması süreçlerini içermektedir. Uygulamada yukarıdaki sınıflandırmayı bulanıklaştıran istisnalar vardır, çünkü cihazların gruplanması bazı durumlarda değişiklik göstermektedir. Örneğin SIM kartı olmayan tabletler veya akıllı telefonlar bilgisayar olarak kabul edilebileceği gibi bellek kartları akıllı telefonlarda ve tabletlerde sıklıkla bulunur, bu nedenle mobil adli bilişim veya bilgisayar adli bilişimi altında değerlendirilebilirler.

Klavyeli tabletler, dizüstü bilgisayarlar olarak kabul edilebileceği gibi mobil cihaz olarak da kabul edilebilmektedir.

Gelişen teknoloji ile birlikte insanların faaliyetlerini kaydeden yeni dijital veri türleri ortaya çıkmaya devam etmektedir. Bu durum adli bilişim bilimine olan ihtiyacı arttırmaktadır. Her ne kadar adli bilişim, adli bilimin ana akımları dışında başlamış olsa da, şimdi tam olarak bir adli bilim dalı olarak kabul edilmektedir [52].

Cep telefonlarının yetenekleri, oyun, sosyal medya, çevrimiçi bankacılık ve hisse senedi ticareti de dâhil olmak üzere sayısız kullanım içerecek şekilde genişlemiştir. Mobil cihazların çoğalması aynı zamanda bu cihazların suça konu olduğu durumların artmasına neden olmuştur. Bazı durumlarda, kötü niyetli geliştiriciler kullanıcı bilgisi olmadan hassas bilgiler toplayabilmektedir. Bu nedenlerle mobil cihazlar birçok durumda kilit kanıt olarak görülmektedir [54].

Mobil uygulamalar önemli miktarda kullanıcı bilgisini işlemektedir. Böylece akıllı telefonlarda çok miktarda hassas bilgi yerel olarak depolanır. Bu nedenle, mobil uygulamalar tarafından üretilen eserlerin elde edilmesi ve analiz edilmesi, mobil cihazların adli analizinde çok önemli bir adımdır [55]. Mobil cihazların adli bilişimi, bu cihazlardan veri toplama süreçleri ile devam eden soruşturmaya ilişkin kanıt olup olmadığını belirlemeyi ve sonuçlandırmayı içerir. Mobil cihazlarda yerel olarak depolanan dijital veriler ile ilgili aşağıdaki üç soruya cevap aramak gerekir. Bunlar depolanan bilgilerin ne olduğu (örneğin, GPS), bilgilerin nerede saklandığı (örneğin dosya yolu) ve bilginin nasıl saklandığını (örneğin, bir veri tabanı tablosunun yapısı) olarak sıralanabilir [54].

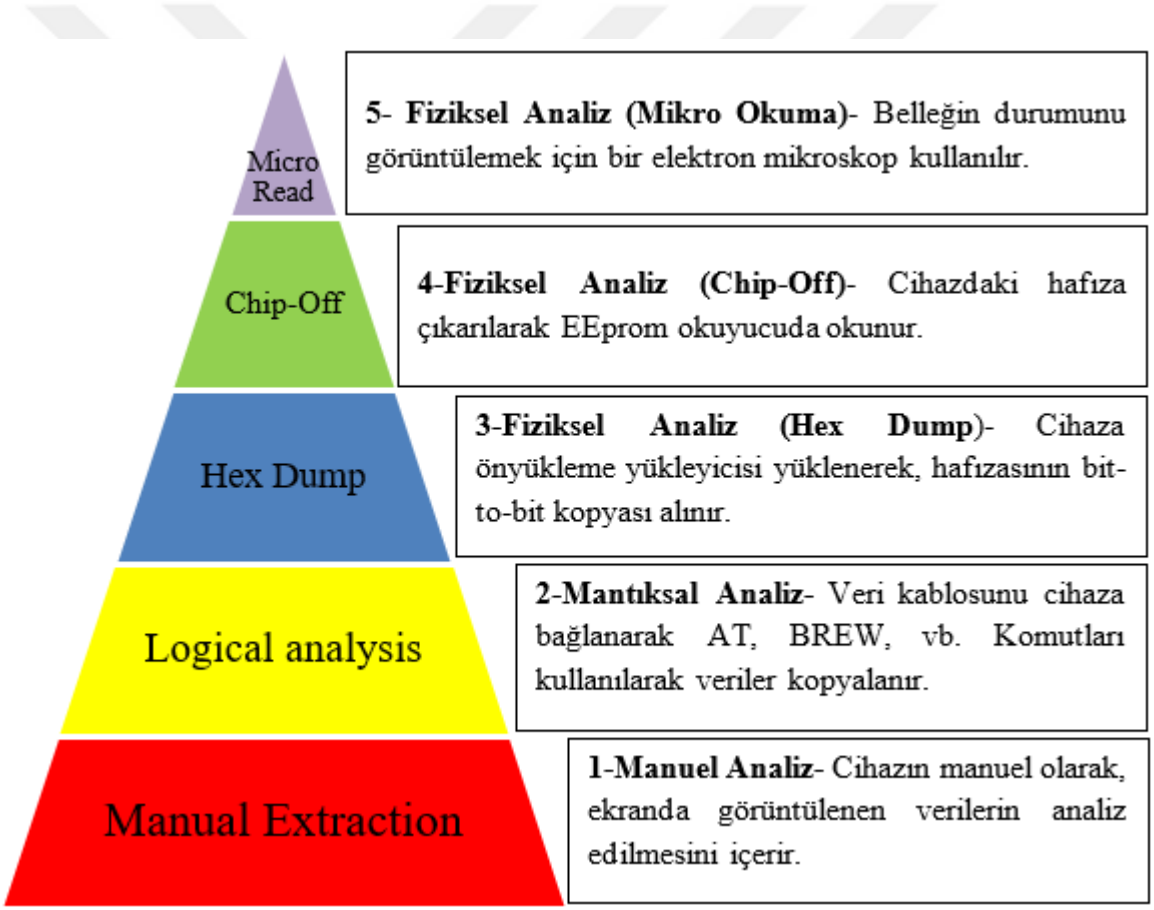
Mobil cihazlardan dijital kanıt elde etmek ve bu kanıtları analiz etmek oldukça karmaşık bir iştir. Bu işlemler adli araç setlerine tamamen bağımlı olarak yürütülmektedir. Gelişen teknolojiye bağımlı olarak yeni kanıt elde etme ve analiz yöntemleri ortaya çıkmaktadır. Ayrıca mobil adli bilişim analizleri bir nevi canlı analiz olarak da değerlendirilebileceğinden mahkemede delillerin kabul edilebilirliği için işlemlerin ayrıntılı olarak açıklanması önemlidir.

2.6. Adli Kopya Alma Yöntemleri

Mobil cihazların veri toplama ve analiz işlemleri, cep telefonlarından bilgilerin çıkarılması, kanıtın uygun olup olmadığının belirlenmesi ve raporlanmasını süreçlerini içermektedir. Adli bilişim analizi yapmak için çoğu zaman cihazın tüm hafızasının dijital kopyasını almak gerekse de zaman zaman yalnızca belirli mobil uygulamaları ayıklamak ve incelemek yeterli olabilir. Bu durumlarda, mobil cihazlardaki dijital kanıtlar belirli uygulamalar tarafından üretilmekte ve yerel olarak depolanmaktadır [54]. Mobil cihaz işletim sistemleri sürümlerinin sürekli güncellenmesi ve güvenlik teknolojilerinin devreye alınması, mevcut veri toplama yöntemlerinin çalışmamasına neden olmuştur [56].

Birçok araştırmacı mobil işletim sistemine sahip mobil cihazların veri toplama teknolojilerini inceleyerek, çeşitli veri toplama yöntemleri önermiştir. Bu yöntemler genel olarak mantıksal kazanım yöntemleri ve fiziksel kazanım yöntemleri olarak ikiye ayrılmıştır [52]. Bu yöntemlerin yanında çeşitli adli araçlar mobil cihazlardan bu yöntemlerle elde edilemeyen verileri manuel görüntüleme araçları yardımı ile alınmasına imkân tanıyan farklı yöntemler geliştirmiştir.

Tüm adli araçların avantajlarının yanında dezavantajlarının da olduğu ve tek bir aracın tüm amaçlar için yeterli olmadığı bilinmelidir. Bu nedenle çeşitli türlerdeki mobil adli araçların anlaşılmasının yanında mobil cihazların adli kopyasının alınması ve analizi için kullanılacak uygun araçları belirlemek zordur. Bu nedenle Sam Brothers mobil cihaz adli araç sınıflandırma sistemini örenmiştir. Önerilen mobil cihaz adli araç sınıflandırma sistemi Şekil 2.3'de gösterilmiştir [57].



Şekil 2.3. Mobil cihaz adli araç sınıflandırma sistemi [57].

Manuel Çıkarım Yöntemi

Mobil cihazın kullanıcı ara yüzünü yardımı ile mobil cihaz içeriğinin fotoğraflanarak alınmasıdır. Bu yöntem ile sadece kullanıcı ara yüzündeki verilere ulaşılmaktadır.

Mantıksal Kazanım Yöntemleri

Mantıksal bir kazanım, genellikle bir mobil cihazdaki yalnızca silinmeyen verilerin edinimini sağlar. Mobil cihazın kullandığı donanım ve işletim sisteminin yanında kullanılan adli araçlara bağlı olarak verilerin büyük bir kısmı veya tamamı edinilebilir. Nadir olmasına rağmen, mantıksal bir kazanım gerçekleştirirken silinen verileri almak mümkündür. Bu yalnızca telefondaki ayrılmamış alanın mantıksal bir dosyaymış gibi alınabileceği modeller için geçerlidir [58]. Mantıksal edinme yöntemleri, cihaz dosya sistemine erişerek cihaz verilerini almaktadır. AFLogical gibi tipik geleneksel mantıksal kazanım yöntemleri [59], Android Hata Ayıklama Köprüsü (ADB) Çekme [60] ve Android Yedekleme Çıkarıcı [61], daha önceden tanıtılmıştır. Geleneksel mantıksal kazanım yöntemleri sezgisel ve uygundur, ancak kullanıcı erişim sürecinin ayrıcalığı ve uygulamaların yapılandırılmasıyla sınırlıdır. Köksüz bir Android cihazdan uygulama verilerini elde etmek için geleneksel mantıksal edinme yöntemlerini kullanmak zordur.

Geleneksel mantıksal bir edinmede sadece cihaz içerisindeki verileri çıkarılabilmektedir. Verileri senkronize etmek veya yedeklemek için TWRP yüklemek suretiyle cihaz yedeğini harici bir bellek içerisine aktarma gibi teknikler kullanılarak da cihaz içerisindeki veriler kopyalanabilmektedir [62].

Köklü bir cihaz içerisindeki veriler Android Hata Ayıklama Köprüsü (ADB) “adb pull “komutu kullanılarak çıkarılabilirken kök ayrıcalığı alınamayan bir cihaz içerisindeki verileri “adb pull” komutu kullanılarak çıkarılamaz. 2017 yılında yapılan bir çalışmada WeChat isimli uygulama verileri almak için “Köksüz Yedekleme Yöntemi” olarak adlandırılan yeni bir yöntem kullanılarak WeChat uygulamasına ait veriler başarılı şekilde çıkarılmıştır. Bu yöntem, önce uygulama verilerinin korunması koşuluyla yeni sürüm uygulamasını (yedeklemeye izin verilmez) kaldırır, ardından aynı uygulamanın eski bir sürümünü yükler (yedeklemeye izin verir). Son olarak, uygulama verileri adb backup (yedekleme) komutu ile çıkarılır. Ancak bu yöntemle sadece sürümü düşürülen uygulama içerisindeki veriler çıkarılabilmektedir [63]. Android 7.0 özel dosyaların güvenliğini arttırdığından Android 7.0 veya daha üst bir sürümde bu yöntem veri kayıplarına neden olabilmektedir [64].

Sistem düzeyinde yedekleme yöntemi ile cihaz üreticileri tarafından sağlanan Windows için smart switch ve Samsung smart switch gibi sistem düzeyinde veri yedekleme araçlarını kullanır. Cihaz yedekleme dosyalarını yakalamak ve bunları bir PC'de depolamak, ardından cihaz yedekleme dosyalarını ayrıştırmak için analiz araçlarını kullanılmaktadır. Bununla birlikte, birçok işletim sistemi üreticisi farklı geçiş dosyaları depolama formatları ve farklı şifreleme algoritmaları benimseyebilecek kendi işletim sistemlerini ve sistem düzeyinde veri yedekleme araçlarını kullanmıştır. Bu nedenle yedek dosyalar çıkarılabilse bile her birini ayrıştırabilecek evrensel bir araç bulmak zordur [56].

Fiziksel Çıkarım Yöntemleri

Fiziksel toplama yöntemi, aygıtların tüm hafızasını bit-bit bellek içerisine aktarır. Mobil adli bilişim araçlarının çoğu, sistem güvenlik açıklarından yararlanarak veya özel kurtarma görüntülerini kullanarak cihazın hafızasını çıkarmaktadır. Ayrıca fiziksel çıkarım için kullanılan yazılım güncelleme protokollerine dayanan yöntemler ile donanım tabanlı yöntemlerde kullanılmaktadır.

Özel kurtarma görüntüsü yükleme yöntemi ile Android cihazlar, tipik olarak MTD cihazlarına eşlenmiş birkaç bölümden oluşur. Tam bölümleme şeması, satıcı uygulamasına bağlıdır. Android cihazlarda en yaygın kullanılan sistem, kullanıcı verisi, önbellek, önyükleme ve kurtarma olmak üzere beş bölüm bulunur. Android cihazlarda normal çalışma sırasında, kurtarma bölümünde hiçbir kullanıcı verisinin kaydedilmediğini unutmamak gerekir; bu nedenle bu bölümdeki verilerin bozulması veya üzerine yazılması, daha sonra mahkemede güvenilebilecek olan cihazdaki içeriği değiştirmeyecektir. Ancak Android sisteminin sürekli güncellenmesi, güvenlik açıklarının gidermesi kök ayrıcalığını elde etmeyi zorlaştırmaktadır. Öte yandan, güvenli önyükleme (Secure Boot) ve Samsung KNOX gibi güvenlik teknolojilerinin kullanılması özel kurtarma görüntüleri ile çıkarım yapılması önünde bir engel teşkil etmektedir [65].

Yazılım (Firmware) güncelleme protokollerine dayanan bir fiziksel çıkarım yöntemi ile bellenim güncelleme protokolünü tersine mühendislikle okuma komutunu kullanılarak fiziksel çıkarım yapılmaktadır [66].

Donanım Tabanlı Yöntemler olan JTAG tabanlı, Chip-off tabanlı ve MTK tabanlı fiziksel çıkarım yöntemleri riskli yöntemlerdir. Çünkü tüm Android mobil cihazları JTAG'ı desteklemez veya bir MTK-CPU kullanmaz ve Chip-off tabanlı satın alma yöntemi yongaları PCB cihaz panelinden kaldırır [56].

Apple mobil cihazların fiziksel edinimi uzun bir süredir iphone 4 de ve bazı ipad modelleri ile sınırlı kalmıştır. Ancak bağımsız araştırmacı axi0mX, çığır açan " checkm8 " sömürüsünü halka duyurmasıyla tam dosya sistemi çıkarma için yasal erişimi sağlanmayı başlanmıştır. Adli bilişim dünyası checkm8'i ilk olarak 10 Kasım 2019'dan sonra kullanmaya başlamıştır. Bazı cihazlarda Checkra1n'i kullanmak için, Cydia veya AFC2 (Apple File Conduit 2) gibi ek hizmetlerin yüklenmesi gerekirken, bazılarında ise bu hizmetlerin yüklenmesine gerek kalmadan doğrudan SSH protokolü kullanılarak çalıştırılmıştır. Apple cihazlarda tam dosya sistemi çıkarma, mantıksal çıkarma işleminden çok daha fazla veri sağlamaktadır. Buna, e-postalar, üçüncü taraf uygulama verileri ve "Anahtar Zincirinde*"* saklanan şifreler gibi kritik veriler dâhildir [67].

2.7. Adli Bilişim Süreç Modelleri

Tüm adli disiplinler, geçerli sonuçları sağlamak için inceleme sırasında kullandıkları araçlara bağlı olsalar da tartışmaya açık bir şekilde adli bilişim alanındaki güven düzeyi daha yüksektir.

Adli bilişim analizlerini adli araç setleri olmadan manuel yapmak mümkün olmadığı gibi sadece adli araç setlerinin getirdiği sonuçlarla neticeye varmak da doğru değildir. Analiz işlemleri sırasında dijital kanıtları yorumlama işlemi de büyük önem arz etmektedir. Bu nedenle adli bilişim analizlerinde analiz yapacak uzman ile adli araç setlerinin bir bütün olarak birbirini tamamlamaları gerekmektedir. Hatta analizcinin soruşturmanın her safhasında bulunması ile ilgili öneriler bulunmaktadır [7]. Dijital soruşturmaların insan ve adli araçlarla bağlı olmasından dolayı, hatalarında insan ve adli araç faktörlerinden kaynaklı hatalar olması beklenir. Adli bilişimde insan hataları ele alınan adli kararları etkileyebilecek "önyargı kaynakları taksonomisi" ile adli araçların güvenirliğini test etmek için çeşitli testler geliştirilmiştir [68] [7].

Bir adli bilişim analizcisinin soruşturma sırasında kanıt olabilecek sonuçları rapor etmeden önce eldeki sonuçların kanıt olma potansiyelini desteklemeleri hayati önem taşımaktadır. Bu nedenle verilerin güvenilir bir şekilde raporlanması sürecinde, analizcileri desteklemek için dijital kanıt raporlama ve karar destek (DERDS) çerçevesi sunulmuştur [69].

Adaletin doğru bir şekilde sağlanmasına olanak sağlayacak model ve tekniklerin geliştirilmesi adli bilişim alanında bu güne kadar yapılan çalışmaların odak noktası olmuştur [70]. Bu alanda kritik ve zahmetli olan süreçlerden biride şüpheli mobil cihazların adli bilişim analizidir. Bu nedenle mobil cihazların delil niteliğini koruyarak içerisindeki verilerin çıkarılması ve analiz edilmesi ile ilgili farklı süreç modelleri önerilmiştir [71]. Hızla gelişmeye devam eden dijital dünyada kanıtları korumak gittikçe zor görünse de, işlemlerin bilinçli ve sistematik yapılması hem maliyeti azaltacağını hem de kanıtları korumayı kolaylaştıracağını savunan Baş Polis Memurları Derneği ACPO (Association of Chief Police Officers) konu ile ilgili dört temel ilke den söz etmiştir [72]. ACPO'nun 4 temel ilkesi Tablo 2.1'de gösterilmiştir.

Tablo 2.1. ACPO ilkeleri [72]

İlke 1	Kolluk kuvvetleri veya onların temsilcileri tarafından yapılan hiçbir işlem, daha sonra mahkemede güvenebilecekleri bir bilgisayarda veya depolama ortamında tutulan verileri değiştirmemelidir.
İlke 2	Bir kişinin bir bilgisayarda veya depolama ortamında tutulan orijinal verilere erişmeyi gerekli gördüğü durumlarda, o kişi bunu yapmaya yetkin olmalı ve eylemlerinin uygunluğunu ve etkilerini açıklayan kanıtlar sunabilmelidir.
İlke 3	Bilgisayar tabanlı elektronik kanıtlara uygulanan tüm işlemlerin bir denetim izi veya başka bir kaydı oluşturulmalı ve korunmalıdır. Bağımsız bir üçüncü taraf bu süreçleri inceleyebilmeli ve aynı sonucu verebilmelidir.
İlke 4	Soruşturmadan sorumlu olan kişinin (dava memuru), kanuna ve bu ilkelere uyulmasının sağlanması konusunda genel sorumluluğu vardır.

Adli bilişim süreçleri, bilgisayar suçu ile ilgili kanıtların bütünlüğünü ve gözetim zincirini koruyarak düzgün bir şekilde mahkemeye sunulmasını sağlamak için oluşturulan bilimsel süreçlerdir. Bu süreçlerin nihai amacı ise "neler oldu, kim dâhil oldu, ne zaman gerçekleşti, nerede gerçekleşti, neden oldu ve olay nasıl meydana geldi" sorularını cevaplayabilecek kanıtlar elde etmektir [73].

Suç soruşturmalarında olayların yeniden inşasını kolaylaştırmak veya ilerletmek amacıyla dijital kaynaklardan elde edilen kanıtları bilimsel bir yol izleyerek gerçeğe uygun değerlendirilmesi için adli bilişim süreçleri ile ilgili birçok model geliştirilmiştir [74]. Ancak geliştirilen her model kendi alanı içerisindeki sorunlara çözüm üretmek için geliştirilmiştir. Suç soruşturmalarında kanıtların mahkemeye sunulma aşaması genelde kanıtları elde etme, koruma, analiz ve raporlama aşamalarından oluşmaktadır. Adli bilişim soruşturmaları için geliştirilen süreç modelleri de bu temel üzerinde geliştirilmektedir.

Kruse ve Heiser Modeli (2001)

Lucent modeli olarak da bilinen bu model adli bilişim süreçlerini "Elde Etme (Acquire), Belgeleme (Authenticate) ve Çözümleme (Analyses)" olarak üç aşamada ele almıştır. Ayrıca ilk harflerinden dolayı literatürde 3A modeli olarak da bilinmektedir. Bu model adli bilişim süreçlerini basit ve genel bir çerçeve ile ele almıştır [75].

ABD Adalet Bakanlığı Modeli (USDOJ, 2001)

Dijital kanıtlarla ilişkili suç mahallinin soruşturma sürecini içeren ve acemi katılımcılar için bir rehber haline gelen bu model, daha sonra kolluk kuvvetleri ve diğer kurumlar tarafından dijital kanıtları güvence altına almak ve tanımlamak için de kullanılmıştır.

Bu modelin ilk aşaması, suç mahallinde kapsamlı bir araştırma süreci gerçekleştirdikten sonra kanıtların toplanmasıyla ilgilidir. İkinci aşama, önceki aşamadan toplanan kanıtları şeffaf bir şekilde bir araya getirmek ve kaynağını tanımlamak olan inceleme sürecini içermiştir. Üçüncü aşama, kanıtların kullanılabilirliği ile ilgili analizin yapıldığı süreçtir. Son aşama ise önceki tüm aşamaların sonuçlarının raporlanması ve tüm süreçte toplanan bilgileri içerir [76]. Bununla birlikte, bu modelin tek kısıtlaması, belirsiz kalması ve düzgün bir şekilde açıklanmamasıdır.

DFRWS Modeli (2001)

Dijital Adli Araştırmalar Çalıştayı tarafından yönetilen ilk büyük ölçekli konsorsiyumda, adli bilişim uzmanları, uygulayıcılar, güvenlik kurumları ve siviller tarafından "Tanımlama, Sunma, Toplama, İnceleme, Analiz Etme ve Raporlama" aşamalarından oluşan altı (6) basamaklı süreç olarak geliştirilmiştir. Bu model adli bilişim süreçlerinin standart ve tutarlı bir iskeletini oluşturmanın yanında teknik ve teknik olmayan kullanıcılar tarafından kolayca anlaşılabilir bir

yapıya sahiptir. DFRWS modelinin tanımlama aşaması, bir olaya müdahale etmeden önce adli süreçleri organize etmek için olay öncesi hazırlığı dışarıda bıraktığı için yeterince geliştirilememiştir [77].

Soyut Dijital Adli Tıp Modeli (ADFM, 2002)

2002 yılında dijital adli soruşturma modelini daha da netleştirmek ve sadeleştirmek için DFRWS modeline kanıtları biriktirme konusundaki geleneksel yaklaşımı dâhil ederek yeni bir model geliştirilmiştir. Bu model "Tanımlama, Hazırlık, Yaklaşım Stratejisi, Muhafaza, Toplama, İnceleme, Çözümleme, Sunum ve Delilin İadesi" aşamalarından oluşmaktadır.

Bu modelin ilk aşaması, meydana gelen olayın türünü tanımlamak ve bu modelin amacına ulaşması için tüm yardımı sağlamaktır. İkinci aşama, bu adli modelin kalan aşamalarında kullanılacak yöntem ve prosedürler hakkında hazırlık yapmaktır. Ayrıca, kanıtları toplamak için gerekirse farklı arama emirlerinin hazırlanmasına da rehberlik eder. Üçüncü aşama, kanıt toplama sürecinin beşinci aşamasındaki yaklaşım ve süreçler geliştirmektir. Modelin dördüncü aşaması, potansiyel olarak ilgili delilleri içeren tüm bileşenleri ve cihazları korumaktır. Cihazları ve bileşenleri içeren kanıtları sağlamlaştırdıktan sonra, fiziksel sahneyi kaydetmek ve prosedürlerin birleştirilmesi için beşinci toplama aşaması kullanılır. Altıncı aşama, işlenen suçun ilgili şüphelisini bulunmasıyla ilgilenen analiz aşamasıdır. Yedinci aşama, denetimin yapıldığı maddelerin önemini analiz etmektir. Sekizinci aşama analiz aşaması ve daha sonraki aşamada gelen sonuçların sunumunu içerir. Son ve dokuzuncu aşama, görevlerin yerine getirilmesinden sonra cihazları ve dijital kaynaklarını gerçek sahibine iade etme sürecini içerir. Tanımlanan bu modeldeki kusur veya boşluk, üçüncü aşamanın bir dereceye kadar ikinci aşamaya oldukça benzer olmasıdır [76].

Entegre Dijital Araştırma Süreci (IDIP, 2003)

Entegre Dijital Araştırma Süreci olarak adlandırılan bu model adli bilişim araştırması yapmak ve kanıtları toplamak için adli uzmanlar için başlıca bir rehber haline gelmiştir. Bu model "Hazırlık Aşaması, Dağıtım Aşaması, Fiziksel Suç İnceleme Aşaması, Dijital Suç İnceleme Aşaması ve Gözden Geçirme Aşaması" olmak üzere beş aşamada ele alınmıştır.

Hazırlık aşamasının amacı soruşturma sürecinin geri kalan aşamalarını hazırlanmaktır. İkinci aşama, adli uzmanlara olayı tespit etme ve ardından sertifikalandırma becerisi kazanabilecekleri bir sistem sağlar. Üçüncü aşama, olay yerindeki fiziksel delilleri toplamak, incelemek ve olay sırasında ortaya çıkan eylemlerin keskin gözlemini yapmakla ilgilidir. Dördüncü aşama üçüncü aşamaya benzer olarak fiziksel suç mahalli araştırma aşamasında elde edilen dijital kanıtların incelenmesi ve toplanmasıyla ilgilidir. Beşinci ve son aşama, dijital adli soruşturma sürecinin önceki aşamalarında yapılan tüm analizleri gözden geçirmektedir. Bu modelin ikinci aşamasında meydana

gelen olayın belgelendirilmesi ile ilgilenmesi, modelin yaygın olarak kullanılmasına engel olmuştur [78].

Geliştirilmiş Dijital Araştırma Süreç Modeli (EDIP, 2004)

Adli bilişim sürecini, IDIP 'dan farklı olarak yinelemeli olarak tasvir eder. Fiziksel ve dijital olay yeri inceleme aşamalarındaki aşamaları yeniden tanımlamıştır. Bu model "Hazırlık Aşaması, Dağıtım Aşaması, Geri İzleme Aşaması, Dinamit ve Gözden Geçirme Aşaması" olmak üzere beş (5) aşamada ele alınmıştır

EDIP modeli elektronik ve dijital olmayan teknolojiler için tutarlı ve standartlaştırılmış bir model oluşturmanın yanında gelecekteki dijital teknolojilere uygulanabilir bir çerçeve sunmaktadır. Bu avantajlarının yanında modelin ek alt aşamalarının bazı belirsizlikler içermesi ve bazı faaliyetlerinin birbirinin tekrarı durumunda olması, bu modelin dezavantajları arasında gösterilebilir [79].

Bilgisayar Adli Tıp Saha Triyaj Süreç Modeli (CFFTPM, 2006)

Bu model kısa bir sürede olay yerinde inceleme ve analiz yapabilmenin yanında araştırmacılara zamana duyarlı potansiyel psikolojik avantaj sağlamaktadır. Modelin odak noktaları "1. Hemen kullanılabilir kanıt bulun, 2. Akut risk altındaki mağdurları belirleyin, 3. Devam eden soruşturmayı yönlendirin, 4. Potansiyel masrafları belirleyin ve 5. Suçluların topluma yönelik tehlikelerini doğru bir şekilde değerlendirin" şeklindedir. CFFTPM modeli "Planlama, Triyaj, Kullanıcı Kullanım Profilleri, Kronoloji Zaman Çizelgesi, İnternet Faaliyeti ve Vakaya Özgü Kanıtlar" aşamalarını içerir. Bu altı (6) aşama içerisinde yüksek bir sınıflandırma düzeyi ve her aşamada çeşitli alt görevleri vardır.

Sadece olay yerinde yapılan araştırma için uygun olan bu model hızlı bilgi edinme ve kritik durumlarda araştırma için avantaj sağlar. Soruşturma aşamasında sahne dışında ek çalışmalar yapılması gerektiğinde de kanıtlardan ödün verme olasılığı vardır [80].

Genel Bilgisayar Adli Tıp Soruşturma Süreci Modeli (GCFIPM, 2011)

GCFIPM modeli "Ön işlem, Edinme ve Koruma, Analiz, Sunum ve Son İşlem" aşamaları olmak üzere toplam beş (5) aşamadan oluşmaktadır. Ön işlem aşaması, soruşturmanın başlaması, gerçek zamanlı veri toplama, ilgili makamdan gerekli onayların alınması gibi yürütülen faaliyetleri ele almaktadır.

Edinme ve koruma aşamasında; tanımlama, toplama, taşıma, depolama ve koruma ile ilgili görevler yerine getirilir. Adli soruşturmanın çekirdeği olarak kabul edilen analiz aşamasında; elde edilen veriler üzerinde suç kaynağı ve muhtemelen suçu işleyen kişinin tespiti ile ilgili analizler yapılır. Sunum aşamasında; analiz aşamasından elde edilen çeşitli sonuçların kolayca anlaşılan ve yeterli kabul edilebilir bir şekilde desteklenen bir formatta belgelenerek yetkililere

raporlanmaktadır. Soruşturmanın uygun şekilde kapatıldığı son işlem aşaması sonrası hak sahiplerine gerekli dijital ve fiziksel kanıtlar verilerek soruşturma süreci gözden geçirilir.

Bu modelin çeşitli adli bilişim soruşturmalarına uygulanabilirliği ve yeni adli bilişim araştırma modelinin geliştirilmesi için iyi bir başlangıç noktası sağlayacak geniş bir çerçeve görevi görmesi avantajları arasında sayılmaktadır. Öte yandan bu modeldeki aşamalar, diğer modellerin aşamalarının gruplandırılması ile oluşturulmuştur. Sonuçta gruplandırılmış aşamalarda yinelenen faaliyetler ortaya çıkar. Genelleştirilmiş doğası nedeniyle bu model, bir modelden ziyade bir yönerge çerçevesi olarak değerlendirilmektedir [74].

Bulut Bilişim için Entegre Kavramsal Dijital Adli Model (2012)

Bulut ortamındaki adli soruşturmayla ilgili olarak, bu yeni teknoloji cezai faaliyetler için fırsatlar ve kolluk kuvvetlerine zorluklar getirmiştir. Bu çerçevenin diğer modellerden temel farkı, kanıt kaynağı tanımlama, koruma aşaması, inceleme ve analiz aşaması üzerinde uygulanan yineleme özelliğidir. Verilerin bulutta nasıl işlendiğinin merkezi olmayan doğası, araştırmacılar için yeni yıkıcı zorluklar yaratmaktadır [81].

Veri Azaltma ve Veri Madenciliği Modeli (2014)

Dijital soruşturmalarda karşılaşılan yeni zorluklar göz önünde bulundurarak adli bilişimin toplama, azaltılmış depolama alanı, zamanında inceleme, istihbarat, araştırma, bilgi yönetimi, arşiv ve erişim gibi yedi gereksinimini listeler. Bu model adli bilişimdeki en büyük zorluklardan birinin sürekli artan veri hacmi olduğuna dikkat çekmiştir. Modelin ana fikri, veri indirgeme yöntemini kullanarak verilerin bir alt kümesini elde etmektir. Ana odak noktaları; daha hızlı indeksleme, veri madenciliği, istihbarat analizini kullanma potansiyeli sağlama, çapraz vaka analizi, geçmiş vaka verilerinin ve istihbarat analizinin araştırılmasını sağlamak olarak listelenebilir [82].

Nesnelerin İnterneti Tabanlı Dijital Adli Model (2015)

Nesnelerin İnternetinin (IoT) artan yaygınlığı adli bilişim için yeni sorunlar getirmektedir Bu alandaki analiz, muayene ve depolama gibi korunması gereken çeşitli formatların analizini ele almayı amaçlayarak IoT tabanlı araştırmayla ilgili standart bir prosedürü tanımlamaktadır [83].

Saha İşleme Modeli (2016)

Önerilen son modellerden biri dijital adli alanı çevreliyor. Saha işleme modeli dijital olmayan kanıtları eğitmeye odaklanmıştır. Olay yerinde araştırmanın erken aşamasını yürüten uzmanlar önce ilgili bilgileri analiz ettikten daha sonra laboratuvarda ayrıntılı analizi gerçekleştirmektedir. Yani, geleneksel laboratuvar tabanlı muayenenin bir dizüstü bilgisayar aracılığıyla sahada yapılabilirliği ve bulut sistemi ile birleştirilmesi ile ilgilenmiştir [84].

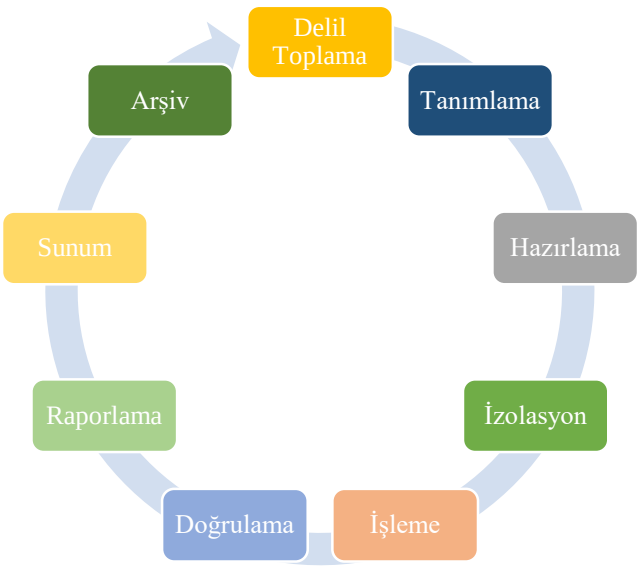
D4I - Siber Saldırıları İncelemek ve Araştırmak İçin Dijital Adli Bilişim Modeli (2020)

Siber saldırıların incelenmesi ve araştırılması için D4I çerçevesi sunulmaktadır. D4I mevcut adli bilişim süreçlerinin yerini almak üzere tasarlanmıştır. D4I çerçevesi, saldırının niteliğine, türüne ve karmaşıklığına bakılmaksızın adım adım ve yarı otomatik bir siber saldırı araştırması yöntemi sağlamaktadır. D4I, diğer adli bilişim süreçleriyle birlikte NIST'in 4 aşamalı dijital adli bilişim sürecini kabul ederek düzenlemiştir [73].

2.8. Mobil Adli Bilişim Süreç Aşamaları

Mobil cihaz adli analizleri süreç olarak iki ayrı yaklaşımla yürütülmektedir. Birinci modelde süreç; Şekil 2.4.'de gösterilen veri girişi, tanımlama, hazırlama, izolasyon, işleme, doğrulama, belgeleme/raporlama, sunum ve arşiv aşamalarından oluşan dokuz katmanlı bir süreç modelidir [14]. Diğer bir süreç ise ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanan mobil cihaz adli inceleme kılavuzunda; Elde Etme, Koruma, İnceleme/Analiz ve Raporlama olarak dört (4) aşamada ele alınmıştır [17]. Mobil cihaz inceleme süreçleri temel olarak birbirine benzerdir. Ancak kullanılan adli araç çeşitliliği ve farklı uygulamalar süreç aşamalarında bazı hatalara sebebiyet vermektedir. Bu nedenle bu hataları en aza indireceği değerlendirilen temel iki süreç modeli ile bağlantılı farklı süreç model önerileri hazırlanmıştır [71].

Mobil cihaz analizlerinin başarılı bir şekilde tamamlanabilmesi için mobil cihaz teknolojisindeki hızlı ilerleyiş karşısında temel süreç modellerinin de sürekli geliştirilmesi ve güncel tutulması gerekmektedir. Ayrıca farklı işletim sistemine sahip mobil cihazların farklılıkları göz önüne alınarak özel süreç modellerine ihtiyaç duyulmaktadır.



Şekil 2.4. Mobil cihazlarda adli bilişim aşamaları [14]

Delil Toplama

Bu aşama inceleme talebinin alınmasıyla birlikte başlamaktadır. Analize konu olay ile ilgili evrakların tanzim edildiği, genel bilgilerin toparlandığı ve tasniflendiği aşamadır.

Tanımlama Aşaması

Mobil cihaz ile ilgili analiz taleplerinin teyit edildiği, analiz konusu ile ilgili genel amaçlarının belirlendiği, adli kopyaların aktarılacağı veri saklama alanlarının hazırlandığı aşamadır.

Hazırlık Aşaması

Analiz edilecek mobil cihazın işletim sistemi, yonga seti ve diğer donanımsal özellikleri ile ekran kilidi vb. adli kopya alınmasına engel durum olup olmadığı ile ilgili genel bilgilerin toplandığı ve en uygun adli araç setlerinin seçildiği aşamadır.

İzolasyon Aşaması

Mobil cihazlar ile ilgili yürütülen adli bilişim işlemleri sırasında bu cihazların çeşitli veri transferi kabiliyetlerinin olduğunun unutulmaması gerekmektedir. Adli süreçlerin sağlıklı yürütülmesi ve elde edilen dijital kanıtların şüpheye mahal bırakmaması için cihaz içerisinde, cihaza el konulan tarihten sonra yeni veri bulunmaması gerekmektedir. Bu nedenle el konulan mobil cihazların izole bir ortamda muhafazası çok önemlidir. Bununla birlikte mobil cihazlara uzaktan erişim yöntemleri ile bağlanak veri kayıplarına sebebiyet verecek durumlarda olabileceğinden adli bilişimin her aşamasında cihazın izolasyonu büyük öneme sahiptir.

İşlem Aşaması

Mobil cihazın izolasyonundan sonra soruşturma konusu ile ilgili cihaz hafızasındaki verilerin tamamı veya bir kısmının çıkarılarak anlamlandırıldığı aşamadır. Şifreli verilerin çözülmesi ile silinen verilerin kurtarılması yine bu aşamada yapılmaktadır.

Doğrulama Aşaması

Mobil cihaz içerisinde elde edilen kanıtların veri bütünlük değerlerinin kontrol edilerek, başka adli araçlarla kanıtların teyit edildiği aşamadır. Elde edilen kanıtlar ayrıca telefon içerindeki veriler ile karşılaştırılarak tutarlılık kontrolleri de bu aşamada yapılmaktadır.

Raporlama Aşaması

Dijital kanıtların belgelendirilerek temel bilgiler ile raporlanması aşamasıdır. Bu aşamada analiz sırasında kullanılan araç setleri, adli kopya alma yöntemleri, materyal bilgileri ve elde edilen kanıtların öz nitelik ile veri bütünlük değerleri raporlanmaktadır.

Sunum Aşaması

Tespit edilen kanıtların açık ifadeler ve görseller ile adli mercilere sunulmasını içeren aşamadır. Gerekli durumlarda tespit edilen dijital kanıtlar dijital bir rapor formatında hazırlanarak sunulmaktadır.

Arşiv Aşaması

Mobil cihazın adli kopyası içerisinde elde edilen dijital kanıtların, düzenlenen bütün belgelerin ve adli kopyalarım yapılacak itirazlara ve değerlendirmelere esas olmak üzere saklanması ve korunmasını içeren süreçtir.

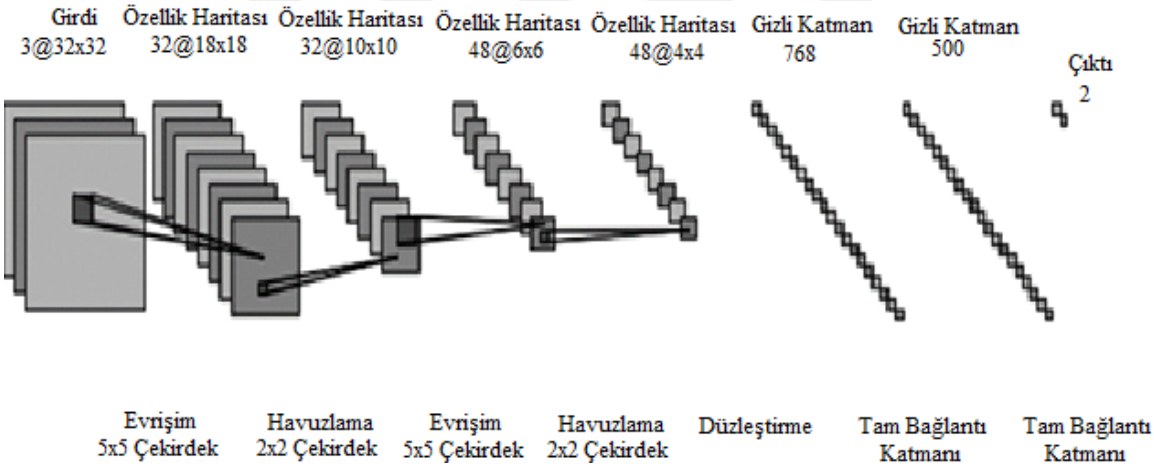
3. DERİN ÖĞRENME YAKLAŞIMLARI VE ÖZELLİK ÇIKARIMI YÖNTEMİ

Bilgi ve iletişim teknolojilerindeki son gelişmeler ışığında, dokunmatik ekran güvenliği de önemli bir başlık haline gelmiştir [85]. Cihazlarını olası tehlikelere karşı korumak için, cep telefonu kullanıcıları öncelikle kullanıcı doğrulaması gerektiren yöntemleri kullanırlar [86]. Bugün, PIN doğrulaması yerine cep telefonu üreticileri; biyometri, örüntü tanıma, hareket algılama, örüntü eşleştirme gibi farklı alternatif yöntemler geliştirmiştir [87]. Dokunmatik ekran teknolojisi, yüksek esneklik ve kullanım kolaylığı nedeniyle mobil bilgi işlem cihazları için kullanıcı kimlik doğrulama teknolojilerinin geliştirilmesini sağlamıştır. Mobil cihazın kilidini açmak için geleneksel teknikler arasında kaydırma, tıklama veya özel bir desen oluşturma, parola verme yer alır. Daha ileri yöntemlerde çeşitli biyometrik yöntemler kullanılmıştır [88]. Bu yöntemler arasında yüz [89], ses [90], parmak izi [91], tuş vuruşu [92] tabanlı kimlik doğrulama yöntemleri yer alır. Mobil dokunmatik ekranların güvenlik özelliklerini geliştirmek için çeşitli desen / jest tabanlı kimlik doğrulama yöntemleri önerilmiştir. Feng ve diğ., kullanıcı kimlik doğrulamasına odaklanan dokunmatik ekranı kullanarak bir dokunmatik sinyale dayalı kullanıcı kimlik doğrulama çerçevesi (parmak hareketi onayı) önerir [86]. Frank ve diğ. kayıt aşamasında bir kullanıcının dokunma davranışını içeren ve dokunmatik ekranla işbirliğini gözlemleyerek kullanıcıyı kabul eden veya reddeden bir sistem önerdi [93]. Shahzad ve diğ. Cep telefonu dokunmatik ekranlarına erişimi güvenli hale getirmeye çalıştı. Yazarlar, mimik tabanlı kullanıcı kimlik doğrulaması için sinyal tabanlı bir kimlik doğrulama planı önermektedir [94]. Meng ve Wong, cihaz kullanıcı kimlik doğrulamasını artırmak için bir dokunma hareketi oluşturan hafif ve avantajlı bir dokunma ilerlemesi doğrulama tekniği öneriyor. Bilgi işlemede zaman kullanımını azaltmak için hafif bir sistem önerilmektedir [95]. Murao ve diğ. yaptıkları çalışmada, gizli tanıma ve benzersiz sinyal doğrulaması yoluyla herhangi bir saldırıyı savunmak için cep telefonu cihazının arkasına monte edilmiş bir ağırlık sensörü kullanarak kavrama hareketleri hakkında bir kullanıcı kimlik doğrulama planı önerdiler [96]. Nader ve ark., dokunma hareketleri açısından tutarlı ve anlaşılır bir kimlik doğrulaması içeren hibrit bir doğrulama yöntemi önermişlerdir [97]. Antal ve Szabó cep telefonlarının kimlik doğrulamasını güçlendirmek için dokunma davranışına ve cihazın minyatürleştirilmiş ölçekli gelişimlerine dayanan bir kullanıcı kimlik doğrulama yöntemi önermişlerdir [98].

3.1. Evrişimli Sinir Ağları (CNN)

Evrişimli sinir ağları [99] (Convolution Neural Networks, CNN) doğadaki gelişmiş görme sistemlerinin taklit edilerek geliştirildiği çok katmanlı algılayıcı ağların bir türüdür. CNN, görüntü

işleme alanında çok iyi sonuçlar vermesinin yanında ses işleme, doğal dil işleme, tavsiye sistemleri, biyometri tanıma sistemleri gibi çok çeşitli alanlarda da başarılı sonuçlar vermektedir. Geleneksel yapay sinir ağlarından (Artificial neural networks, ANN) farklı bir mimaride bulunmaktadır [100]. CNN, ANN ye benzer şekilde girdi, çıktı ve birden fazla gizli katmandan oluşur. Gizli katmanlar içerisinde evrişim katmanları (convolution layers), havuzlama katmanları (pooling layers) ve tam bağlı katmanlar (fully connected layers) bulunmaktadır [101]. Temel katmanlar giriş görüntüsünden özellik çıkarmak için istiflenmesi (stack) sebebiyle CNN için özellik çıkarma mühendisliği gerekli değildir [100]. Havuzlama ve evrişim katmanlarından sonra tam bağlı katmanlar geleneksel yapay sinir ağlarına benzer şekilde görüntü sınıflandırma problemlerini çözmeye çalışır. CNN temel olarak iki dizi arasında bir matematiksel matris işlemi yaparak evrişim işlemini gerçekleştirir [102]. Bu dizilerden birincisi filtre veya çekirdek, ikincisi ise giriş görüntüsünden bir parça veya bu görüntünün sonraki dönüşümlerinden elde edilen parçadır. Eğitim yapılırken CNN bu filtreler için en iyi değerleri öğrenir ve bu şekilde otomatik özellik çıkarma işlemini gerçekleştirir. Şekil 3.1'de genel bir CNN mimarisi gösterilmiştir.



Şekil 3.1. Genel CNN mimarisi [103]

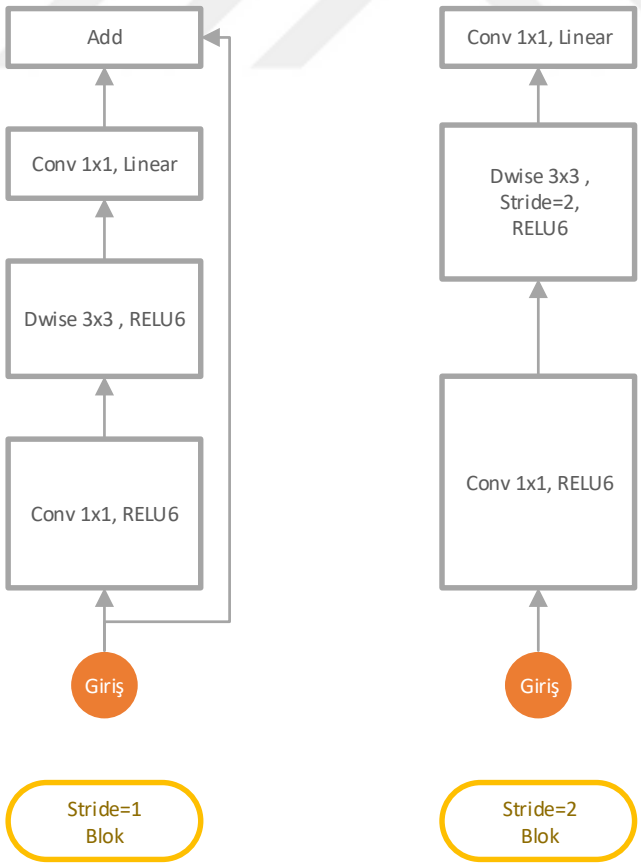
Bir giriş görüntüsü CNN'e verildiği zaman her katmanda sabit boyutlu parçalar çıkarılır ve evrişim işlemleri uygulanır. Her katmanın çıktısı kendisini izleyen katmanın girdisidir. Katmanlar arasında bir görüntü bölgesinden maksimum değeri alarak, boyutu ve parametre sayısını azaltan maksimum havuzlama (max-pooling) operatörleri bulunmaktadır. Bir CNN üzerinde sınıflandırma görevini yerine getiren tam bağlı katmanlar (fully connected) bulunmaktadır [103].

CNN, yeterli kapasitesi ve akıllı model yapısı sayesinde büyük miktardaki verileri işleyebilir ve başarılı sonuçlar çıkarabilir. CNN için başarılı modeller geliştirilmiş ve geliştirilmeye devam edilmektedir. Bu modellerden başlıcaları LeNet-5 [104], AlexNet [105], GoogleNet [106],

VGGNet [107,108], Inception [109], ResNet [110,111] sayılabilir. Sinir ağının bir alanı, mimariyi bir bütün olarak sıkıştırmak için çalışır ve bu nedenle SqueezeNet, ShuffelNet, MobileNet-V1, MobileNet-V2 gibi ardışık ağlarda artan iyileştirmeler bulunmaktadır [112-114]. SqueezeNet ve MobileNet (V1, V2) mimarileri de son zamanlarda hız ve performans açısından tercih edilen mimariler arasında yer almaktadır.

3.1.1. MobileNet-V2 Mimarisi

MobileNet-V2, kısıtlı bir ortamda çalışma üzere oluşturulmuş en optimal derin öğrenme mimarilerinden birisidir [113]. Bu model daha az boyutlu alanda bir pikselin ilgi alanını temsil etmeyi sağlayan ve MobileNET-V1 de tanıtılan genişlik çarpanı kavramının genişletilmiş halidir. Ağ ters artık (residual) bağlantılar dahil edilerek darboğaz katmanı (bottleneck layer) üzerinde ilerler. İki tane genişletilmiş birimi bağlamak için kullanılan normal artık bağlantıların aksine, buradaki ters artık bağlantılar bloklar arasındaki bağlantıyı ifade eder. Genişlik çarpanı, aktivasyon alanını azaltmaya çalışır. Bu şekilde performans olumsuz etkilenmeden rectified linear unit (ReLu) sayesinde yükselir [113]. MobileNet-V2 evrişim yapısı Şekil 3.2'de gösterilmiştir.



Şekil 3.2. MobileNetV2 Evrişimli Bloklar [113]

MobileNet-V2 modelinin öne çıkan özellikleri aşağıdaki gibi özetlenebilir:

- MobileNetV2'de iki tür blok vardır. Birisi artık (residual) bloktur. Diğeri ise küçülme için 2'lik adım olan bloktur.
- Her iki blok da 3 katmana sahiptir.
- İlk katman ReLU6 ile 1 × 1 evrişimlidir.
- İkinci katman derinlemesine evrişimlidir (depthwise convolution).
- Üçüncü katman, 1 × 1 evrişimlidir, ancak doğrusallığı yoktur. ReLU'nun tekrar kullanılması durumunda, derin ağların çıktı alanının sadece sıfır olmayan hacim kısmında doğrusal bir sınıflandırıcı gücüne sahip olduğu ifade edilir.

  Tablo 3.1'de MobileNet-V2 modülüne ait tüm mimari gösterilmiştir.

Tablo 3.1. MobileNetV2 Ana Mimarisi [113]

Input	Operator	t	c	n	s
224^2 x 3	conv2d	-	32	1	2
112^2 x 32	bottleneck	1	16	1	1
112^2 x 16	bottleneck	6	24	2	2
56^2 x 24	bottleneck	6	32	3	2
28^2 x 32	bottleneck	6	64	4	2
14^2 x 64	bottleneck	6	96	3	1
14^2 x 96	bottleneck	6	160	3	2
7^2 x 160	bottleneck	6	320	1	1
7^2 x 320	conv2d 1x1	-	1280	1	1
7^2 x 1280	avgpool 7x7	-	-	1	-
1 x 1 x 1280	conv2d 1x1	-	k	-	

Mimaride verilen kısaltmalardan t: genişleme faktörü, c: çıkış kanalı sayısı, n: yinelenen sayı, s: adım sayısını ifade etmektedir.

3.1.2. SqueezeNet Mimarisi

SqueezeNet, 2016 yılında DeepScale Şirketi, California Üniversitesi, Stanford ve Berkeley Üniversitesi'ndeki araştırmacılar tarafından geliştirilen CNN mimarilerinden biridir. SquezeeNet mimarisinin amacı, bilgisayara kolayca sığabilecek daha az parametreye sahip daha küçük bir sinir ağı modeli oluşturmaktır [115]. SqueezeNet ile oluşturulan model, AlexNet gibi modellere göre çok daha küçük boyutlara sahip olmasına rağmen başarılı sınıflandırma doğruluğu oranlarına ulaşabilmektedir [116]. SqueezeNet mimarisinin ana avantajları küçük modeller oluşması sebebiyle daha hızlı çalışması, daha az iletişim ihtiyacı gerekmesi sebebiyle daha sık aralıklarla güncellenebilmesi yanında gömülü veya mobil sistemler içerisine entegre edilebilmesi şeklinde belirtilebilir. Iandola et al. [116] AlexNET den 50 kat daha hızlı ve 0.5 MB'dan daha küçük olan SqueezeNet modelini duyurdukları çalışmada mimarinin ayrıntılarından bahsetmişlerdir. Bu

amaçla önerdikleri üç strateji bulunmaktadır. İlk strateji için, belirli sayıda evrişim filtresinin maliyeti göz önüne alındığında, 1 × 1 filtrenin 3 × 3 filtreden 9 kat daha az parametreye sahip olması nedeniyle bu filtrelerin çoğunun 1 × 1 seçilmesi önerilmiştir. İkinci strateji olarak, Giriş kanalı sayısını 3 × 3 filtreye düşürülmesi önerilmiştir. Son strateji olarak büyük aktivasyon haritalarının daha yüksek sınıflandırma doğruluğuna yol açabileceği belirtilmiştir. İlk iki strateji doğruluğu korumaya çalışırken CNN'deki parametrelerin miktarını makul bir şekilde azaltmayı amaçlar. Üçüncü strateji ise sınırlı bir parametre maliyeti ile doğruluğu en üst düzeye çıkarmayı amaçlamaktadır. SqueezeNet mimarisine ait boyutlar Şekil 3.3'de verilmiştir.

Katman Adı	Çıktı Boyutu	Filitre Boyutu /Adım	Derinlik	S1x1 #1x1 Sıkıştırma	e1x1 #1x1 Genişletme	e3x3 3x3 Genişletme	S1x1 Sıkıştırma	e1x1 Sıkıştırma	e3x3 Sıkıştırma	#bit	# Budama öncesi parametre	# Budama sonrası parametre
Giriş Görüntüsü	224x224x3											
Evrişim 1	111x111x96	7x7x/2(x96)	1				100%(7x7)			6bit	14,208	14,208
Havuzlama 1	55x55x96	3x3/2	0									
Ateş 2	55x55x128		2	16	64	64	100%	100%	**33%**	6bit	11,920	5,746
Ateş 3	55x55x128		2	16	64	64	100%	100%	**33%**	6bit	12,432	6,258
Ateş 4	55x55x256		2	32	128	128	100%	100%	**33%**	6bit	45,344	20,646
Havuzlama 4	27x27x256	3x3/2	0									
Ateş 5	27x27x256		2	32	128	128	100%	100%	**33%**	6bit	49,440	24,742
Ateş 6	27x27x384		2	48	192	192	100%	50%	**33%**	6bit	104,880	44,700
Ateş 7	27x27x384		2	48	192	192	**50%**	100%	**33%**	6bit	11,024	46,236
Ateş 8	27x27x512		2	64	256	256	100%	50%	**33%**	6bit	188,992	77,581
Havuzlama 4	13x13x512	3x3/2	0									
Ateş 9	13x13x512		2	64	256	256	**50%**		**30%**	6bit	197,184	77,581
Evrişim 10	13x13x1000	1x1/1(x1000)	1					**20%(3x3)**		6bit	513,000	103,400
Ortalama Havuzlama	1x1x1000	13x13/1	0									
	Aktivasyonlar			Parametreler			Sıkıştırma Bilgisi				**1.248,424 (toplam)**	**421,098 (toplam)**

Şekil 3.3. SqueezeNet mimari boyutları [116]

3.2. Minimum İhtiyaç Maksimum Alaka (Minimum Redundancy Maximum Relevance) Özellik Seçimi

Minimum ihtiyaç özellik seçimi, genlerin ve fenotiplerin özelliklerini doğru bir şekilde tanımlamak ve alaka düzeylerini daraltmak için kullanılan bir algoritmadır. Genellikle Minimum İhtiyaç Maksimum Alaka (Minimum Redundancy Maximum Relevance, mRMR) ilgili özellik seçimi ile eşleştirilmesinde tanımlanır. Örüntü tanımadaki temel problemlerden olan özellik seçimi, kullanılan parametrelerle ilişkili ve normalde Maksimum Alaka olarak adlandırılan veri alt kümelerini tanımlar. Bu alt kümeler genellikle ilgili ancak gereksiz veri içerir ve mRMR bu alt kümeleri kaldırarak bu sorunu gidermeye çalışır. mRMR algoritması, sınıf etiketleriyle en çok ilişkilendirilen öznitelikleri seçmeye çalışırken, seçilen özniteliklerin arasındaki fazlalığı en aza indirmeye çalışan bir filtreleme yöntemidir [117]. Algoritma, her bir niteliği ayrı bir tesadüfi

değişken olarak görür. İki özellik arasındaki X ve Y arasındaki benzerlik düzeyini ölçmek için aralarındaki karşılıklı bilgileri kullanır. Denklem (3.1) 'de bu durum gösterilmiştir.

$$I(X;Y) = \sum_{y \in Y} \sum_{x \in X} p(x,y) \, log \frac{p(x,y)}{p(x)p(y)} \tag{3.1}$$

Karşılıklı bilgi, iki özelliğin paylaştığı bilgi miktarını ölçmeyi amaçlamaktadır. Bu nedenle, eğer iki özellik yüksek bir karşılıklı bilgi miktarına sahipse, bunların yüksek derecede ilişkili olduğu söylenebilir ve biri diğerini minimum bilgi kaybıyla değiştirebilir [118].

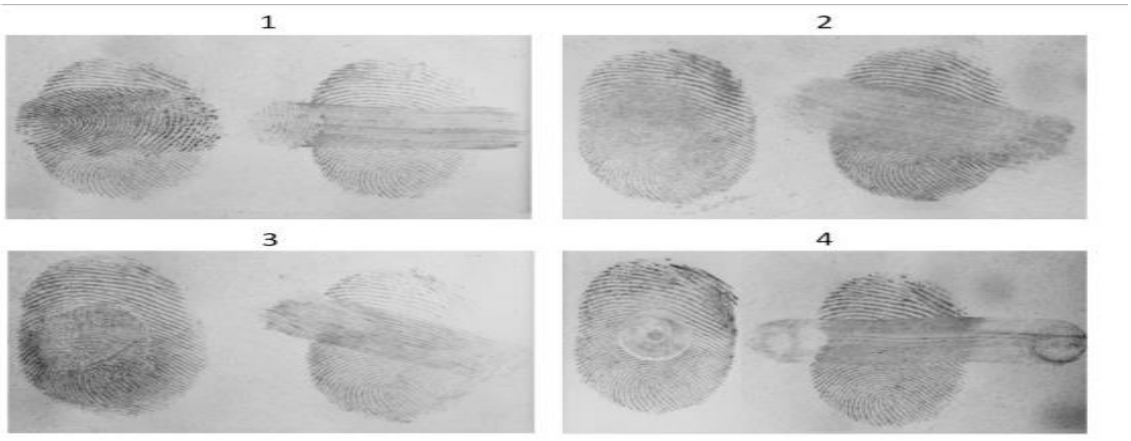
4. ÇALIŞMA METODOLOJİSİ

Tez çalışmasının üç ana amacı bulunmaktadır. Bunlar mobil cihazlardaki ekran izlerinden desen şifresi tespit yöntemi geliştirmek. Desen şifresi tesit yöntemi ile ilişkili mobil cihaz süreç modeli önerilmesi ve son olarak önerilen süreç modeli ile ilişkili Android cihazların adli bilişim analizinin gerçekleştirilmesidir.

4.1. Desen Kilidi Tespit Yöntemi Ön Hazırlık Aşaması

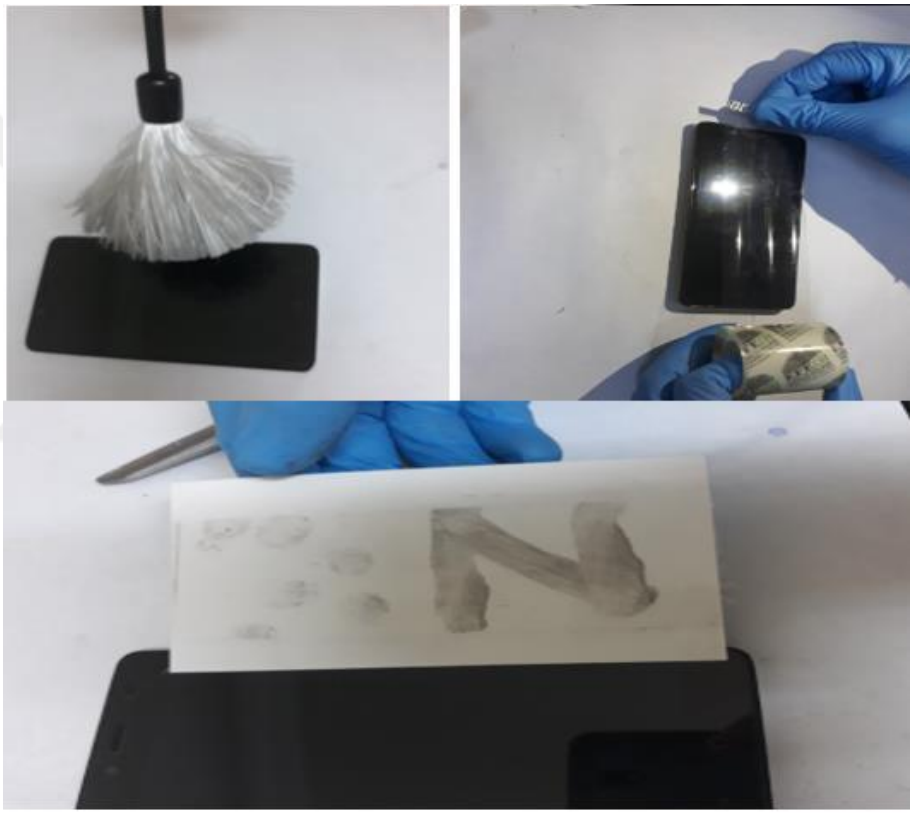
Mobil cihaz kullanıcıların büyük bir çoğunluğu cihazlarına izinsiz girişleri engellemek için desen ve PIN ile koruma yöntemini kullanmaktadırlar. Mobil cihaz üreticileri güncel işletim sistemleri sürümlerinde PIN ve desen kilitlerinin etkisiz hale getirilmesine karşı ek güvenlik önlemleri ile cihaza izinsiz erişimlerin önüne geçmeyi amaçlamaktadır. Bu güvenlik önlemleri adli bilişim açısından mevcut yöntemler ile mobil cihazlardan veri elde etmeyi gittikçe imkânsız hale getirmiştir. Bu nedenle kullanılan donanım ve yazılım kaynaklı kilit atlatma yöntemlerinin dışında ön görülemeyen bir desen ve PIN tespit yöntemi geliştirmek önemli bir ihtiyaç halini almıştır.

Mobil cihaz ekranı üzerindeki izler çıplak parmakla, lateks eldiven, pamuklu eldiven ve stylus pres (Ekran Kalemi) ile dokunma ve kaydırma yapılarak bırakılan izlerin tespit edildiği örnek çalışmada; çıplak parmakla basma ve kaydırma işleminin etkileri (1), lateks eldiven presinin ve kaydırmanın etkileri (2), pamuklu eldiven presi ve kaydırmanın etkileri (3) ve Bir stylus pen (Ekran Kalemi) ve kaydırmanın etkileri (4) 'de gösterilmiştir [119]. Farklı yüzeylerin ekran üzerindeki baskı izi örneklemi Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Dört farklı yüzeyin mobil cihaz ekranı üzerinde bıraktığı kaydırma ve baskı izi [119]

Şekil 4.1.'deki izler incelendiğinde farklı yüzeylerin mobil cihaz ekranlarında bıraktıkları bastırma ve kaydırma izlerinin her koşulda oluştuğu anlaşılmıştır. Mobil cihaz ekranları üzerindeki bu izleri anlamlı verilere dönüştürebilecek sistemler geliştirilmesi ve adli bilişim süreçlerinde entegre edilmesi bu süreçlere önemli bir fayda sağlayacaktır. Bu nedenle yapılacak çalışmaya esas olmak üzere; test için kullanılacak mobil cihazın ekranı 1>2>3>5>7>8>9 desen (pattern) şifresi kullanılarak şifrelenmiş ve cihaz ekran kilidi belirtilen iz yönü takip edilerek açılmıştır. Sonraki aşamada kömür tozu kullanılarak bu izler yapışkan bir bant yardımı ile beyaz bir yüzeye aktarılmıştır. Bu amaçla yapılan ön çalışmaya ait fotoğraflar Şekil 4.2'de gösterilmiştir.



Şekil 4.2. Ekran üzerindeki desen izlerinin belirginleştirme aşaması

Bu izler test aşamasında başarılı bir şekilde alınmıştır. Ancak testler devam ederken cihaz üzerindeki izin netleştirilmesi için fırça ile kömür tozlarının çok hassas bir şekilde dağıtılması gerektiği aksi takdirde izin bozulduğu tespit edilmiştir. Bu yöntem asıl kanıtlara uygulandığında izin bozulması ile yöntemin uygulanabilirliğini etkileyeceği değerlendirildiğinden izin alınması için farklı yöntemler üzerinde çalışılmıştır.

Yapılan çalışmalarda vücuttaki ter vb. sıvılarının cihaz ekranına yapışması ile ekran üzerinde kaygan ve parlak bir yüzey oluşturduğu bu yüzeyin üzerindeki parmak hareketlerinin ışık altında

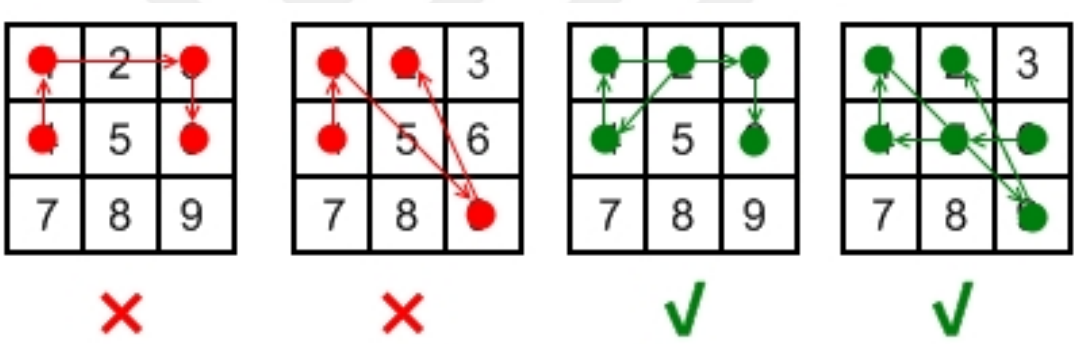
yansıma yaptığı tespit edilmiştir. Ekran üzerindeki izlerin net şekilde tespiti için karanlık oda içerisinde farklı dalga boylarındaki ışık cihaz ekranına farklı açılardan tutularak ekran fotoğrafları çekilmiştir. Çekilen fotoğraflar incelendiğinde izlerin belirginliği ile ilgili ortaya çıkan farklı sonuçlar Şekil 4.3'de gösterilmiştir.

Şekil 4.3. Farklı dalga boylarındaki ışık altında ekran izlerinin görünümü

Elde edilen sonuçların değerlendirildiğinde; alınan başarılı sonuç ve her koşulda uygulanabilirliği nedeniyle 1 numaralı ışık (gün ışığı) kullanılarak veri seti oluşturmanın daha uygun olacağı sonucuna varılmıştır.

4.2. Veri Seti Oluşturma Aşaması

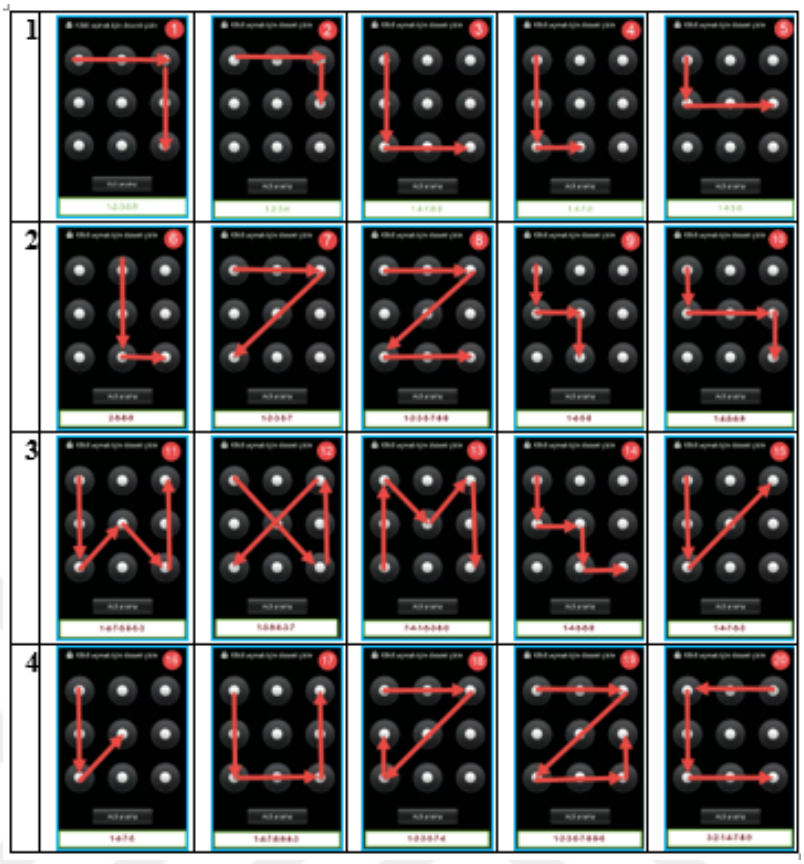
Mobil cihazlar ekran kilitlerinin oluşturulması için cihaz üzerindeki en az 4 en çok 9 nokta birleştirilmesi gerekmektedir. Ayrıca desen oluştururken bir defa geçilen noktadan ikinci defa geçilememektedir. Bu durum oluşturulabilecek desen sayısının sınırlı olmasına neden olmuştur. Mobil cihaz üreticileri bu sınırlı desen sayısının çözümü için belli bir sayıda yanlış deneme hakkından sonra cihazı sıfırlama ya da 50 sn. 1 dk. gibi deneme sürelerini uzatma yöntemleri kullanmaktadır. Mobil cihazlarda kilidi ekranı 1'den 9'a kadar rakamlardan oluşan 3x3 şeklinde konumlanmıştır. $1 \leq m \leq n \leq 9$ olmak üzere iki m ve n tamsayısı verildiğinde, her desen en az m tuşu ve en fazla n tuşu bağlamalı ve tüm anahtarlar farklı olmalıdır. Desendeki iki ardışık anahtarı bağlayan çizgi başka tuşlardan geçerse, diğer tuşların kalıpta önceden seçilmiş olması gerekir. Seçili olmayan tuşa atlamaya izin verilmez. Ayrıca kullanılan anahtarların sırası önemlidir [120]. Bu durumu örneklendiren geçerli ve geçersiz desenler Şekil 4.4'de gösterilmiştir.



Şekil 4.4. Örnek desen oluşturma şeması [120]

İlk desen olan (4-1-3-6) deseni geçersiz bir desendir. Çünkü 1'den 3'e geçerken seçilmemiş olan 2 anahtarından geçeceği için bu desen 4-1-2-3-6 olarak kayıt edilir. Aynı durum (4-1-9-2) deseni içinde geçerlidir. Diğer taraftan (2-4-1-3-6) ve (6-5-4-1-9-2) desenleri seçili olmayan bir anahtar üzerinden atlamadığından geçerli desenlerdir.

Desen şifresi oluşturma adımları belirlendikten sonra uygulamada en çok kullanılan desen şekillerinden 150 tanesi belirlenmiştir. Bu 150 adet desen şifresinden Şekil 4.5'de gösterilen 20 tanesi kullanılarak veri seti oluşturulmuştur.



Şekil 4.5. Veri seti için kullanılan 20 adet desen

Veri seti oluşturma aşamasında ışık altında mobil cihaz ekranındaki yansımayı en aza indirmek için karanlık ya da az ışık alan bir ortam seçilmiştir. Mevcut açıyı korumak için fotoğraf makinası tutucu ile sabitlenmiş ve zemin yansımasını azaltmak için de mat bir plastik zemin kullanılmıştır. Test için kullanacağımız mobil cihazın ayarlarından desen kilidi oluşturulduktan sonra tekrarlı adımlara geçilmiştir.

Tekrarlı adımlar;

1. Mobil cihaz ekranı bir pamuklu bezle temizlenmiştir.
2. Oluşturulan desen kilidi ile cihaz açılmıştır.
3. Desen kilidi açıldıktan sonra ekran tekrar kapatılmış ve fotoğraf makinesi altına yerleştirilmiştir.
4. El feneri kullanılarak uygun açı ile cihaz üzerine ışık verilmiş ve ekran fotoğrafı çekilmiştir.

1'den 4'de kadar olan işlemler Şekil 4.5'de belirtilen her bir desen için 100 defa tekrarlanarak toplam 2000 fotoğraflık veri seti oluşturulmuştur. Bu veri setinin her bir deseni yaklaşık 2 saatlik bir sürede tamamlanarak veri setinin tamamı yaklaşık 40 saatlik bir çalışma sonrasında tamamlanmıştır.

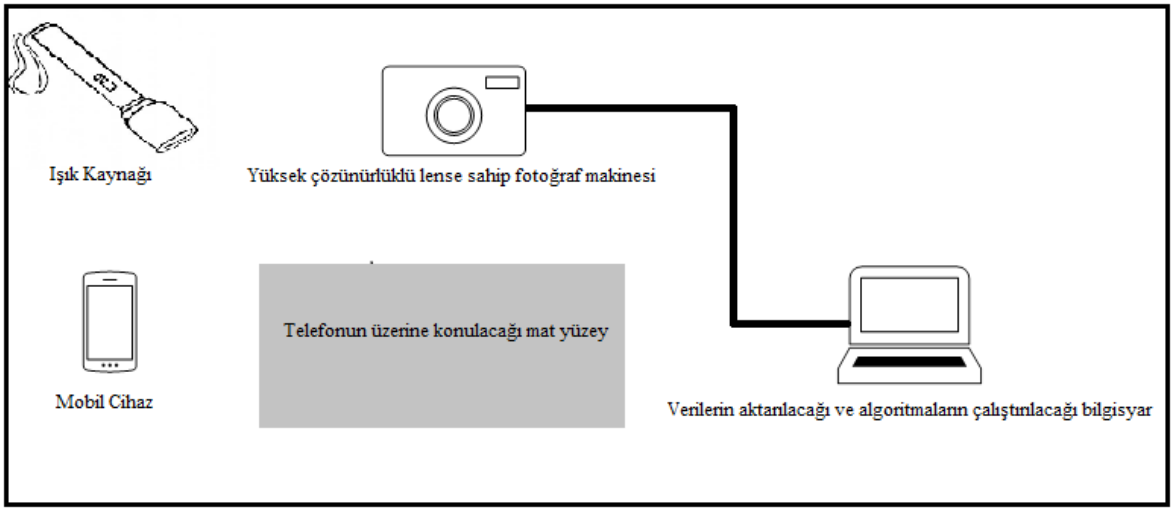
Tez çalışmasında kullanılacak donanımlar Tablo 4.1'de listelenmiştir.

Tablo 4.1. Kullanılan donanımlar

Donanım	Kullanım Amacı
Canon DS126311 Fotoğraf Makinası	Ekran izlerini fotoğraflamak
Fotoğraf makinası tutucu	Fotoğraf makinasını sabitlemek
Mat zemin	Yüzey yansımasını engellemek
Samsung J5 Pro Cep telefonu (Android sürümü 9)	Test cihazı
El feneri	Işık kaynağı
Bilgisayar (Intel i7-7700 CPU, 16 GB RAM, Nvidia GeForce GT740)	Verilerin aktarıldığı ve algoritmaların çalıştırıldığı bilgisayar.

Bu donanımlardan fotoğraf makinası ile mobil cihaz ekranın fotoğrafları çekilerek desen şifresi dijitalleştirilmiştir. Çekilen fotoğraflar daha sonraki aşamalarda önerilen derin öğrenme modeli ile sınıflandırılmıştır.

Desen şifresi tespiti için kullanılacak donanımların kullanım amaçlarını gösteren şema Şekil 4.6'da gösterilmiştir



Şekil 4.6. Önerilen yöntemin çalışma şeması

Bahse konu şemaya göre elimizdeki donanımlar yerleştirilerek veri seti oluşturulmuş ve önerilen yöntem test edilmiştir.

Kullanılan donanımların şemaya uygun olarak konumlandırılmış görselleri Şekil 4.7'de gösterilmiştir.

Şekil 4.7. Kullanılan donanımların konumlandırılması ile ilgili görseller

Önerilen yöntemde desen şifresi ışık kaynağının konumuna göre daha belirgin hale gelmektedir. Farklı desenler için ışık kaynağının konumuna göre faklı sonuçlar alındığından ışık kaynağı sabitlenmemiştir. Desen şifresinin ışık kaynağı altındaki belirgin görüntüsü Şekil 4.7'de gösterilmiştir.

4.3. Mobil Cihaz Analizi Hazırlık Aşaması

Mobil cihazların kullanımındaki artışa paralel olarak Android işletim sistemine sahip akıllı telefonların sayısı da her geçen gün artmaktadır. IDC tarafından yapılan araştırma sonuçlarına göre Android işletim sisteminin pazar payı 2023 yılında %86,7 olması beklenmektedir [121] . Android işletim sisteminin ergonomik, esnek ve özellik bakımından zengin olmasının yanı sıra, başarılı bir işletim sisteminin gerçek gücü mevcut uygulamaların sayısında da yatmaktadır. 2020 yılının ilk çeyreğinden itibaren önde gelen uygulama mağazalarında indirilebilecek uygulamaların sayısına ilişkin verilere göre Android uygulama sayısı 2.56 milyon civarındadır [122]. Bu kadar çok uygulamanın olması Android uygulama geliştiricileri topluluğunun bir sonucudur. Dünya çapında 12 milyondan fazla mobil uygulama geliştiricisinin olduğu ve bunların yarısından fazlasının dikkatini Android 'e odakladığı tahmin edilmektedir [123]. Dolayısıyla halen popüler olan ve pazar

payının büyük bir kısmına sahip işletim sistemine sahip akıllı telefonların dijital suç soruşturmalarında karşılaşılma ihtimalide artacaktır. Bu sebeple Android cihazların adli bilişim incelemelerinde yaşanan sorunlar ve kısıtlılıklara karşı üretilen çözüm yöntemleri, etki edeceği dava sayısı göz önüne alındığında, Android cihazların adli bilişim analizleri daha önemli bir hal almaktadır.

Bu nedenle tez çalışmasında Android cihazların örnek adli kopya alma ve analiz işlemleri gerçekleştirilmiştir. Yapılan örnek analiz ile ilgili kullanılan yazılım ve donanımlara ilişkin bilgiler Tablo 4.2'de listelenmiştir.

Tablo 4.2. Örnek mobil adli bilişim analizinde kullanılacak yazılım ve donanımlar

Donanım/Yazılım	**Kullanım Amacı**
Windows 10 Pro, 64-bit işlemci 16 RAM HP bilgisayar	İş istasyonu
Oxygen Forensic Detective	Adli Araç
XRY	Adli Araç
Ufed Physical Analyzer	Adli Araç
UFED 4PC	Adli Araç
Samsung J5 Pro Cep telefonu (Android sürümü 9)	Test cihazı

Adli bilişim analizleri istisna durumlar dışında delil bütünlüğünün korunması amacıyla adli kopya üzerinden gerçekleştirilmektedir. Cihaz içerisindeki tüm veriler üzerinden analiz gerçekleştirilmesi için cihazın tüm hafızasının kopyasının alınması esastır. Ancak mobil cihazların yapısı gereği çoğu durumda bu pek mümkün olmadığından mantıksal ve dosya sistemli adli kopya alma işlemleri de adli bilişim alanında kabul görmüştür.

Mobil cihaz analizi için yapılan hazırlıklar aşağıda listelenmiştir.

1. Test cihazımız desen şifresi ile koruma altına alınmıştır.
2. Test cihazımız içerisindeki verilerin gerçeği yansıtması için tez çalışmasının başlangıcından itibaren sosyal medya ve sohbet yazışmaları gibi uygulamalar aktif olarak kullanılıştır.
3. Adli kopya alma işleminden önce desen şifresi ile telefon açılmış, Whatsapp uygulaması üzerinden mesaj yazılmış, instagram uygulaması içerisindeki gönderiler kontrol edilmiş ve masa üstüne bırakılmıştır.
4. Bu aşamadan sonra el koyma aşamasındaki prosedürler uygulanarak cihaz ekran resimleri çekilmiş ve daha sonra cihazın adli kopya alma aşamasına geçilmiştir.
5. Yapılacak örnek analizde ortaya çıkacak farklılıkları tespit etmek için test cihazımızın mantıksal ve fiziksel kopyası alınmıştır.

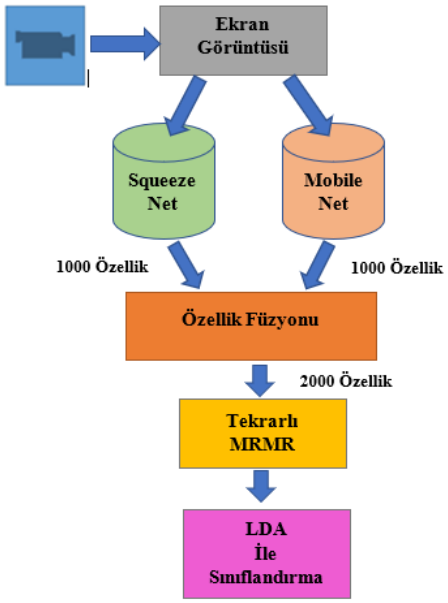
Adli kopya alma ve analiz süreçleri ile ilgili kullanılan yöntemler yedinci bölümde verilmiştir.

5. EKRAN İZLERİNDEN DESEN KİLİDİ TESPİT YÖNTEMİ

Mobil cihazlarını açabilmek için kullanılan desenlerin tespit edilebilmesi amacıyla alınan ekran görüntüleri üzerinde derin öğrenme yaklaşımlarından SqueezeNet ve MobilNET-V2 beraber kullanılmıştır. Özellik çıkarma için tekrarlı mRMR özellik çıkarıcı yönteminden faydalanılmıştır. Elde edilen sonuçların başarımının değerlendirilebilmesi için LDA sınıflandırıcı ile sınıflandırma yapılarak farklı performans metrikleri ile başarım oranları sunulmuştur.

5.1. Desen Tanıma Yöntemi Basamakları

Bilindiği gibi, dokunmatik ekran güvenlik kimlik doğrulama yöntemleri yaygın olarak mobil güvenlik yöntemi olarak tercih edilmiştir. Bu kodları kırmak için adli bilişim uygulamalarında birçok yöntem sunulmuştur. Bu şifreleri otomatik olarak kırmak için, akıllı bir kripto analiz yöntemi sunulmuştur. Derin öğrenme yöntemleri, makine öğrenimi ve yapay zekanın yeni fenomenleridir ve kullanılan ekran güvenliği kimlik doğrulama kodunun tanınmasını otomatikleştirmek için derin öğrenmenin avantajlarından yararlanılmaktadır. Bu nedenle, dokunmatik ekran güvenlik kimlik doğrulaması için yeni bir kaynaşmış derin hafif özellik çıkarma ağı ve Tekrarlı mRMR tabanlı özellik seçim yöntemi sunulmuştur. Kullanılan derin ağlar önceden eğitilmiş ve hafif sıklet ağlardır. Bu yöntemde derin öğrenme yöntemleri özellik mühendisliği yaklaşımı açısından değerlendirilmiştir. Önerilen yöntemin şematik olarak açıklaması Şekil 5.1'de gösteriliştir.



Şekil 5.1. Önerilen modelin grafiksel şeması

Önerilen modelin ImRMR tabanlı ekran deseni tanıma yöntemine ait sözde kod satırı Şekil 5.2‘de gösterilmiştir.

Prosedür: Derin hafif sıklet TmRMR tabanlı görüntü sınıflandırma metodu

Giriş: Ekran Görüntüsü Fotoğrafları (EGF)

Çıkış: Tahmin Değerleri (TD)

00: Görüntüleri Yükle

01: $\boldsymbol{f^1 = SqueezeNet\ (EGF);}$ // ilk 1000 özellik için $\boldsymbol{SqueezeNet}$ uygula

02: $\boldsymbol{f^2 = MobileNetV2\ (EGF)}$; // ikinci 1000 özellik için $\boldsymbol{MobileNetV2}$ uygula

03: $\boldsymbol{X = [f^1\ f^2]}$; // özellikleri birleştir

04: $\boldsymbol{idx = mRMR\ (X, hedef)}$

05: for i=0 to 900 **do**

06: **for** j=1 to 100+i **do**

07: $\boldsymbol{f^s = X(idx(j))}$;

08: **end for j**

09: $\boldsymbol{hata(i+1) = LDA(f^s, hedef, 10)}$; //10 kat çaprazlama ile $\boldsymbol{LDA}$ kullanıp hatayı hesapla

10: end for i

11: $\boldsymbol{[mini, ind] = min(hata)}$; //en iyi özellik setinden minimum hatayı hesapla

12: for i=1 to $\boldsymbol{ind}$ + 99 **to** //en iyi özellikleri seç

13: $\boldsymbol{f^{eniyi}(i) = X(idx(i))}$;

14: enf for i

15: $\boldsymbol{TD = LDA(f^s, hedef, 10)}$;

Şekil 5.2. Önerilen yöntemin sözde kodu

Önerilen yöntemin alt bölümleri, çalışmanın devam eden kısımlarında alt başlıklar halinde detaylandırılmıştır.

Tümleşik Derin Hafif Özellik Üretim Ağı

Makine öğreniminin en önemli aşamasından biri özellik çıkarmadır. Birçok derin ve el yapımı özellik çıkarma yöntemleri vardır. Özellik oluşturmak için önceden eğitilmiş ağlar kullanılmıştır. Bunlar Şekil 5.1'de görüldüğü gibi SqueezeNet ve MobileNet V2'dir. Bu ağların tam bağlantı katmanları, her ağ için 1000 özellik oluşturmak için kullanılmıştır. Bu tümleşik derin hafif

üretici ağda hem SqueezeNet hem de MobileNet V2'nin etkinliğini birlikte kullanılması amaçlanmıştır. Önerilen özellik oluşturma aşamaları aşağıdaki gibidir.

Adım 1: Özellik oluşturmak için ekran görüntüsüne SqueezeNet ve MobileNet V2'yi uygulayın.

$$f^1 = SqueezeNet(SI) \tag{5.1}$$

$$f^2 = MobileNetV2(SI) \tag{5.2}$$

Burada f^1 ve f^2 SqueezeNet ve MobileNet V2'nin 1000 boyutlu özellik çıkarılmış halidir.

Adım 2: iki özellik vektörünün birleştirilmesi ile tümleşik özellik vektörü (X) elde edilmiştir.

$$X\big((h-1)*1000+i\big) = f^h(i), h = \{1,2\}, i = \{1,2,\dots,1000\} \tag{5.3}$$

Adım 1 ve Adım 2, Şekil 5.2'de gösterilen kodun 1-3 arasındaki satırlarını göstermektedir. Bu aşamada, 2000 özellik iki hafif siklet derin ağ kullanılarak üretilir.

Tekrarlayan mRMR Özellik Seçici

mRMR, literatürdeki parametrik özellik seçim yöntemlerinden biridir. En uygun özellik seçim sürecini bulmak çok zordur. Bu aşamada, mRMR kullanılarak otomatik bir özellik seçici sunulmuş ve TmRMR olarak adlandırılmıştır. Bu işlemi gerçekleştirmek için LDA hata üreteci olarak kabul edilir. Minimum hataya sahip özellikler seçilerek, en uygun özellik vektörü seçimi işlenir. Önerilen yöntemin sözde kod satırındaki 4-14 arasındaki satırları, önerilen ImRMR özellik seçicisini ifade etmektedir.

TmRMR'nin adımları;

Adım 3: özellik vektörüne (X) mRMR uygulanarak ve idx değerini hesaplanmıştır. idx, mRMR özellik seçiciyi kullanarak özelliklerin sıralı dizin değerini ifade etmektedir. idx kullanılarak mRMR tabanlı özellik seçim süreci başlatılmıştır.

$$idx = mRMR(X, hedef) \tag{5.4}$$

Adım 4: En değerli özellikler arasından 100 'den 1000 'e kadar seçim yapılmıştır. Zaman maliyetini azaltmak için özellik sayıları bir diziye atanmıştır.

$$f^S_{R-99}(i) = X\big(idx(i)\big), R = \{100,101,\dots,1000\}, i = \{1,2,\dots,R\} \tag{5.5}$$

Burada f_{R-99}^{S} seçilen özellikleri temsil etmektedir. Bu adımda 901 özellik tekrarlı olarak seçilmiştir.

Adım 5: 10 kat çapraz doğrulama ile Doğrusal Diskriminant Analiz (Linear Discriminant Analysis, LDA) yöntemi kullanılarak seçilen her özellik için hata oranları hesaplanmıştır.

$$hata(i) = LDA\left(f_{R-99}^{S}, hedef\right), i = \{1,2, \dots ,901\} \quad (5.6)$$

Adım 6: Minimum hatası olan dizin değeri özelliklerini bulunur.

$$[mini, index] = \min(hata)\,, index = index + 99 \quad (5.7)$$

Burada $mini, index$ dizinin minimum hata değeri ve minimum hata değerinin $index$ değeridir.

Adım 7: idx ve index değerlerini kullanarak en uygun özellikler seçilmiştir.

$$f^{eniyi}(i) = X\left(idx(i)\right), i = \{1,2, \dots , index\} \quad (5.8)$$

Burada f^{eniyi} en iyi özellikleri tanımlamaktadır.

Sınıflandırma

Önerilen tümleşik derin özelliklerin ve TmRMR tabanlı yöntemin son aşaması sınıflandırmadır. Bu aşamada basit ve doğrusal bir sınıflandırıcı seçilir ve seçilen bu sınıflandırıcı LDA'dır. LDA'dan öngörülen değerler Şekil 5.2'nin 15. satırından elde edilir.

Adım 8: Öngörülen değerleri elde etmek için, LDA kullanarak seçilen f^{Best} sınıflandırılır (pv).

$$pv = LDA(f^{eniyi}, hedef, 10) \quad (5.9)$$

Bulgular ve Tartışma

Önerilen derin hafif kaynaştırılmış özellikleri ve ImRMR özellik seçici tabanlı akıllı kripto analiz yöntemini uygulamak için, i7 3.2 GHz CPU ve 32 GB RAM ‘e sahip masaüstü bilgisayarı ve MATLAB2019b programı kullanılmıştır. MATLAB 'ın hem derin öğrenme hem de sınıflandırma öğrenen araç kutusunu sırasıyla özellik çıkarma ve sınıflandırma için kullanılmıştır. Önerilen yöntemin başarımını test etmek amacıyla çeşitli performans metriklerinden faydalanılmıştır. Çalışma için kullanılan performans metrikleri; doğruluk (acc), F1 skoru ($F1$) ve geometrik ortalamadır (gm). Bu performans metriklerinin matematiksel tanımları (5.10) – (5.12) arasındaki denklemlerde verilmiştir.

$$acc = \frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i} \tag{5.10}$$

$$gm = \sqrt[N]{\prod_{i=1}^{N} \frac{TP_i}{TP_i + FP_i}} \tag{5.11}$$

$$F1 = \frac{2 * UAP * UAR}{UAP + UAR} \tag{5.12}$$

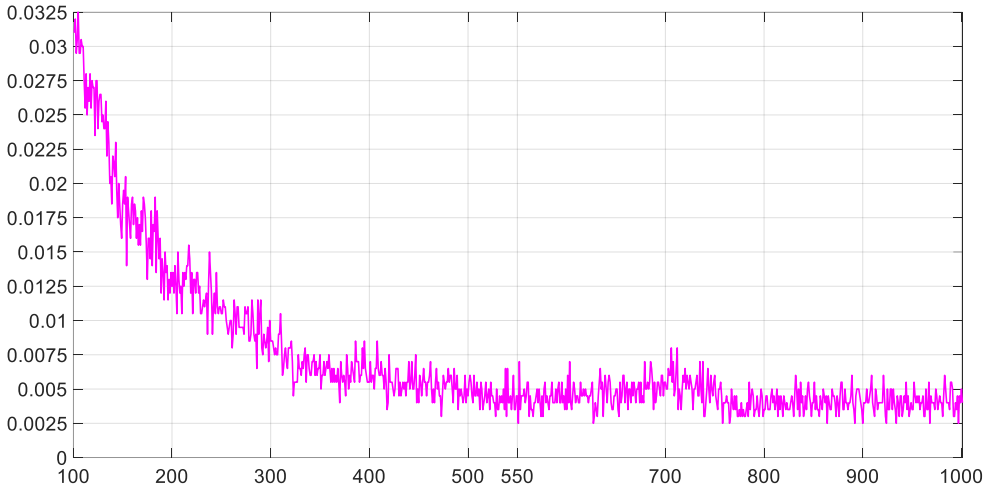
Kullanılan performans metrikleri içerisindeki ifadelerden; TP, doğru pozitif sayısını, TN, doğru negatiflerin sayısını, FP, yanlış pozitif sayısını, FN, yanlış negatiflerin sayısını ifade etmektedir.

LDA sınıflandırıcısı kullanılarak hesaplanan sonuçlar Tablo 5.1'de listelenmiştir. Daha iyi sonuçlar elde edilebilmesi için 10 kat çaprazlama işlemi yapılarak sınıflandırıcıdan sonuçlar alınmıştır.

Tablo 5.1. LDA ile toplanan ekran kilidi desen görüntü veri kümesinde yöntemimizin sonuçları

Performance Metrics	**Rate (%)**
Accuracy	99.75
gm	99.75
F1	99.75

Önerilen yöntemin acc, gm ve F1 skorlarıyla %99,75 sınıflandırma başarısına ulaştığı Tablo 5.1‘de gösterilmiştir. Sonuçlara göre, yanlış sınıflandırılan gözlemlerin sayısı sadece 5‘dir. Tablo 5.1’de gösterilen sonuçlar TmRMR tarafından seçilen 550 özellik kullanılarak hesaplanmıştır. Önerilen TmRMR'nin özellik seçme işlemi ayrıca Şekil 5.3'de gösterilmiştir.



Şekil 5.3. TmRMR yinelemeli özellik seçim işlemi

Şekil 5.3'de verilen satır da gösterilen veriler özellik sayısını, sütün da gösterilen veriler ise hata oranını göstermektedir. Hata oranları 0.0025-0.0325 arasında hesaplanmıştır. Bu oranları kullanarak, LDA sınıflandırıcısına ait doğruluk değeri %96,75 den %99,75' e ulaşmıştır. Minimum hata oranına sahip önerilen TmRMR özellik vektörü kullanarak %99,75 sınıflandırma doğruluğu elde edilmiştir. Tablo 5.1'de belirtilen sonuçlar ile önerilen yöntemin başarısını daha iyi göstermek için toplanan ekran kilidi veri setine daha önceden eğitilmiş bazı derin ağlar ile LDA sınıflandırıcısı kullanılarak performanslar karşılaştırılmıştır. Karşılaştırmalı sonuçlar Tablo 5.2'de gösterilmiştir.

Tablo 5.2. Önerilen derin hafif sıklet tümleşik özellik tabanlı yöntem ile yaygın olarak tercih edilen bazı derin ağların karşılaştırmaları

Yöntem	**Doğruluk**	**Özellik Sayısı**
SqueezeNet	99.45	1000
MobileNetV2	98.20	1000
GoogLeNet	97.0	1000
ResNet18	99.05	1000
ResNet50	99.10	1000
ResNet101	98.75	1000
Önerilen yöntem	99.75	550

Tablo 5.2 'de gösterilen sonuçlar incelendiğinde; önerilen yöntemin bu yöntemler arasında en iyi sınıflandırma doğruluğunu sağladığı görülmüştür.

6. MOBİL CİHAZLARIN EKRAN İZLERİNDEN PAROLA TESPİT YÖNTEMİ İLE İLİŞKİLİ YENİ SÜREÇ TANIMLAMA MODELİ

Android kilidi açma deseni, alfa sayısal şifrelerin ve PIN kodlarının aksine yeni bir kimlik doğrulama mekanizması olarak görülür. Güvenlik açısından, model olarak 3 × 3 ızgara kullanan toplam 389.112 geçerli desene sahiptir. Yayınlanmış araştırmalara göre, kullanıcılar ortalama 7 ila 8 karakter uzunluğundaki şifreleri hatırlayabildiği bildirilmiştir. Android kilit açma deseni, küçük dokunmatik ekranlara uyan etkileşimli ve grafiksel formu nedeniyle mobil cihazlar için daha uygun bir kimlik doğrulama biçimidir. Akıllı telefonlar bir gün boyunca çeşitli durumlarda kullanılmaktadır. Mobil cihazlar sanal klavye ile uzun parolalar yazmak için uygun değildir. Bu nedenle kullanıcılar hızlı ve hatırlanması kolay bir kimlik doğrulama mekanizması kullanmayı tercih etmektedirler [124].

Desen kilidini açma, Google tarafından 2008 yılında tanıtılan nispeten yeni bir jest tabanlı giriş koruma mekanizmasıdır. Android desen kilidiyle cihazın kilidini açmak için, metin kutusuna bir şifre / PIN girmek yerine, kullanıcıdan 3 × 3 ızgaraya noktaları bağlayarak kullanıcı tanımlı bir yol çizmesi istenir. Bu çizilen yola bir kilit açma deseni denir. Bu şekilde noktaların bağlanması ile oluşturulacak desen sayısı Tablo 6.1'de gösterilmiştir.

Tablo 6.1. Android kilit deseninin kombinasyonları [124]

Nokta Sayısı	**Kombinasyon Sayısı**
4	1624
5	7152
6	26016
7	72912
8	140704
9	140704
TOTAL	**389112**

Mobil cihaz kullanıcılarının alışveriş uygulaması, akıllı telefon ekran kilidi ve çevrimiçi bankacılık işlemleri için üç desen oluşturmaları istenilen bir çalışmada; kullanıcıların akıllı telefon ekranını kilitlemek için daha basit desenler seçerken bankacılık ve alış veriş uygulamaları için daha güçlü desenler oluşturmayı tercih ettiğini sonucuna ulaşılmıştır [125].

Araştırmanın bazı sonuçları aşağıda verilmiştir;

- Kişilerin %10'nu harf benzeri desenler kullanmayı tercih etmektedir.
- Şifre oluşturmak için en çok 4 ve 5 nokta kullanılmaktadır.

- Desen oluşturmak için sol elini kullanan kişiler ve sağ elini kullanan kişiler şifre oluşturmaya aynı noktadan başlamaktadır.
- Desenlerin yaklaşık yarısı sol üst köşeden başlamaktadır.
- Sol alt ve sağ üst köşeyi içeren kombinasyonlar insanların kullandığı tüm kombinasyonların %73'ünü oluşturmaktadır.

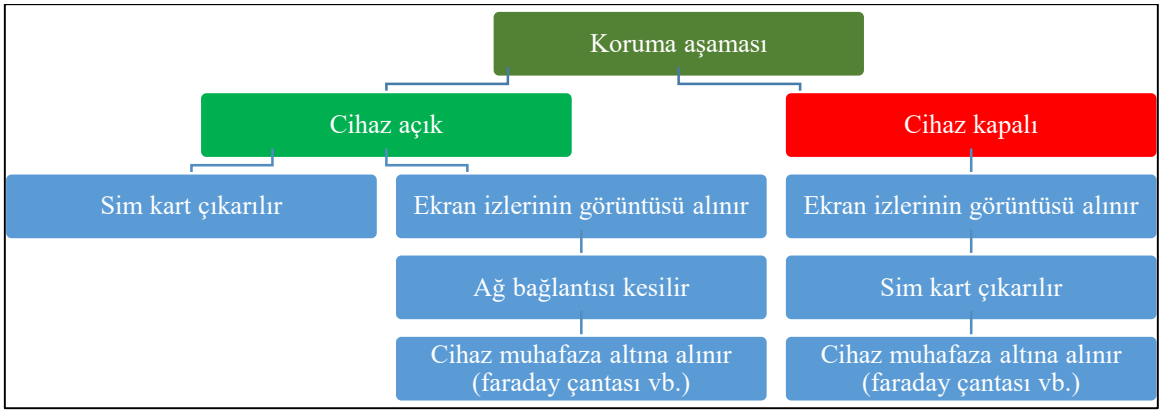
Araştırma sonuçları incelendiğinde; kişisel alışkanlıkların desen şifresini oluşturmada önemli rol oynadığı anlaşılmıştır. Kullanıcıların desen kilidi oluştururken özensiz ve kısa uzunlukta desen belirlemeleri önerilen desen tespit yöntemin başarısını arttıracaktır. Bu nedenle mobil adli bilişim süreçlerine önerilen desen tespit yöntemi ilave edilerek yeni bir model önerisi sunulmuştur.

Mobil cihaz adli inceleme süreç modelleri NIST tarafından hazırlanan mobil cihaz adli inceleme rehberinde de belirtilen "Koruma, Elde Etme, İnceleme/Analiz ve Raporlama" aşamaları ile bu aşamaların kendi içinde genişletilmiş formları olan "Veri girişi, Tanımlama, Hazırlama, İzolasyon, İşleme, Doğrulama, Raporlama, Sunum ve Arşiv" şeklinde ele alınmıştır.

Önerilen model de ekran izlerinden parola tespit edilmesi ile ilgili çalışmalar ile ilişkili olarak adli bilişim temel süreçlerine alt süreçler dâhil edilmiş ve yeniden düzenlenmiştir.

6.1. Koruma Aşaması Süreç Modeli

Dijital delillere el koyma aşamaları göz önene alınarak bu aşamada alınan önlemlerin, elde etme aşamasını olumlu etkilemesi hedeflenmiştir. Gelişen mobil alt yapı, donanım ve yazılım teknoloji ile Android sürümlerindeki güvenlik açıklarının kapatılması, yeni koruma yöntemlerinin gelişmesini sağlamıştır. Bu nedenle mobil cihazların adli kopyasını almak giderek zorlaşmaktadır. Koruma aşamasında el koyma prosedürleri yerine getirilirken süreç şemasındaki hususlar yerine getirilmesi durumunda elde etme aşamasında bazı zorluklar kısmen de olsa aşılacağı değerlendirilmiştir. Koruma aşaması süreç modeline eklenen aşamalar Şekil 6.1'de gösterilmiştir.



Şekil 6.1. Koruma aşaması süreç şeması

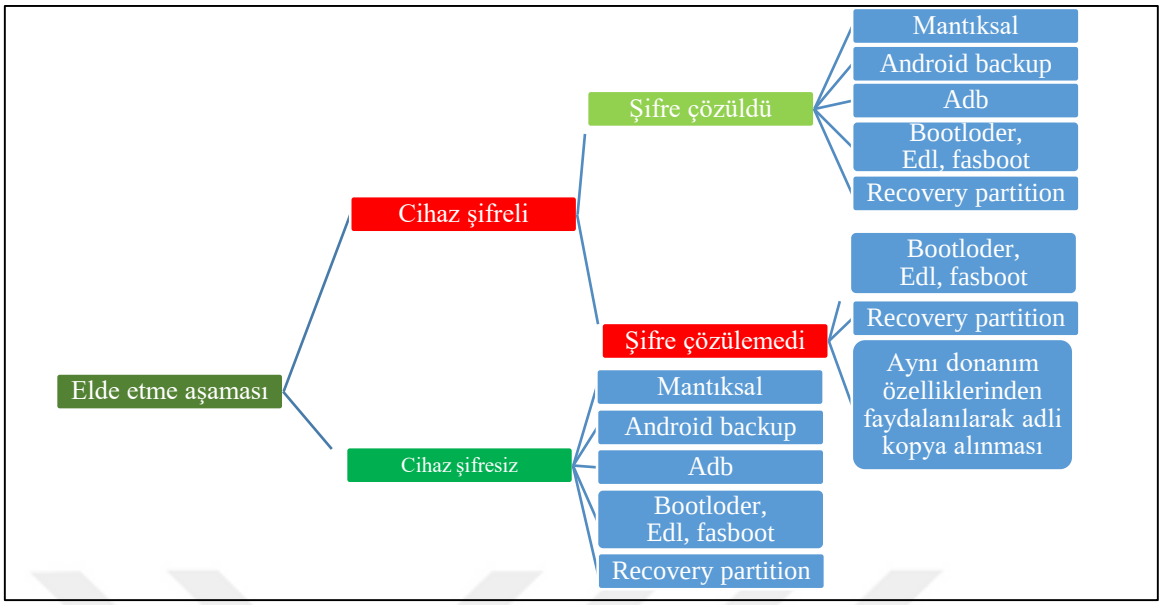
- El Koyma Aşamasında; cihaz açık ya da kapalı olarak karşımıza çıkmaktadır. Her iki durumda ilk olarak cihaz üzerindeki ekran izleri bölüm 4'te ayrıntılı olarak anlatılan yönteme uygun olarak fotoğraflanmalıdır.
- Cihaz üzerindeki ekran izleri alındıktan sonra ağ bağlantıları kesilmelidir. Sim kart çıkarıldıktan sonra cihaz uçak moduna alınarak, faraday çantası gibi izole bir ortamda muhafaza edilmelidir. Böylece cihaz uzaktan müdahale yöntemlerine karşı korunmuş olacaktır.
- Cihazın şifreli olup olmadığı kontrol edilerek varsa cihaz parolası devre dışı bırakılmalıdır.

Ekran izlerinden tespit edilen olası desen, şifre ve PIN elde etme aşamasında en az mantıksal çıkarım yapılmasına imkân tanıyacağı gibi analiz aşamasında karşılaşılan şifreli dosya, doküman ve veri tabanlarının şifre kırma süreçlerinde kullanılabilecektir.

6.2. Elde Etme Süreç Modeli

Elde Etme aşaması süreç modelinde; temel alınan prensip cihazın fiziksel kopyasını almaktır. Ancak bazı soruşturmalarda bu yönteme gerek kalmadan cihazın belirli bölümlerindeki verilerin alınması yeterli olabilir. Her iki durumda cihazın fiziksel adli kopyasının alınması silinmiş verileri kurtarma ihtimalini arttıracaktır. Bazı silinmiş verilerin soruşturmanın seyrini ve karar sürecini değiştirebileceği göz önüne alındığında fiziksel adli kopya alınması önemli bir hal almaktadır.

Yeni nesil Android sürümler, cihaz yonga setleri ve güvenlik uygulamaları fiziksel adli kopya alma sürecinde büyük sorunlara sebep olmaktadır. Fiziksel adli kopya alma süreci ile ilgili dikkat edilmesi gereken adımlar aşağıda sıralanmıştır. Adımlar anlatılırken ticari mobil adli araçları kullanılarak gerçekleştirilebilecek yöntemler ve araç yetenekleri dikkate alınmıştır. Elde etme aşamasında cihazlar ile şifreli ve şifresiz olmak üzere iki farklı şekilde karşılaşılır. Cihazın şifresiz olduğu durumlarda yapılacak işlemler belli olduğundan şifreli cihazlara uygulanan aşağıdaki süreç, şifresiz cihazlar içinde uygulanabilmektedir. Elde Etme aşaması süreç şeması Şekil 6.2 'de gösterilmiştir.



Şekil 6.2. Elde etme aşaması süreç şeması

- Android cihazların hepsi veri alışverişini ADB (Android Debug Bridge) komut kütüphanesi komutları ile gerçekleştirmektedir. Bu komutun kullanılabilmesi için cihazın geliştirici seçeneklerinin açılarak USB hata ayıklama modülünün aktif edilmesi gerekir. Bu modül cihazlarda varsayılan olarak kapalı geldiğinden ve açık olsa dahi cihaz ekranından bu modülün kullanılmasına onay verilmeden bu komutlar kullanılamayacaktır. Bu nedenle şifreli bir cihazın en düşük seviye mantıksal çıkarımını yapmak mümkün değildir.
- Cihaz şifreli ise ticari mobil yazılımların kilit atlama ve devre dışı bırakma yöntemleri ile cihaz şifresi devre dışı bırakılmaya çalışılır.
- Şifre devre dışı bırakma yöntemleri başarı sağlanamadığı durumlarda yazılım güncelleme protokollerine dayanan Bootloader, EDL, Fastboot yöntemlerini kullanılır.
- Bootloader, EDL, Fastboot yöntemlerinin başarısız olması halinde; diğer yöntemlere geçmeden aynı yonga setini kullanan diğer cihaz modelleri tespit edilmelidir. Aynı yonga setini kullanan cihaz listesini bulmak için, bu işi yapan web sitelerinden faydalanılabilir [126]. Tespit edilen benzer cihaz üzerinden adli kopya alma ve kilit atlatma yöntemleri tekrar uygulanmalıdır.
- Bootloader, EDL, Fastboot yöntemlerini ile imaj alınamaması halinde özel kurtarma görüntüsü yükleme yöntemi kullanılmalıdır. Ancak FRP kilidi gibi güvenlik yöntemleri bu yöntemin uygulanması için risk oluşturmaktadır. Bazı modellerde bu yöntem uygulanırken cihazın fabrika ayarlarına dönmesi muhtemeldir.
- Cihaz Android sürümü Android 7 ve üst sürümlerden biri olması halinde yazılım güncelleme protokollerine dayanan fiziksel çıkarım yöntemleri ve özel kurtarma görüntüsü yükleme

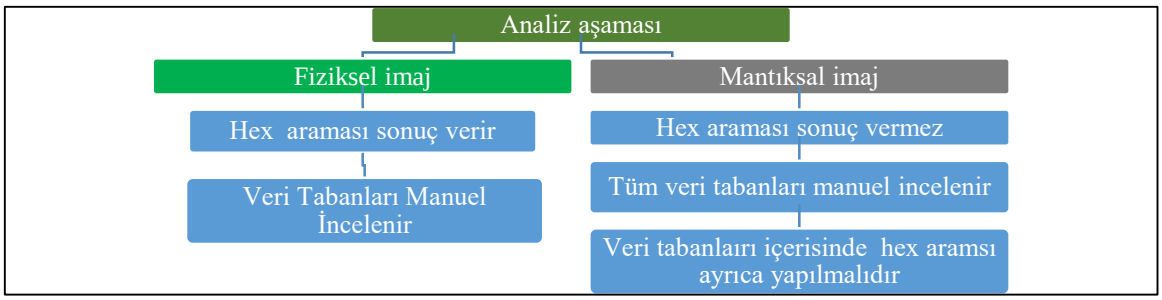
yöntemleri kullanılarak cihaz kapalı konumda alınan adli kopyalar şifreli geleceğinden veriler analiz aşamasında anlamlandırılamayacaktır.

- Ancak adli araç setlerinin bir kısmı son sürüm güncellemeleri ile Android 7 ve üst versiyon cihazların fiziksel ve dosya sistemli imajları için Decryping Qualcomm, Decryping MTK, Decryping Bootloader gibi yöntemler geliştirilmiştir. Bu yöntemlerin daha düşük Android sürümlerine sahip cihazlara uygulanması durumunda cihaz yazılımının çökmesi ve bozulması muhtemeldir.
- Ayrıca koruma aşamasında cihaz ürerindeki parmak izleri alınması durumunda izlerden tespit edilecek olası desen, şifre ve PIN bu tarz cihazların adli kopyaları alınırken ve verilerin şifresi çözülürken kullanılabilmektedir.

6.3. Analiz Aşaması Süreç Modeli

Analiz aşaması süreç modelinde; temel alınan ana prensip elde edilen adli kopya formatı ve yapılacak analizin konusudur. Elde edilen adli kopyanın fiziksel kopya olması halinde hafıza erimlerinde yapılacak Hex aramaları sağlıklı sonuçlar verirken, mantıksal kopya formatlarında Hex araması sonuçları kesin sonuçlar olmamaktadır. Bu yüzden mantıksal adli kopya üzerinden yapılan analizlerde; edinilen veri tabanları ile geri görüntüleme günlükleri içerisinde ayrıca inceleme ve Hex araması yapılması sağlıklı bir analiz için gereklidir.

Analiz işlemleri adli araçların anlamlandırdığı ve ara yüzünde sunduğu verilerin yanında, veri tabanlarının manuel analiz edilmesi önemlidir. Çoğu durumda adli araçlar desteklemediği uygulama verilerine ara yüzlerinde yer vermemektedir. Bu verilere veri tabanları içerisinde ulaşmak mümkündür. İnceleme aşaması süreç şeması Şekil 6.3'de gösterilmiştir.

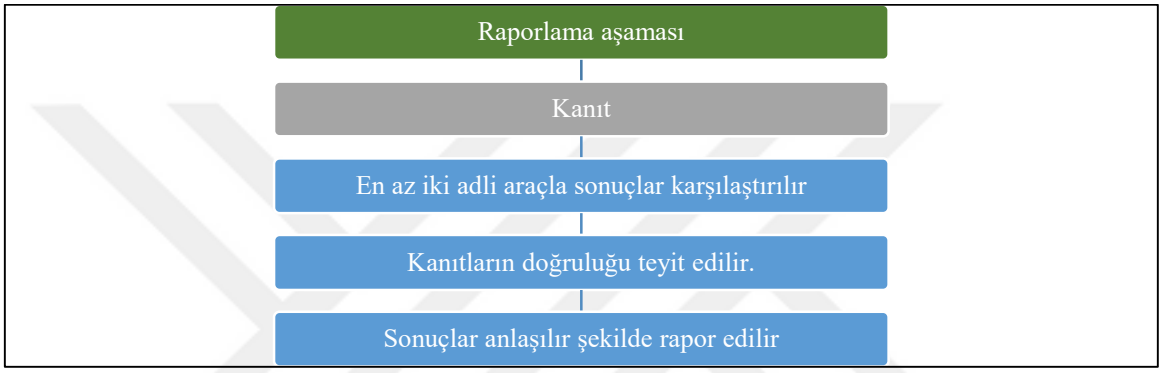


Şekil 6.3. İnceleme aşaması süreç şeması

Kullanıcılar oluşturdukları şifreleri hatırlamak için bağlantılı ve benzer şifreler kullanmaktadırlar. Bu nedenle elde etme aşamasında mobil cihazdan alınan ekran görüntüsünden elde edilene desen, şifre ve PIN analiz aşamasında şifreli verilerin çözülmesinde kullanılacaktır.

6.4. Raporlama aşaması süreç modeli

Raporlama aşaması süreç modelinde; Temel alınan ana prensip analiz süreçlerinin insan ve adli araç faktörüne bağlı olduğu gerçeğidir. Adli araçlar temelde aynı prensiplerde çalışsa da kaynak kodları ve işleyiş farklılığı nedeniyle verileri anlamlandırma ve kurtarma işlemlerinde farklı performanslar sergileyebilmektedir. Bu nedenle Raporlama sürecinde en az iki farklı adli araç ile kanıtlar ve veriler değerlendirmelidir. Kanıt doğruluğu desteklenerek, sonuçlar anlaşılır bir şekilde raporlanmalıdır. Raporlama aşaması süreç şeması şekil 6.4.'de gösterilmiştir.



Şekil 6.4. Raporlama aşaması süreç şeması

Raporlama aşamasında yapılan en büyük hatalardan biri, adli araç setlerine olan güvendir. Bu durum analizcinin kanıtları teyit etmeden raporlamasına neden olmakla birlikte, adli aracın çeşitli sebeplerle anlamlandırmadığı diğer kanıtların tespit edilmesini de engellemektedir.

Bulgular ve Tartışma

Önerilen derin öğrenme tabanlı ekran izlerinden desen tanıma yönteminin girdisi, mobil cihaz ekran fotoğraflarıdır. Bu yöntemin başarısı el koyma aşamasında elde edilen ekran izi fotoğraflarına bağlıdır. Bu nedenle mobil cihaz temel analiz süreçlerine bu yöntem entegre edilerek yeni bir mobil cihaz süreç metodolojisi önerilmiştir.

Önerilen mobil cihaz süreç metodolojisinin uygulanması, önemli bir ekran izi veri seti oluşmasına imkân tanıyacaktır. Bu veri setinin sonraki çalışmalar için ciddi kaynak oluşturması değerlendirilmektedir.

Ayrıca mobil cihaz elde etme sürecine eklenen cihazların benzer donanım özelliklerinden faydalanılarak adli kopya alma yöntemi, durmuş olan süreçlerin devam etmesine imkân sağlayan faydalı bir yöntemdir. Önerilen yöntemin uygulama alanındaki başarısı Bölüm 7 içerisinde örnek adli kopya alma ve analiz uygulamasıyla test edilmiştir.

7. MOBİL CİHAZ ADLİ BİLİŞİM ANALİZ UYGULAMASI

Tez çalışmasının bu bölümünde; örnek bir mobil cihaz adli bilişim analizi ile önceki bölümlerde önerilen ekran izlerinden desen şifresi tespit etme yöntemi ve önerilen mobil cihaz süreç tanımlama modelinin uygulaması gösterilmiştir. Android cihazlarda kullanılan yonga setlerindeki çeşitlilik, adli kopya alma ve analiz aşamalarında birçok farklı yöntemin geliştirilmesine neden olmuştur. Ayrıca Android işletim sisteminin kullanım oranı ve yöntem çeşitliliği nedeniyle örnek adli bilişim analizi Android mobil cihaz kullanılarak gerçekleştirilmiştir.

7.1. Koruma Aşaması

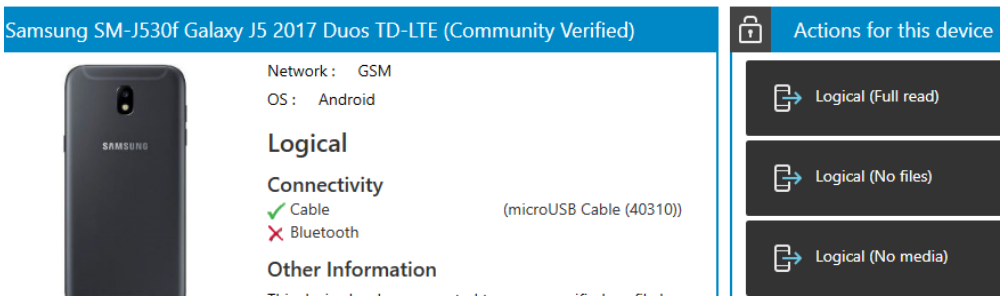
Elde etme aşaması ve analiz aşamasında kullanılmak üzere test cihazımızın ekran izlerinin fotoğrafları çekilmiştir. Sonrasında test cihazımızın ekran kilidi olduğundan sim kart çıkartılmış ve faraday çantası kullanılarak Wifi vb. dışarıdan veri alması engellenmiştir.

7.2. Elde Etme Aşaması

Bu aşamada test cihazının adli kopya (imaj) oluşturma işlemleri gerçekleştirilecektir. Test cihazında desen şifresi olduğundan uygun adli aracın seçimine geçilmiştir.

XRY 9.0.0 Yazılımı Kullanılarak Adli Kopya Alma İşlemi

XRY yazılımı, araştırmacılar tarafından 2003 yılından bu yana resimler, SMS, çağrı geçmişi, iletişim listeleri ve uygulama verileri gibi bilgileri hızlı ve etkili bir şekilde almak için kullanılmaktadır. XRY, dünya çapında 100'den fazla ülkede Polis, Kolluk Kuvvetleri, Askeri, Devlet İstihbarat Kurumları ve Adli Laboratuvarlar tarafından suçu araştırmak, istihbarat toplamak, sahtekarlığı araştırmak ve yolsuzlukla mücadele soruşturmalarında kullanılmaktadır. Akıllı telefon analizi sağlamak için ayrı bir yazılım olarak XAMN kullanmaktadır [127]. XRY yazılımı ile görüntülenen test cihazının desteklendiği adli kopya formatları Şekil 7.1'de gösterilmiştir.



Şekil 7.1. XRY yazılımının Samsung SM-J530F modeline ait desteklenen adli kopya formatları

Samsung marka SM-J530F model test cihazımızın XRY adli aracının desteklediği modeller arasında olduğu anlaşılmıştır. Ancak test cihazımızın sadece mantıksal ve dosya sistemli kopya alma yöntemlerini desteklediği Şekil 7.1'de gösterilmiştir. Dosya sistemli ve mantıksal kopya alma yöntemlerinin uygulanması için cihazın ekran kilidinin kaldırılması ve Android hata ayıklama izinlerinin verilmiş olması gerekmektedir. Test cihazımızda desen kilidi olduğundan mevcut desteklenen yöntemler ile adli kopya alınamamıştır.

Oxygen Forensic 12.0.0.151 Yazılımı İle Adli Kopya Alma İşlemi

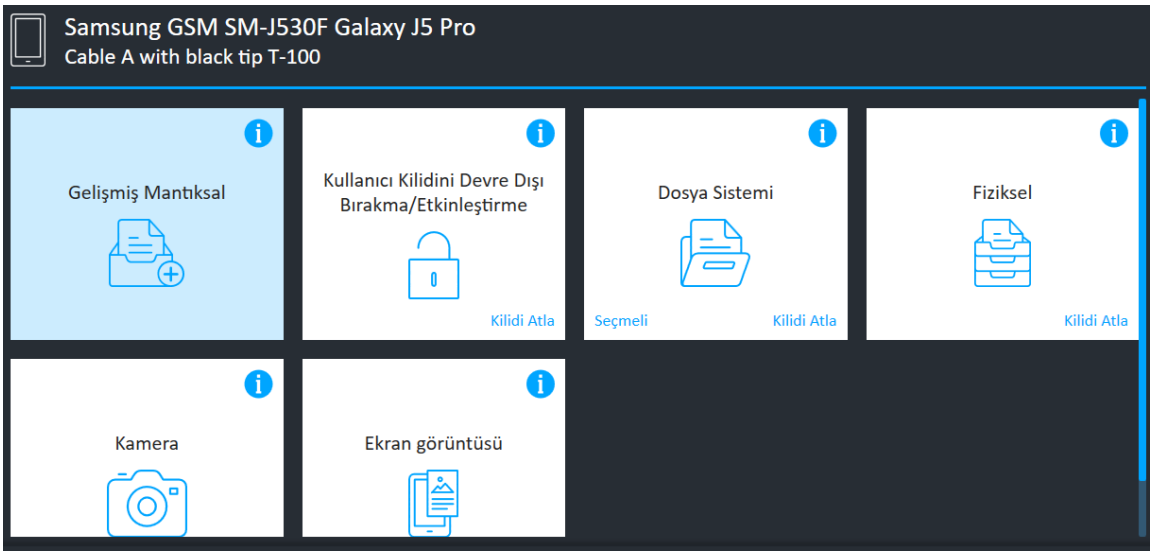
Oxygen Forensic, kolluk kuvvetleri, federal kurumlar ve işletmeler tarafından kullanılan dijital adli bilişim yazılımıdır. Mobil cihazlar, bulut, dronlar ve IoT verileri konusunda uzmanlaşmış olan Oxygen cezai ve kurumsal soruşturmalar için gelişmiş dijital adli veri çıkarma ve analiz araçları sağlamaktadır [128]. Oxygen Forensic yazılımı tarafından desteklenen Samsung J serisi modeller Şekil 7.2'de gösterilmiştir.

Şekil 7.2. Oxygen Forensic yazılımı tarafından desteklenen Samsung J serisi modeller

Samsung marka SM-J530F model test cihazımızın Oxygen Forensic adli aracının desteklediği modeller arasında olmadığı Şekil 7.2'de gösterilmiştir. Dosya sistemli ve mantıksal kopya alma yöntemlerin uygulanması için cihazın ekran kilidinin kaldırılması ve Android hata ayıklama izinlerinin verilmiş olması gerekmektedir. Test cihazımızda desen kilidi olduğundan mevcut desteklenen yöntemler ile adli kopya alınamamıştır.

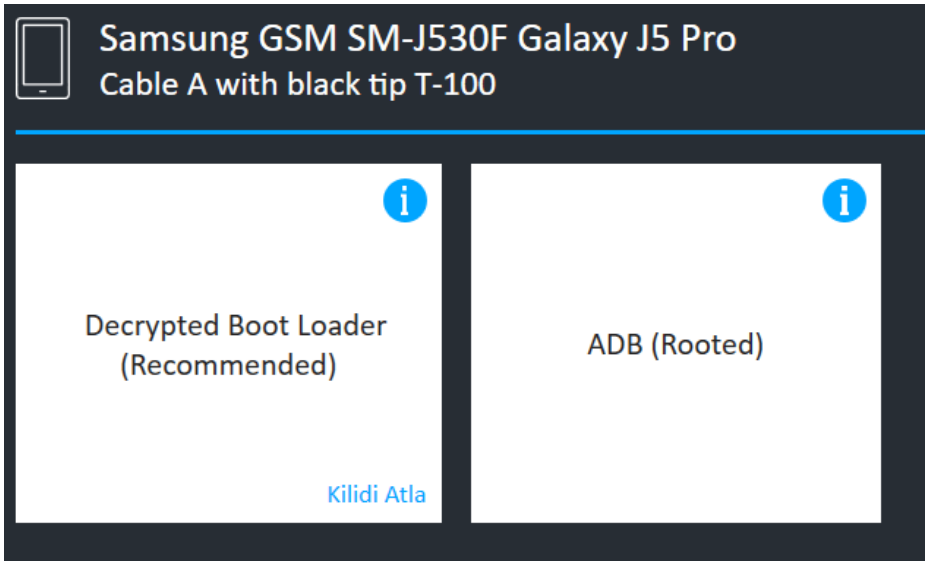
UFED4PC v.7.33.095 Adli Aracı Kullanılarak Adli Kopya Alma İşlemi

Cellebrite, 2007 yılında dijital adli tıp ve soruşturma endüstrisini hedef alan Evrensel Adli Tıp Ekstraksiyon Cihazı (UFED) adını verdiği bir ürün serisi duyurmuştur. UFED sistemi, isteğe bağlı masaüstü yazılımı, veri kabloları, adaptörler ve diğer çevre birimleri ile elde taşınan bir cihazdır. Ayrıca adli kopya almak için donanımsal çözüm üreterek birçok avantaj sağlamaktadır [129]. UFED 4PC yazılımı ile görüntülenen test cihazının desteklendiği adli kopya formatları Şekil 7.3'de gösterilmiştir.



Şekil 7.3. UFED4PC yazılımının Samsung SM-J530F model cihaz için desteklediği adli kopya alma yöntemleri

Samsung marka SM-J530F model test cihazımızın UFED4PC adli aracının desteklediği modeller arasında olduğu, cihazımızın mantıksal, dosya sistemli ve Fiziksel kopya alma yöntemlerinin yanında kilit atlama ve manuel çıkarım yöntemlerini de desteklediği Şekil 7.3'de gösterilmiştir. Dosya sistemli ve mantıksal kopya alma yöntemlerin uygulanması için cihazın ekran kilidinin kaldırılması ve Android hata ayıklama izinlerinin verilmiş olması gerekmektedir. Test cihazımızda desen kilidi olduğundan bu iki yöntem denenememiştir. Fiziksel kopya alma yöntemlerine geçildiğinde seçenek olarak Decrypted Boot Loader ve ADB yöntemleri olduğu Şekil 7.4'de gösterilmiştir.



Şekil 7.4. UFED4PC yazılımının desteklediği Samsung SM-J530F model mobil cihazın fiziksel adli kopya yöntemleri

Bu iki yöntemden ADB (Rooted) kök izni alınmış ve desen kilidi olmayan cihazlarda uygulanabildiğinden test cihazımıza uygulanamamıştır.

Decrypted Boot Loader yöntemi test cihazımızın modeli için Android 8.0 ve alt sürümlerini desteklendiği yöntemin açıklama kısmından anlaşılmıştır. Test cihazımız işletim sistemi Android 9 olduğundan bu yöntemle adli kopya alınamamıştır.

Bu aşamadan sonra adli araçların kilit atlama yöntemleri denenmiş ancak sürüm desteklenmediğinden cihaz kilidi devre dışı bırakılamamıştır.

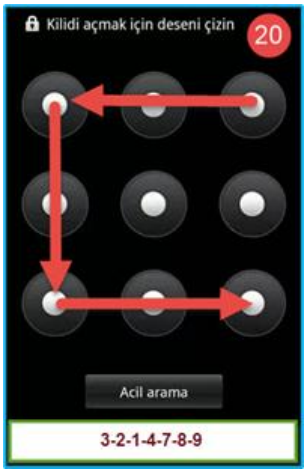
Mevcut yöntemler ile 3 adli araç setinin test cihazımızın modelini desteklediği yöntemler kullanılarak adili kopya alınamamış ve desen kilidi atlatılamamıştır. Bu nedenle mobil cihaz analiz süreci durmuştur.

Desen Kilidi Tespit Yönteminin Uygulanması

Durmuş olan adli bilişim sürecinin devam etmesi için bölüm 4 ve 5'de sunduğumuz ekran izlerinden desen şifresinin elde edilmesi yöntemi ile desen şifresi Şekil 7.5'de gösterildiği üzere tespit edilmiştir. Bu aşamadan sonra cihaz ekranı açılmış ve test cihazımızın dosya sistemli ve mantıksal kopyası alınmıştır.

Şekil 7.5. Önerilen yöntemle tespit edilen ekran desen şifresi

Tespit edilen ekran izlerinin Şekil 7.6'da gösterilen desen ile benzerlik gösterdiği anlaşılmıştır. Ekran üzerinde kullanıma bağlı lekelerin fazla olması resmin daha gürültülü olmasına neden olacağından bu aşamada önerilen derin öğrenme modelimiz ile daha başarılı sonuçlar alınacağı değerlendirilmiştir.



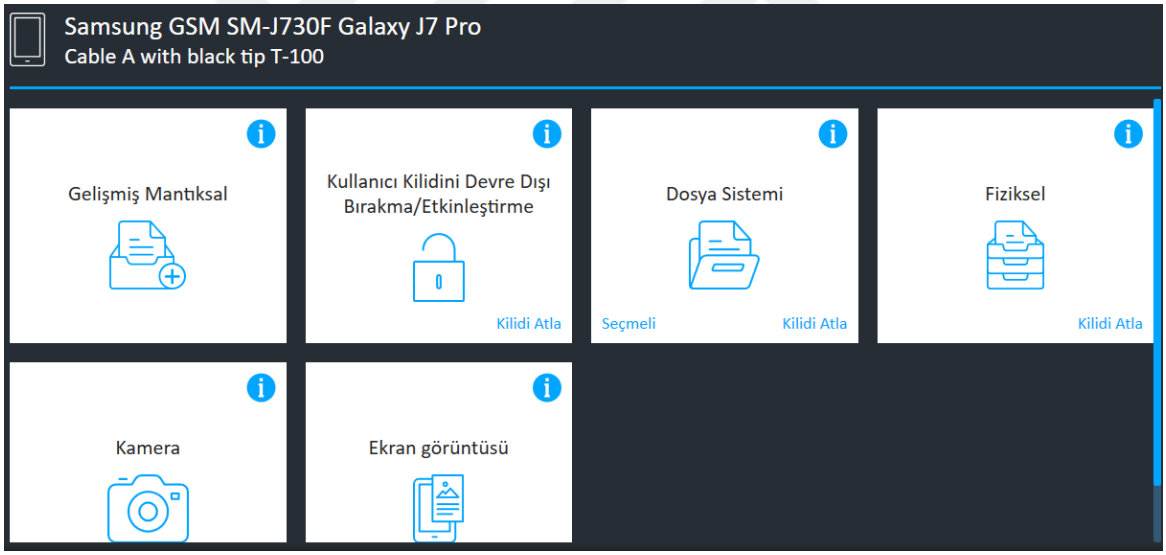
Şekil 7.6. Ekran izlerinin benzerlik gösterdiği desen şifresi

Ekran kilidi ile korunan test cihazımızın 3 adli araç setiyle adli kopyasının alınma sürecinde başarı sağlanamamıştır. Ancak önerdiğimiz yöntemle desen kilidi tespit edildiğinden adli kopya başarılı şekilde alınmıştır.

Aynı Donanım Özelliklerinden Faydalanılarak Adli kopya Alınması

Bölüm 6'de önerilen süreç tanımlama modelinde elde etme aşamasında cihazların aynı donanım özelliklerinden faydalanılarak adli kopya alınabileceği belirtilmiştir. Test cihazımızın donanım özelliklerinin tespiti ile ilgili yapılan açık kaynak araştırmalarında; Samsung Exynos 7 Octa 7870 yonga setine sahip olduğu tespit edilmiştir.

Test cihazımızın "Samsung Exynos 7 Octa 7870" yonga setine sahip olduğu ve aynı yonga setine sahip 44 adet benzer mobil cihaz tespit edilmiştir. Bahse konu test cihazı ile aynı yonga setini kullanan cihazlardan Samsung marka J7 Pro model cep telefonu üzerinden adli kopya alma işlemlerine geçilmiştir. Bu aşamadan sonra 3 adli analiz aracının benzer donanıma sahip cihazları destekleyip desteklemediğine bakılarak uygun modeller üzerinden kilit atlama ve imaj alma yöntemlerine geçilmiştir. Test cihazımız ile aynı yonga setine sahip Samsung J7 Pro model cihazımızın UFED 4PC adli aracı tarafından desteklenen adli kopya yöntemleri Şekil 7.7'de gösterilmiştir.



Şekil 7.7. Test cihazımız ile aynı yonga setine sahip muadil modelin UFED 4PC adli aracı tarafından desteklenen adli kopya yöntemleri

Test cihazımız ile aynı yonga setine sahip cihaz listesinde belirtilen Samsung marka J7 Pro model mobil cihaz UFED 4PC adli aracı içerisinde aratılarak desteklediği adli kopya alma formatları incelendiğinde kilit atlama yöntemlerinin yanında kilitli cihazların dosya sistemli ve fiziksel kopya alma yöntemlerinin Android 9 sürümlerine sahip cihazlar için desteklendiği anlaşılmıştır.

UFED 4PC yazılımıyla Samsung marka SM-J730F model üzerinden Decrypted Boot Loader yöntemiyle test cihazımızın fiziksel çıkarımı gerçekleştirilmiştir. Bu durumu gösteren ayıklama özeti ekranı Şekil 7.8'da gösterilmiştir.

Şekil 7.8. Adli kopya ayıklama özeti

Adli kopya alma aşaması birçok etkene bağlı karmaşık bir süreçtir. Bu karmaşık süreç içerisinde cihazların benzer donanımsal özelliklerinden faydalanılarak adli kopyası alınamayan birçok cihazın farklı modeller üzerinden adli kopyaları başarılı şekilde alınmıştır.

Benzer şekilde mobil cihaz üreticilerin alt yapı ve donanım yetenekleri kullanılarak farklı markalarda cihaz üretilmektedir. Ancak bazen adli araç setlerinin desteklediği markalar içerisinde bu markalara rastlanamamaktadır. Bu durumda cihaz üreticisi asıl markanın modelleri üzerinden adli kopya alma işlemleri gerçekleştirilmelidir. Örneğin General Mobile markalı mobil cihazlar ile Gione markalı ürünler ve Casper markalı ürünler ile Wikoo markalı ürünler aynı adli kopya alma yöntemlerini desteklediği test edilmiş ve başarılı sonuçlar alınmıştır.

7.3. Analiz Aşaması

Bu aşama adli kopya içerisinde analizin konusu ile ilgili verilerin tespit edilmesi ve bu verilerin değerlendirilmesini süreçlerini içerir. Test cihazımızın elde etme aşamasında alınan fiziksel ve dosya sistemli kopyaları içerisindeki veriler bu aşamada analiz edilerek, farklı kopya türleri içerisindeki veri miktarları karşılaştırılmıştır.

Adli araçların Google Play Platformu ve diğer uygulama marketleri içerisindeki bütün uygulamaları desteklemesi mümkün değildir. Bu nedenle analiz aşamasında adli aracın anlamlandırdığı verilerin dışında veri tabanlarının manuel analiz edilmesi çok önemlidir.

Cihaz Temel Bilgileri

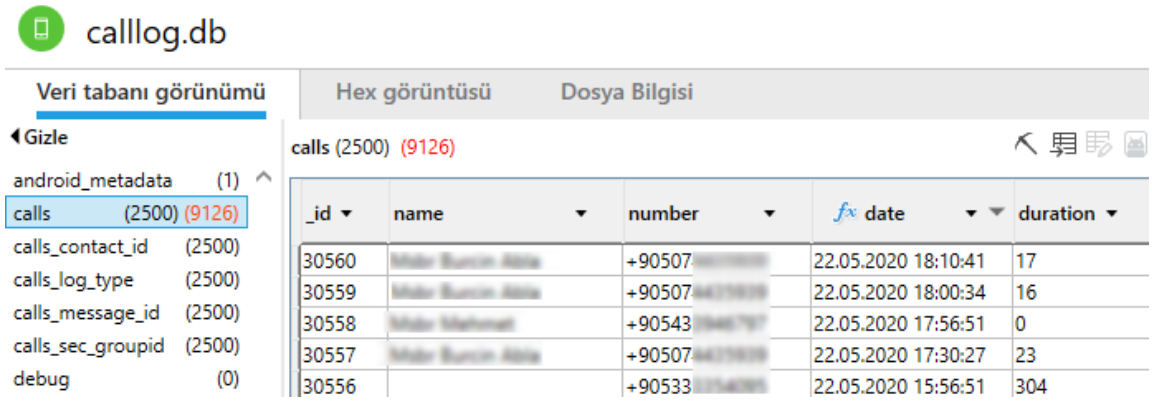
Adli araçlar ara yüz formatlarında genellikle cihaz bilgilerine yer vermektedir. Ancak bazı durumlarda bu bilgilerin manuel kontrol edilmesi gerekmektedir. Test cihazımıza ait cihaz bilgilerinin tutulduğu dosya yolları ve hex görüntüleri Tablo 7.1'da gösterilmiştir.

Tablo 7.1. Cihaz temel bilgileri ve yolu

Cihaz Temel Bilgisi		Yol
IMEI	354053091111857	/Root/data/com.wssyncmldm/2400257.cfg
Marka- Model	Samsung / SM-J530F	/Root/build.prop
Seri No	RF8JB1DDKMD	/Root/FactoryApp/serial_no

Çağrı Kayıtları

Çağrı kayıtları dizinde /Root/data/com.android.providers.contacts/databases/calllog.db yolunda bulunan calllog.db veri tabanı dosyası içerisinde bulunur. Calllog.db bir SQLite veri tabanıdır ve çoğu adli araç tarafından desteklenir veya herhangi bir SQLite görüntüleyicisi tarafından okunabilir. Analizcileri çoğunlukla ilgilendiren birkaç tablo vardır, Bunlar aranan numaralar, süresi, durumu vb. içeriklerdir. Calllog.db veri tabanı dosyası Şekil 7.9'de gösterilmiştir.



Şekil 7.9. Çağrı kayıtlarının tutulduğu calllog.db veri tabanı görünümü

Calllog.db dosyası veri tabanı görünümünde açılıp analiz edildiğinde:

number: gönderenin veya alıcının telefon numarası;

date: çağrı tarihi;

name: telefon numarasıyla ilişkilendirilmiş kişi adı;

duration: çağrı süresini; göstermektedir.

Calllog.db bir SQLite veri tabanı olduğundan benzer verileri getirse de üzerinde kazıma yapmak mümkündür.

SMS/MMS Kayıtları

SMS/MMS kayıtları /Root/user_de/0/com.android.providers.telephony/databases/ mmssms.db dizininde bulunan mmssms.db veri tabanı dosyası içerisinde saklanır. Mmssms.db bir SQLite veri tabanıdır ve çoğu adli araç tarafından desteklenir veya herhangi bir SQLite görüntüleyicisi tarafından okunabilmektedir. SMS/MMS veri tabanı, bazı cihazlarda ADB yedeklemesine dahil edilebilir, ancak genellikle dahil edilmez ve üçüncü parti uygulamalar kullanılarak başka bir şekilde çıkarılması gerekir.

SMS nasıl çalışır;

SMS, depola ve gönder bazında çalışır. Doğrudan alıcıya gönderilmek yerine, SMS mesajları alıcıya ulaşmadan önce birkaç önemli aşamadan geçer.

- SMS mesajı kablosuz iletişim servis sağlayıcısının SMS Merkezine gönderilir.
- İleti dahili olarak işlendikten sonra SMS Merkezi, Ev Konumu Kaydı'na (HLR) bir istek gönderir ve alıcı için yönlendirme bilgilerini alır.
- SMS Merkezi mesajı Mobil Anahtarlama Merkezi'ne (MSC) gönderir.
- MSC, alıcının bilgilerini Ziyaretçi Konum Kaydından (VLR) toplar ve bir kimlik doğrulama işlemiyle devam eder.
- MSC, mesajı bir mobil sunucuya iletir.
- MSC, kısa ilet işleminin sonucunu SMS Merkezi'ne döndürür.
- SMS Merkezi kısa iletinin teslim durumunu gönderene bildirir.

SMS/MMS kayıtlarının tutulduğu mmssms.db veri tabanı dosyası Şekil 7.10'de gösterilmiştir.

sms (4048)

_id	thread_id	address	date	read	type	body
9063	372	+9055	17.05.2020 16:06:35	1	2	
9062	372	+9055	17.05.2020 16:00:56	1	1	
9061	372	+9055	17.05.2020 16:00:54	1	1	
9060	8	ZIRAATBANK	16.05.2020 17:55:28	1	1	16.05.2020 20:55:27 tarihinde internet ve mobil bank
9059	8	ZIRAATBANK	16.05.2020 17:54:58	1	1	Onay kodunuz:550991. Guvenliginiz icin mobil banka
9058	415	AYAKKABICTY	16.05.2020 15:01:09	0	1	BAYRAMA ÖZEL Kadin Erkek Çocuk Ayakkabilarinda

Şekil 7.10. mmssms.db veri tabanı görünümü

Mmssms.db veri tabanı dosyasındaki kayıtların tutulduğu tablolar içerikleri;

id: mesajın veri tabanındaki sıra numarası;

thread_id: mesaj ile ilişkilendirilmiş numaraya atanan sıra numarası;

address: mesaj ile ilişkilendirilmiş numara;

date: mesaj tarihi;

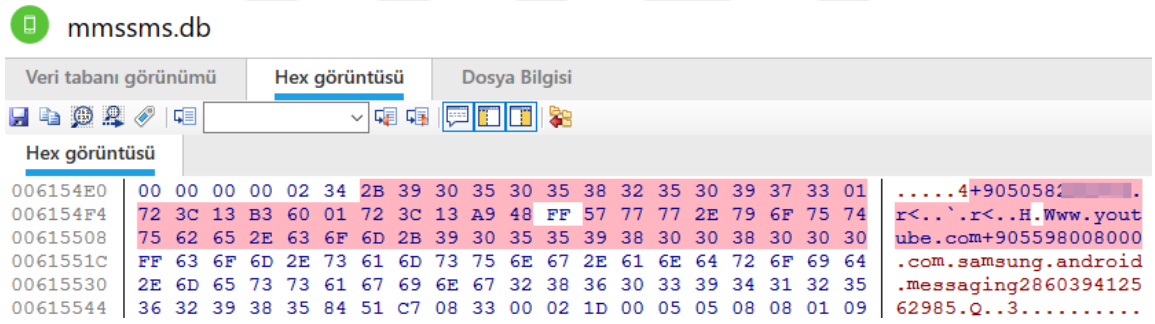
read: okundu/okunmadı bilgisi(değer=1 okundu; değer=0 okunmadı)

type: gönderilen / alınan mesaj bilgisi (değer =1 alındı; değer=2 gönderildi)

body: mesaj içeriği.

Mmssms.db veri tabanı içerisindeki tablo kayıtlarından analizciler için önemli olanlardan bir kısmı yukarıda açıklanmıştır. SMS/MMS kayıtları ile ilgili yapılabilecek manipülasyon iddiaları ile ilgili yapılacak analizlerde mesajın veri tabanı içerisindeki sıra numarası (id) ile geri görüntüleme günlüklerindeki kayıtların analiz edilmesi önemlidir. Ayrıca SMS çalışma prensibine uygun olarak mesaj hex görüntüsü ile ilgili analizler yapılabilir. SMS kaydının hex görüntüsü Şekil 7.11'de gösterilmiştir.

.



Şekil 7.11. SMS kaydın hex görüntüsü

SMS kaydının hex görüntüsü analiz edildiğinde gönderici numara, mesaj metni, mesaj merkezi numarası ve IMSI (International Mobile Subscriber Identity) numarası şeklinde SMS çalışma sistemine uygun kayıtlı olduğu görülmüştür. Yapılacak analizlerde SMS çalışma sisteminin de göz önünde bulundurulması gerekmektedir.

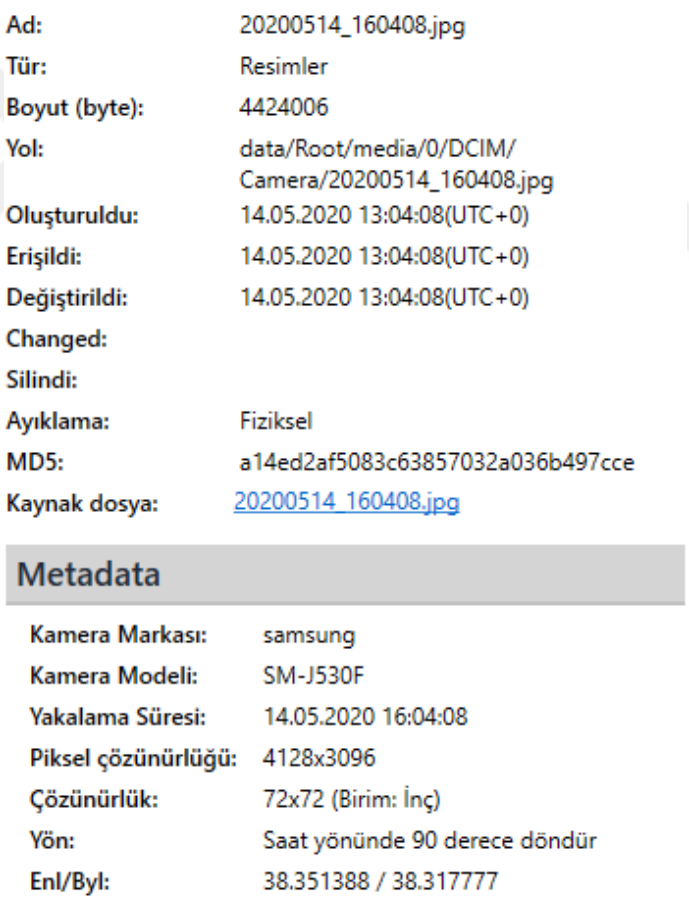
Aranan Öğeler İle İlgili Kayıtlar

Aranan öğeler ile ilgili kayıtlar çoğu zaman bir soruşturmanın kaderini belirleyici sonuçlar içermektedir. Örneğin şüpheli ölüm ve intihar vakalarında internet arama kayıtlarında bulunan intihar ile ilgili sonuçlar başka bir delil olmadığı durumlarda soruşturmanın sonucunu belirleyici rol oynayacaktır. Aranan öğeler ile ilgili kayıtlar birden fazla uygulama kayıtlarından gelebileceğinden tek bir veri tabanında elde etmek imkânsızdır. Örneğin Youtube uygulaması

üzerinden yapılan aramalar /Root/data/com.google.android.youtube/databases/history.db dizininde bulunan history.db içerisinde tutulurken, Play store uygulaması üzerinden yapılan aramalar ise /Root/data/com.android.vending/databases/suggestions.db dizinde bulunan suggestions.db içerisinde tutulmaktadır.

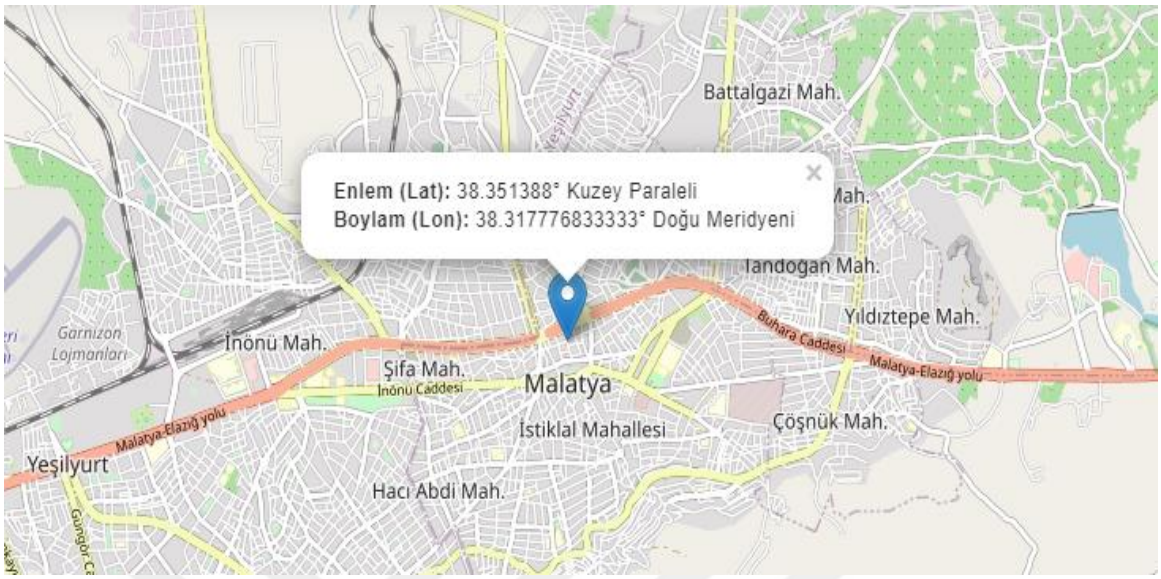
Cihaz Konumu İle İlgili Kayıtlar

Mobil cihaza yüklü uygulamalar, cihaz tarafından izin verilmesi halinde konum bilgilerini kullanmaktadır. Uygulamaların kullandığı konumlar adli bilişim analizlerinde başvurulan önemli kayıtlardır. Örneğin kamera uygulaması ile cihaz konumunu kullanarak çekilen fotoğrafların exif bilgilerinde konum bilgisine ulaşılabilmektedir. Adli kopya içerisinde konum bilgileri belli olan örnek resim dosyasına ait *exif* bilgileri Şekil 7.12'de gösterilmiştir.



Şekil 7.12. Konum bilgileri açık olan resim dosyasına ait exif bilgileri

Resim dosyasının exif bilgileri içerisinde bulunan konum bilgileri kullanılmış ve fotoğrafın çekildiği konum tespit edilerek Şekil 7.13'de gösterilmiştir.



Şekil 7.13. Resim dosyasının tespit edilen konumunun harita gösterimi [130]

Konum bilgilerinin tespit edilebilmesi için uygulamaya konum izinlerini kullanma yetkisi verilmesi gerekmektedir. Aksi halde konum bilgileri kullanılamamaktadır.

Sohbet Uygulamaları İle İlgili Kayıtlar

Mobil uygulama marketlerinde kullanıma sunulan sohbet uygulamalarının sayısı her geçen gün artmaktadır. Şirketler, kurumlar hatta suç örgütleri kendi aralarında güvenli haberleşme için ihtiyaçlarına uygun haberleşme uygulamalarını geliştirerek mensuplarının kullanımına sunmaktadır. Bu durum bazen kendi uygulamalarını özgün olarak geliştirmenin yanında var olan uygulamalarda değişiklikler yapılarak yeni uygulamalar geliştirilmektedir. Adli araçlar bu tarz uygulamalarının veri tabanlarını çözememektedir. Bu yüzden ara yüz üzerinden verilere erişilemez. Bahse konu durumların oluşma ihtimaline karşılık analizciler veri tabanlarını manuel analiz etmek zorundadır.

Play Store ve App Store gibi uygulama marketlerinin dışında farklı uygulama marketlerinde kullanıma sunulan Whatsapp Plus [131] ve Whatsapp2Plus uygulamaları gibi değiştirilmiş uygulamaların adli araçlar tarafından anlamlandırılamayacağı analizci tarafından bilinmelidir.

Yüklü Uygulama İle İlgili Kayıtlar

Mobil cihazları günlük hayatın vaz geçilmez parçası yapan en büyük etkenler farklı uygulamaları çalıştırabilmesidir. 2019 yılının ilk çeyreğinden itibaren önde gelen uygulama mağazalarında indirilebilecek uygulamaların sayısına ilişkin verilere göre Android uygulama sayısı

2.1 milyon civarındadır. Uygulama sayısındaki artış ve mobil cihaz kullanım oranları göz önüne alındığında bazı uygulamaların suçun konusunu oluşturması muhtemel bir durumdur. Öte yandan özel amaçla kullanılan bazı uygulamaları yüklemek bile suç unsuru olabilmektedir. Bu nedenle uygulama kayıtlarının mobil cihazlarda bıraktığı kalıntıları anlamlandırmak adli bilişim analizlerinde önemli bir hal almıştır. Android cihazlarda yüklü uygulamalar ile ilgili analiz yapılırken localappstate.db, Maindata.db, library.db, package_verification.db, suggestions.db, dmappmgr.db ve packages.list dosyalarının kontrol edilmesi gerekmektedir.

- **Localappstate.db**

Android dosya yapısında data/Root/data/com.android.vending/databases/localappstate.db dizini altında bulunan localappstate.db dosyası, Google Play Store üzerinden indirilmiş uygulama kayıtları ile yerel olarak yüklenmiş uygulama kayıtlarını saklar. Appstate tablosuna eklenen bir kayıt Tablo 7.2'da gösterilen uygulama paketinin adını, kurulum süresini vb. bilgileri içerir.

Tablo 7.2. localappstate.db dosyası içerindeki bazı tablo içerikleri ve açıklamaları

Tablo Adı	Değer	Açıklama
package_name	com.whatsapp	Uygulama paketinin adıdır. Paket isminin benzersiz olması gerekir.
title	Whatsapp Messenger	Uygulama Adı
first_download_ms	05.03.2018 12:48:07	İlk indirme tarihi
account	eym****04@gmail.com	Play Store Hesap adı
last_notified_version	453597	Son bildirilen sürüm
last update timestamp_ms	17.05.2020 18:22:00	Son güncelleme zamanı
install_reason	auto_update	Yükleme nedeni

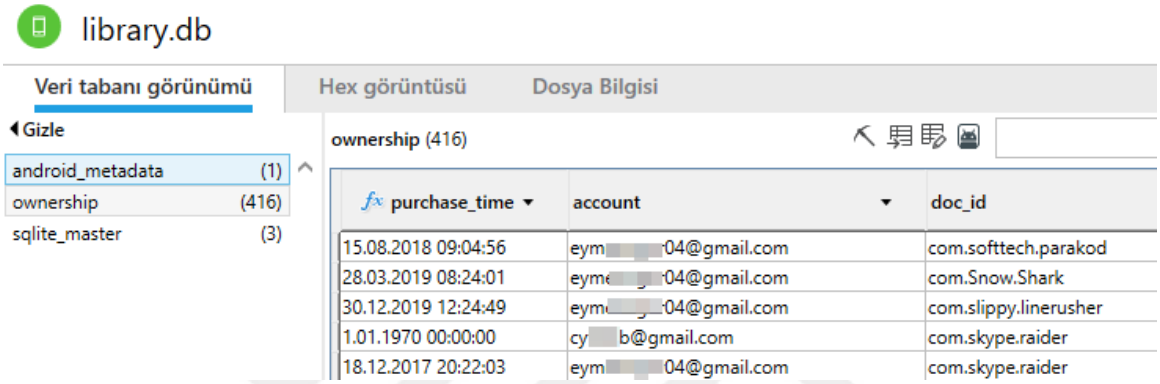
Test cihazımız içerisinde yüklü olan whatsapp uygulamasının localappstate.db dosyası içerisindeki kayıt bilgileri incelendiğinde; uygulamanın ilişkili olarak indirildiği hesap adı, haricen yüklenip yüklenmediği, benzersiz paket adı ve otomatik güncelleme alıp almadığı ile ilgili bilgilere erişilmiştir.

- **Maindata.db**

Yüklü uygulama kayıtlarının tutulduğu ana veri tabanı dosyasıdır. Localappstate.db ile benzer mantıkta çalışmaktadır. LG Android mobil cihazlar genellikle bu veri tabanını kullanmaktadır.

- **Library.db**

Android dosya yapısında data/Root/data/com.android.vending/databases/library.db dizini altında bulunan library.db dosyası, cihaz üzerinde tanımlanan Play Store hesabı ile indirilmiş uygulamalar ilgili kayıtların tutulduğu veri tabanı dosyasıdır. Play Store hesabı cihaza aktif edildiği anda aynı hesap ile daha önce indirilen uygulama kayıtlarına bu veri tabanı dosyası içerisinden ulaşmak mümkündür. Library.db dosyasının içerisindeki kayıtlar Şekil 7.14'de gösterilmiştir.



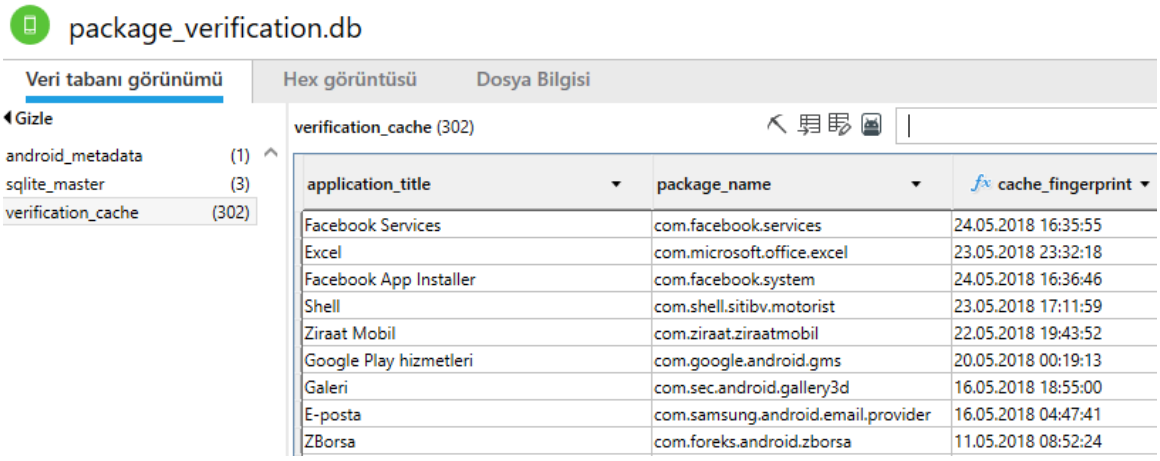
Şekil 7.14. library.db dosyası içerisinde tutulan bazı kayıtlar

Library.db dosyası içerindeki kayıtlar incelendiğinde; cihaz üzerinde kaç adet play store hesabı bulunuyorsa, bu hesaplar (account) ile birlikte indirilen uygulamalara ait benzersiz paket adı (doc_id) ve satın alma tarihi (purchase_time) gibi kayıtların tutulduğu görülmüştür.

Library.db dosyası içerisinde tespit edilen uygulama kayıtlarına bakılarak ilgili uygulamanın mobil cihazda indirildiği sonucu çıkarılmamalıdır. Ancak uygulamanın Play Store hesabı (account) kullanılarak herhangi bir cihaza indirildiği sonucu çıkarılabilir.

- **Package_verification.db**

Android dosya yapısında data/Root/data/com.android.vending/ databases/ dizini altında bulunan package_verification.db dosyası cihaza yerel olarak kurulmuş ve kaldırılmış uygulamaların doğrulama ve güncelleme kayıtlarının tutulduğu dosyadır. Cihaz ayarlarından "Uygulamaları Doğrula" seçeneği etkinse bu veri tabanı görünür. package_verification.db veri tabanı içerisindeki kayıtlar Şekil 7.15'de gösterilmiştir.



Şekil 7.15. package_verification.db dosyası içerisinde tutulan bazı kayıtlar

Veri tabanı içerisindeki kayıtlar incelendiğinde; doğrulaması yapılan uygulamanın isim bilgisi (application_cache), paket adı (package_name) ve doğrulama tarihi (cache_fingerprint) gibi bilgiler tespit edilmiştir.

- **Suggestions.db**

Android dosya yapısında data/Root/data/com.android.vending/databases/suggestions.db dizininde bulunan suggestions.db dosyası Google Play Store arama çubuğunu kullanarak yapılan tüm anahtar kelimelerin arama kayıtlarını içerir. Test cihazımıza ait suggestions.db veri tabanı içerisindeki kayıtlar Şekil 7.16'da gösterilmiştir.

Şekil 7.16. suggestions.db dosyası içerisinde tutulan bazı kayıtlar

Veri tabanı içerisinde; yapılan kelime aramaları (query) kayıtları ve aramanın yapıldığı tarih (date) kayıtları ile ilgili bilgiler bulunmaktadır.

library.db ve suggestions.db dosyalarındaki kayıtların Google Play Store hesabı ile senkronize olduğu analiz aşamasında mutlaka göz önünde bulundurulmalıdır. Yani aynı Google Play Store hesabını kullanan iki cihazdan herhangi birisine bir uygulama kurulduğunda ya da aratıldığında, diğer cihazlarda da kurulan ya da aratılan uygulamanın kaydının bulunacağının bilinmesi önemlidir.

- **Packages.list**

Android dosya yapısında data/Root/system/packages.list dizininde bulunan packages.list dosyası Android cihazda kayıtlı kullanıcı grup kimlik bilgileri ile paket bilgilerinin tutulmaktadır. Android kullanıcılara 1000-9999, arasında kimlik bilgileri atar. Android tek bir kullanıcı için tasarlanmıştır, ancak önceden yüklenmiş sistem uygulamasını, kullanıcı tarafından yüklenmiş her Java uygulamasını da kullanıcı olarak kabul eder. UID aralığı 10000-19999 bu uygulamalar için ayrılmıştır. İlk önyüklemede (önceden yüklenmiş uygulamalar için) veya yeni bir uygulama yüklerken, statik olan benzersiz bir UID / GID atanır. Bu uygulama, UID eşlemesine karşı uygulamada bir kabuk sağlıyorsa veya yerel ikili dosyalar çalıştırabiliyorsa dosyada /data/system/packages.list içerisinde görülebilir [132]. Bazı Android grup yetkileri Tablo 7.3'de gösterilmiştir.

Tablo 7.3. Android cihazlarda çalışan bazı hizmet türleri ve grup yetkileri [133]

SERVİS	**AÇIKLAMA**	**GRUPLAR**
Netd	Ağ ara yüzlerini yapılandırmak, PPP arka plan programı (pppd) çalıştırmak, internet paylaşımı ve diğer benzer görevleri yapmak için Ağ yönetim hizmetleri tarafından kullanılan Android 2.2 ve sonraki sürümlerinde sunulur.	UID: 0 / Root GID:0 / Root
Mediaserver	Audio flinger, Media Player, Kamera Hizmeti gibi medya hizmetlerini başlatmaktan sorumludur.	UID:1013 / Media GID:1005 / Audio Groups: 1006 / Camera 1026 / drmpc 3001 / net_bt_admin 3002 / net_bt 3003 / net_bw_acct
d-bus daemon	D- Veri yoluna özgü IPC / mesaj geçişini yönetir (Android 'e özgü olmayan bileşenlere öncelikli olarak)	UDI:1002 / Bluetooth GID:1002 / Bluetooth Groups:3001 / net_bt_admin

Tablo 7.3 Android cihazlarda çalışan bazı hizmet türleri ve grup yetkileri (devam)

SERVİS	AÇIKLAMA	GRUPLAR
installd	Uygulama paketlerinde (APK) dalvik sanal makinasının (DEX) bayt kodunun ilk optimizasyonu dahil olmak üzere uygulama paketlerinin cihazlara kurulumunu yönetir.	UID:1012 /install GID:1012 / install On pre -4.2 devices: UID:0 / root GID:0 / root
Keystore	Anahtar değer çiftlerinin sistemde güvenli bir şekilde saklanmasından sorumludur (kullanıcı tanımlı bir parola ile korunur).	UID:1017 / keystore GID:1017 / keystore Groups: 1026 / drmpc
drmserver	Dijital hak yönetimi (DRM) için alt düzey işlemler sağlar.	UID:1019 / drm GID:1019 / drm Groups:1026 / drm-rpc 3003 / inet
Servicemanager	Binder IPC uç noktaları ile uygulama hizmetlerinin kaydedilmesi ya da kayıttan çıkarılması için hakemlik yapar.	UID:1000 / system GID:1000 / system
Surface filinger	Android 4.01'de görüntülenecek grafik çerçevesini grafik kartı sürücüsüne göndermekten sorumludur.	UID:1000 / system GID:1000 / system

Pek çok Android cihazda çalışan hizmet türleri ve Kullanıcı Kimliğini (UID), ana Grup Kimliğini (GID) ile ilgili basit bir liste Tablo 7.3'de gösterilmiştir. Uygulamalara ait paketler ve grup izinleri packages.list analizi ile elde edilebilir.

Modifiye Edilmiş Özel Amaçlar İçin Geliştirilmiş Uygulama Kayıtları

Uygulamaların adli bilişim analizi karmaşık bir süreçtir. Analiz aşamalarında özellikle kontrol edilmesi gereken veri tabanları ve sistem dosyaları yukarıda özetlenmiştir. Ancak tüm bunların dışında dikkat edilmesi gereken bir diğer husus ise manipüle edilmiş ve özel amaçlar için geliştirilmiş uygulamaların tespiti ve analizidir.

Bu tarz uygulamalar benzersiz bir paket adına sahip olabileceği gibi, daha önce herhangi bir uygulama tarafından kullanılan paket adı, ara yüz ve ikon vb. özelliklerinin taklit edilerek kullanılmasıdır. Özel bir amaç için geliştirilen sohbet uygulamasının deşifre olmasını engellemek ve tespitini imkânsız kılmak için whatsapp gibi bilinen bir uygulamanın com.whatsapp paket adını ve uygulama simgesini kullanması örnek gösterilebilir. Bu tarz durumlarda cihazda paket adı kopyalanan Whatsapp uygulaması kurulu ise, değiştirilmiş uygulamanın orijinal uygulama ile çakışacağından çalışması beklenmez. Ancak orijinal uygulama kurulu değilse, değiştirilmiş uygulama cihaz üzerinde sorunsuzca çalışabilir.

Değiştirilmiş uygulamalar ile iki türlü karşılaşmak mümkündür.

1. Durum: modifiye edilmiş uygulama, orijinal uygulamanın adını, simgesini ve paket adını kullanır.
2. Durum: modifiye edilmiş uygulama, orijinal uygulamanın adını ve simgesini kullanır.

1. Durumda yapılması gereken:

localappstate.db dosyası kontrol edilerek uygulamaların paket adı ve uygulama adı eşleştirilir. Eğer paket adı uygulama adı ile eşleşmiyorsa uygulama modifiye edilmiş şüpheli bir uygulama olarak değerlendirilir.

Paket adı ile uygulama adı uyuşan ve uyuşmayan durum ile ilgili örnek Tablo 7.4'de verilmiştir.

Tablo 7.4. Paket adı ve uygulama adı uyuşan ve uyuşmayan uygulama örnekleri

S.N	**package_name (Paket Adı)**	**Title (Uygulama Adı)**	**Durumu**
1	com.whatsapp	Whatsapp Messenger	Doğru
2	com.crymobil	Whatsapp Messenger	Yanlış

Tablo 7.4'de belirtilen 1 numaralı örnek 1.durum için kabul edilebilir bir eşleşmedir. Ancak 2 numaralı sırada belirtilen örnekte paket adı ile uygulama adının uyuşmadığından bu uygulamanın modifiye edilmiş bir uygulama olduğu anlaşılmaktadır. Tespit aşamasından sonra bu uygulamanın çalışma prensipleri veri, tabanları kullanım amacı gibi özellikleri tespit edilerek raporlanır.

2.Durumda yapılması gereken:

Bu durum 1. durumdan daha karmaşık ve tespiti zordur bir süreçtir.. Çünkü sadece uygulama adı ve paket adının teyit edilmesi o uygulamanın orijinal bir uygulama olduğu sonucuna ulaşmak için yetersizdir. Bu durumda Tablo 7.4'de 1 numaralı sırada belirtilen örnekteki gibi whatsapp uygulaması ile aynı ad ve paket adını kullanan modifiye edilmiş bir uygulamanın tespiti için aşağıdaki adımlar uygulanır.

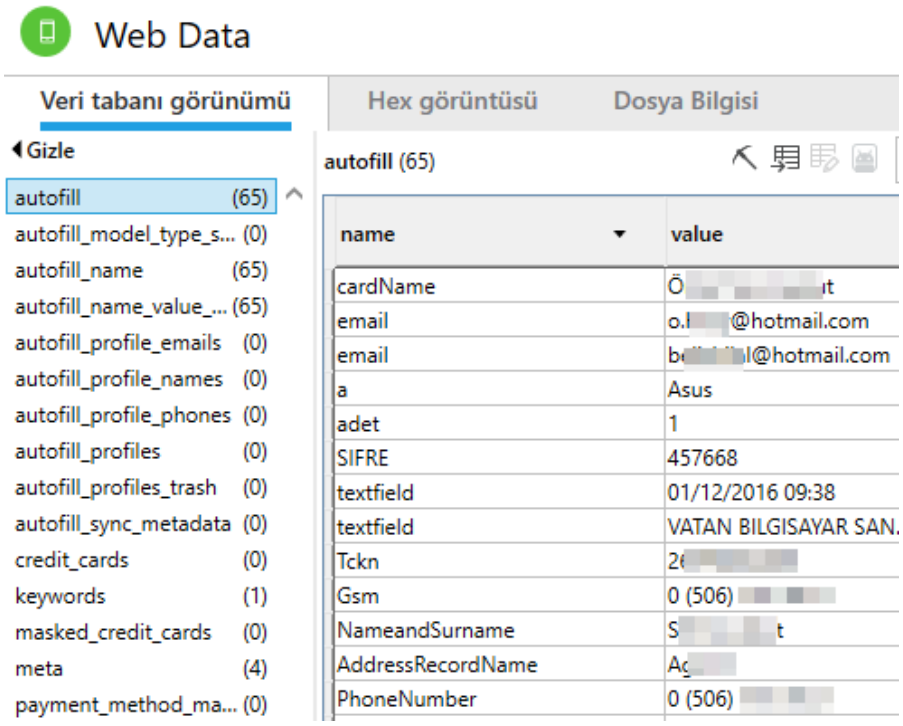
1. Whatsapp uygulamasının mevcut veri tabanları kontrol edilir. Eğer Whatsapp uygulamasının veri tabaları içerisinde; örneğin uygulamanın kullanım amacı dışında silinen uygulama kayıtlarının bulunması bu uygulamanın manipüle edilmiş uygulama olduğunu göstermektedir.
2. Tespit edilen şüpheli uygulamaya ait APK dosyası sanal makinede canlandırılarak kontrol edilir.
3. Android Stüdyo vb. uygulamalar ile APK dosyası analiz edilerek uygulama davranışları analiz edilir.

4. Modifiye edilmiş uygulamalar uygulama marketlerinden indirilmediği için haricen yüklenme durumu göz önüne alınarak adli kopya içerisinde bluetooth, download ve sd kart dizinlerinin altında kalıntılar aranmalıdır.
5. Bluetooth üzerinden alınan ya da gönderilen verilerin kayıtlarının tutulduğu btopp.db, hafıza kartındaki verilerin kayıtlarının tutulduğu external.db ve indirilen dosyaların kayıtlarının tutulduğu downloads.db gibi veri tabanı dosyaları kontrol edilmelidir.

Kullanıcı Sözlüğü ve Otomatik Doldurma Kayıtları

Kullanıcı sözlüğü mobil cihazlarda sıklıkla kullanılan kelime giriş kayıtlarıdır. Çoğunlukla uygulamalar üzerinde klavye girişlerini hızlı tamamlamak için uygulamalar tarafından kayıt edilen kelimeleri içermektedir. Adli kopya içerisinde çoğunlukla bağlantısız kelimeler şeklinde sıralanan bu kayıtlar cihaz içerisindeki şifreli belgelerin şifre çözme aşamasında yapılacak sözlük saldırısı için kullanılabilmektedir.

Mobil cihaz kullanıcıları yüklü uygulamaların bazı kullanıcı bilgilerini hatırlamasına izin verdiği durumlarda, bu bilgiler uygulamalar tarafından gerektiğinde kullanılmak üzere saklanmaktadır. Bu otomatik doldurma kayıtları cihaz kullanıcısı ile ilgili önemli bilgileri içermektedir. Bu bilgiler soruşturmanın konusuna göre kanıt elde edilecek alanlardır. Test cihazımızdan elde edilen Android Browser uygulamasına ait Web Data veri tabanı içerinde bulunan otomatik doldurma kayıtları Şekil 7.17'de gösterilmiştir.



Şekil 7.17. Web Data içerisinde elde edilen otomatik doldurma kayıtları

Web Data veri tabanı içerisindeki kayıtlar incelendiğinde otomatik doldurulan bilgi (name) ve doldurulan değer (value) içerisinde telefon numarası, şifre, kimlik numarası ve email gibi kişisel bilgilere ait kayıtlar bulunmaktadır.

Farklı Adli Kopya Türleri İçerisindeki Verilerin Karşılaştırılması

Adli bilişim analizlerinde tercih edilen yöntem cihazın tüm hafızasının kopyası alınarak işlemlerin yürütülmesi olsa da bu durum her zaman mümkün olmadığından cihaz hafızasının bir kısmının ya da belirli uygulama verilerinin alındığı mantıksal kopya alma yöntemleri de uygulanmaktadır. Test cihazımızın belirtildiği şekilde mantıksal ve fiziksel kopyaları alınmıştır. Mantıksal ve fiziksel adli kopya içerisindeki veri içerikleri karşılaştırıldığında fiziksel kopya içerisindeki verilerin mantıksal adli kopya içerisindeki verilerden daha fazla veri getirdiği anlaşılmıştır. Ayrıca mantıksal kopya içerisinde kurtarılmış veri bulunmazken, fiziksel kopya içerisinde kurtarılan veri sayısı parantez içerisinde belirtilmiştir. Fiziksel ve mantıksal kopyaların içerisindeki verilerin karşılaştırılması Tablo 7.5'de gösterilmiştir.

Tablo 7.5. Farklı adli kopya formatları içerisinden elde edilen verilerin karşılaştırması

MANTIKSAL AYIKLAMA		**FİZİKSEL AYIKLAMA**	
Arama Günlüğü	2000 (0)	Arama Günlüğü	2797 (15)
Cihaz Konumları	979 (0)	Aranan Öğeler	4564 (0)
Kişi Listesi	571 (0)	Kişi Listesi	10651 (37)
MMS Mesajları	3 (0)	MMS Mesajları	7 (0)
SMS Mesajları	4063 (0)	SMS Mesajları	9630 (1036)
Takvim Maddeleri	39 (36)	Takvim Maddeleri	19 (18)
Arşivler	22 (0)	Arşivler	237 (131)
Belgeler	93 (0)	Belgeler	414 (18)
Kategorize Edilmemiş	2527 (0)	Kategorize Edilmemiş	135819 (95915)
Metin	993 (0)	Metin	15296 (11127)
Resimler	10287 (0)	Resimler	143492 (11959)
Ses	439 (0)	Ses	568 (118)
Veri tabanları	122 (0)	Veri tabanları	973 (24)
Videolar	423 (0)	Videolar	1156 (331)
-	-	Baz İstasyonları	3574 (0)
-	-	Cihaz Konumları	6115 (60)
-	-	Cihaz Kullanıcıları	1 (0)
-	-	Cihaz Olayları	9 (4)
-	-	Çerezler	2364 (13)

Tablo 7.5. Farklı adli kopya formatları içerisinde elde edilen verilerin karşılaştırması (Devamı)

MANTIKSAL AYIKLAMA		FİZİKSEL AYIKLAMA	
-	-	Downloads	177 (0)
-	-	E-postalar	413 (5)
-	-	Kablosuz Ağlar	1262 (0)
-	-	Kullanıcı Hesapları	42 (0)
-	-	Otomatik doldurma	66 (0)
-	-	Parolalar	815 (2)
-	-	Sohbetler	1518 (76)
-	-	Web Geçmişi	12328 (2)
-	-	Yüklü Uygulamalar	669 (0)
-	-	Uygulamalar	3999 (1165)
-	-	Yapılandırmalar	56 (1)

7.4. Raporlama Aşaması

Raporlama aşaması elde edilen dijital kanıtların en az iki adli araçla teyit edildiği ve sonrasında adli makamlar için açık bir dille ifade edildiği süreci içerir. Bu süreç içerisinde elde edilen cihaza ait IMEI, Seri No, marka ve model gibi temel ayırt edici özelliklerin yanında cihazın aidiyet bilgisine Tablo 7.6'da gösterildiği gibi yer verilmelidir.

Tablo 7.6. Analiz edilen cihaza ait raporda belirtilecek temel bilgiler

Aidiyet Bilgisi	Adı -SOYADI (TC:11111111111) (ÖRNEKTİR)
Marka	Samsung
Model	SM-J530F
Seri Numarası/IMEI	3598********879 (ÖRNEKTİR)
Adli kopya formatı	Fiziksel
Kullanılan yazılım/Donanım	Adli araç -versiyon-kullanım amacı (A****-V2.1-Adli Kopya) (ÖRNEKTİR)
Adli koya veri bütünlük değeri (SHA1/MD5)	9A355E0A85FD9EA1DA81885D4A2BD8E6E312867C

Daha sonraki süreçlerde olabilecek itirazlar ve doğruluk teyitleri için elde edilen kanıtın isim bilgisi, oluşturma-değiştirme-silme tarihleri, niteliği, kaynak yolu ve veri bütünlük değerleri gibi bilgilerin belirtilmesi gerekmektedir. Bunların yanında adli kopya türü ile kullanılan yazılım ve

donanımların versiyon bilgilerinin de raporda belirtilmesi önemlidir. Tespit edilen dijital kanıt ile ilgili raporda belirtilmesi gereken öznitelik bilgileri Tablo 7.7'de gösterilmiştir.

Tablo 7.7. Tespit edilen kanıt ile ilgili raporda belirtilmesi gereken öz nitelik bilgileri

Adı	IMG_4230
Dosya Türü	jpg
Oluşturma Tarihi	29 .04. 2020 - 23:44:41
Değiştirme Tarihi	30 .04 2020 - 00:17:43
Silme Tarihi (Varsa)	-
Kaynak yolu	Root/data/media/0/storage/whatsapp/media/image/ IMG_4230
Kanıt veri bütünlük değeri (SHA1/MD5)	757D2B5DC40914E46303820480C347A30369249F

Raporda cihaz ve dijital kanıt bilgileri dışında inceleme talep eden makam ve izin bilgilerinin de mutlaka belirtilmesi, süreçlerin kontrolü için gereklidir.

Rapor yazılırken kullanılan dilin yalın ve anlaşılır olması gerekmektedir. Kullanılan teknik terimlerin açıklamalarına yer verilmeli ve sonuçlar açık ve net bir şekilde bağlanmalıdır.

Bulgular ve Tartışma

Android işletim sistemine sahip mobil cihaz üzerinde mobil adli bilişim uygulaması yapılmıştır. Yapılan uygulama, önerilen derin öğrenme yaklaşımına dayalı desen tespit yöntemi ve mobil cihaz süreç metodolojisine uygun olarak gerçekleştirilmiştir.

El koyma aşmasında önerilen metodolojiye uygun olarak test cihazımızın ekran izleri alınarak elde etme aşamasına geçilmiştir. Ancak 3 farklı adli araçla mevcut yöntemler kullanılarak adli kopya almak mümkün olmamıştır. Önerilen mobil cihaz metodolojisinde belirtilen temel donanım benzerliklerinden faydalanılarak adli kopya alınması yöntemi uygulanmış ve test cihazımızın fiziki kopyası başarılı bir şekilde alınmıştır.

Bir sonraki aşamada önerilen desen tanıma yöntemi ile cihaz üzerindeki desen tespit edilerek cihaz kilidi açılmış ve test cihazımızın mantıksal kopyası başarılı bir şekilde alınmıştır. Her iki durumda da önerilen yöntemlerin başarılı sonuçlar verdiği gösterilmiştir.

Cihazımızın mantıksal ve fiziksel kopyaları içerisindeki veriler karşılaştırılmıştır. Buna göre yüklü uygulamaların ve sohbet içeriklerinin konu olduğu soruşturmada mantıksal kopya ile analiz yapılmasının doğru olmadığı, nihai sonuç için mutlaka fiziksel kopya alınması gerektiği sonucu çıkarılmıştır. Ayrıca test cihazımızın adli analizi sonrasında, uygulamaya yönelik birçok öneri sunulmuştur.

8. SONUÇLAR

Bu tez çalışmasında, derin öğrenme yöntemleri kullanılarak mobil cihaz ekran izlerinden desen kilidi tespiti için akıllı bir yöntem geliştirilmiştir. Tespit edilen yöntem mobil cihaz analiz süreçlerine entegre edilerek eski süreçlerle bağlantılı yeni bir süreç tanımlama modeli önerilmiştir. Son aşamada önerilen desen kilidi tespit yöntemi ve mobil cihaz süreçlerine eklenen öneriler test için kullanılan mobil cihaza uygulanmıştır. Adli kopya alma ve analiz işlemleri sonucunda mobil cihazların adli bilişim analizlerinde karşılaşılan zorluklara uygun çözüm önerileri sunulmuştur.

- Dünyanın önde gelen mobil cihaz üreticilerini, Google ve özgür yazılım topluluğunu arkasına alarak en çok kullanılan işletim sistemi olma özelliğini elinde barındıran Android işletim sistemi her geçen gün pazar payını büyütmeye devam etmektedir. Bunun bir sonucu olarak dijital delil kaynağı olarak adli bilişim analizlerinde çok sık karşılaşılmaktadır. Bu nedenle geliştirilen desen kilidi tespit etme yöntemi, mobil cihaz süreç tanımlama modeli ve örnek adli bilişim analizleri Android işletim sistemine sahip mobil cihazlar için geliştirmiş ve uygulanmıştır. Ancak önerilen yöntemler ve analiz önerileri desen kilidi kullanan başka işletim sistemine sahip mobil cihazlar için de uygulanabilmektedir.
- Dokunmatik ekran güvenlik kimlik doğrulama yöntemleri, mobil cihazlar için en çok tercih edilen kimlik doğrulama ve bilgi güvenliği yöntemleridir. Mobil cihazların adli kopyasının alınması için çoğu durumda, ekran kilidinin açılması gerekir. Bu nedenle ekran kilitlerini otomatik olarak çözmek için yeni bir akıllı model sunulmuştur. Yapılacak çalışmada kullanılmak üzere 20 farklı desen kilidine ait 2000 fotoğraflık veri seti oluşturulmuştur.
- Yapılan çalışmalarda derin öğrenme teknikleri özellik mühendisliği açısından değerlendirilmiş ve yüksek doğruluk oranına sahip bir ekran örüntüsü tanıma ve sınıflandırma yöntemi sunulmuştur. Makine öğreniminin en önemli aşamasından biri özellik çıkarma için eğitilmiş ağlar olan SqueezeNet ve MobileNetV2 birlikte kullanılmıştır. İkinci aşamada en uygun özellik seçim sürecini bulmak için mRMR kullanılarak otomatik bir özellik seçici sunulmuş ve TmRMR olarak adlandırılmıştır. Önerilen tümleşik derin özelliklerin ve TmRMR tabanlı yöntemin son aşamasında basit ve doğrusal bir sınıflandırıcı olan LDA ile

sınıflandırma yapılmıştır. Sınıflandırma sonucunda yöntemin başarısı doğruluk (acc), F1 skoru ($F1$) ve geometrik ortalama(gm) performans metrikleri ile ölçüldüğünde acc, gm ve $F1$skorlarıyla %99,75 sınıflandırma başarısına ulaşılmıştır.

- Ekran izlerinden desen kilidi tespit yönteminin ana kaynağı cihaz üzerindeki ekran izlerinin fotoğraflarıdır. Bu fotoğrafların adli bilişim süreçlerinin el koyma aşamasında alınması gerekmektedir. Bu nedenle el koyma aşaması süreç modeline mobil cihazların ekran izlerinin görüntüsünün alınması entegre edilmiştir. Alınan ekran izleri adli bilişim süreçlerinden elde etme aşamasında ekran kilidi ile korunan mobil cihazların adli kopyasının alınmasına imkân tanımıştır. Devam eden süreçte aynı izlerin cihaz içerisindeki şifreli belgelerin şifrelerini çözmek için kullanılabileceği değerlendirilmiştir. Bahse konu hedeflerin gerçekleşmesi için desen kilidi tespit yöntemi mobil cihaz adli bilişim süreçlerine entegre edilmiştir.
- Örnek adli bilişim analizi bölümü içerisinde mobil cihaz adli bilişim süreçleri sırasıyla takip edilmiştir. İlk olarak test cihazının önerilen yönteme uygun şekilde ekran izlerinin görüntüleri alınarak elde etme sürecine geçilmiştir. Elde etme sürecinde ekran kilidi olan test cihazımızın üç farklı adli araç ile kopyasının alınması ve kilidin kırılması mümkün olmamıştır. Bu aşamadan sonra mobil adli bilişim sürecine eklediğimiz aynı donanıma sahip farklı cihaz modelleri üzerinden adli kopya alma yöntemimiz kullanılarak cihazımızın fiziksel adli kopyası alınmıştır. İkinci olarak desen kilidi tespit yöntemimiz başarılı şekilde uygulanarak desen kilidi tespit edilmiş ve test cihazımızın mantıksal çıkarımı yapılmıştır. Böylece önerilen yöntemlerin gerçek kanıtlar üzerindeki başarısı test edilmiştir.
- Test cihazımızın adli kopyası içerisindeki, SMS, çağrı, uygulama, vb. temel verilerin analizi yapılarak manipüle edilmiş verilerin tespiti ile ilgili analiz yöntemlerine değinilmiştir. Yapılan örnek analiz, veri tabanları üzerinden yapılarak adli araçlara bağımlı olmadan bu verilerin değerlendirilmesi hedeflenmiştir. Mantıksal ve fiziksel adli kopyalar içerisindeki veriler karşılaştırıldığında fiziksel çıkarımın mantıksal çıkarımdan çok daha fazla veri getirdiği tespit edilmiş ve karşılaştırma tablosunda sunulmuştur.

ÖNERİLER

Desen kilidi tespit yönteminin ilk basamağı olan ekran izi fotoğrafının alınması, süreçlere entegre edilerek her davaya uygulandığı taktirde, sonraki çalışmalarda kullanılabilecek büyük bir veri setinin oluşmasına imkân tanıyacaktır. Bu şekilde elde edilen veri seti gelecek yıllarda yapılacak birçok çalışmaya önemli bir kaynak oluşturacaktır. Bu nedenle kolluk kuvvetleri ve uygulayıcıların bu yöntemin uygulama aşamalarını mobil adli bilişim süreçlerine dahil etmeleri durmuş olan analiz süreçlerinin kaldığı yerden devam etmesi için bir şans verecektir.

Tez çalışmamızın içerisindeki adli kopya alma ve analiz aşamaları ile ilgili öneriler saha çalışmalarında birçok kez uygulanarak test edilmiştir. Özellikle elde etme aşamasında kanıt olan mobil cihaz ile aynı temel donanım özelliklerini kullanan diğer cihaz modelleri üzerinden adli kopya alınması adli bilişim uzmanları ve uygulayıcılarına büyük fayda sağlayacağı değerlendirilmiştir.

Veri tabanları üzerinden analiz işlemlerinin yürütülmesi, analiz aşamasının adli araçlardan kaynaklanan hatalardan en az etkilenilmesini sağlayacaktır. Ayrıca bölüm 7'de belirtilen manipüle edilmiş uygulama tespit yöntemi de gizlenen kanıtların tespit sürecine katkı sağlayacaktır.

Analiz talep edilen konu ile ilgili verilerin adli kopya içerisindeki varlığı teyit edilmeden analiz aşamasına geçilmememledir. Bölüm 7 içerisinde adli kopya formatları içerisindeki veri miktarlarının karşılaştırılması gösterilmiştir. Bu karşılaştırma tablosuna göre mantıksal kopya içerisinde, cihaz içeriğine ait bütün verilerin olmadığı anlaşılmıştır. Bu durum göz önüne alınarak sadece mantıksal kopya üzerinden analizi sonuçlandırmak doğru bir yaklaşım değildir.

KAYNAKLAR

[1] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years, *Digital Investigation*, C. 7, Sayı SUPPL. doi:10.1016/j.diin.2010.05.009

[2] Casey, E. (2010). *Handbook of Digital Forensics and Investigation*, *Handbook of Digital Forensics and Investigation*. doi:10.1016/C2009-0-01683-3

[3] Jones, R. (2003). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, *International Journal of Law and Information Technology*, C. 11, Sayı 1, 98–100. doi:10.1093/ijlit/11.1.98-a

[4] Digital 2019: Global Internet Use Accelerates - We Are Social. [https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates, erişim 17-5-2020

[5] Alendal, G.; Dyrkolbotn, G. O.; Axelsson, S. (2018). Forensics acquisition — Analysis and circumvention of samsung secure boot enforced common criteria mode, *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, S60–S67. doi:10.1016/j.diin.2018.01.008

[6] Barmpatsalou, K.; Damopoulos, D.; Kambourakis, G.; Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics, *Digital Investigation*, 323–349. doi:10.1016/j.diin.2013.10.003

[7] Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics, *Digital Investigation*, C. 28, 163–175. doi:10.1016/j.diin.2019.01.009

[8] Guttman, B.; Lyle, J. R.; Ayers, R. (2014). Ten years of computer forensic tool testing, *Digital Evidence and Electronic Signature Law Review*, C. 8, Sayı 0. doi:10.14296/deeslr.v8i0.1963

[9] Casey, E. (2017). Editorial - A smörgåsbord of digital evidence, *Digital Investigation*, 1–2. doi:10.1016/j.diin.2017.11.003

[10] Mellars, B. (2004). Forensic examination of mobile phones, *Digital Investigation*, C. 1, Sayı 4, 266–272. doi:10.1016/j.diin.2004.11.007

[11] Jansen, W.; Ayers, R. (2007). Guidelines on Cell Phone Forensics Recommendations of the National Institute of Standards and Technology, *Nist Special Publication*, C. 800, Sayı 101, 1–104. doi:10.6028/NIST.SP.800-124

[12] Yates, M. (2010). Practical investigations of digital forensics tools for mobile devices, *Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10*, 156–162. doi:10.1145/1940941.1940972

[13] Grispos, G.; Storer, T.; Glisson, W. B. (2011). A comparison of forensic evidence recovery techniques for a windows mobile smart phone, *Digital Investigation*, C. 8, Sayı 1, 23–36. doi:10.1016/j.diin.2011.05.016

[14] Murphy, C. A. (2012). Developing Process for Mobile Device Forensics, 1–9

[15] Gözde, K.; Akhan, A.; Abdül Halim, Z. (2016). Istanbul Commerce University Journal of Science, C. 15, Sayı 30, 55–75

[16] UŞKAL mesut. (2015). *Mobile Cihazlarda Adli Bilişim*İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü

[17] Rick, A.; Jansen, W.; Sam, B. (2013). Guidelines on Mobile Device Forensics, *NIST Special Publication 800-101*. doi:10.6028/NIST.SP.800-124

[18] Naraei, P.; Amiri, I. S.; Saberi, I. (2014). Design and Implementation for Mobile Devices, *Optimizing IEEE 802.11i Resource and Security Essentials*, 29–46. doi:10.1016/b978-0-12-802222-1.00004-3

[19] Conrad, E.; Misenar, S.; Feldman, J. (2016). Domain 4: Communication and Network Security (Designing and Protecting Network Security), *CISSP Study Guide*, 219–291. doi:10.1016/b978-0-12-802437-9.00005-9

[20] DİLEK, Ö. (2019). Akıllı Telefon Kullanım Tercihlerini Etkileyen Faktörler: Recep Tayyip Erdoğan Üniversitesi Öğrencileri Üzerine Bir Çalışma, *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, C. 33, Sayı 1, 203–218

[21] Fatma, Ç.; Neslihan, D. (2014). Üniversite Öğrencilerinin Akıllı Telefon Satın Alma Tercihlerini Belirlemeye Yönelik Bir Araştırma, *Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi*, C. 29, Sayı 1, 213–243

[22] Al Mutawa, N.; Baggili, I.; Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices, *Proceedings of the Digital Forensic Research Conference, DFRWS 2012 USA*, S24–S33. doi:10.1016/j.diin.2012.05.007

[23] Kuyucu, M. (2018). Gençlerde Akıllı Telefon Kullanımı ve Akıllı Telefon Bağımlılığı Sorunsalı: "Akıllı Telefon (kolik) Üniversite Gençliği"., *Global Media Journal TR Edition*

[24] Rico, D. F.; Sayani, H. H.; Field, R. F. (2008). History of Computers, Electronic Commerce and Agile Methods, *Advances in Computers*, C. 73, 1–55. doi:10.1016/S0065-2458(08)00401-4

[25] Sanchez, M. I.; De La Oliva, A.; Bernardos, C. J. (2016). Experimental analysis of connectivity management in mobile operating systems, *Computer Networks*, C. 94, 41–61. doi:10.1016/j.comnet.2015.11.021

[26] Glisson, W. B.; Storer, T.; Buchanan-Wollaston, J. (2013). An empirical comparison of data recovered from mobile forensic toolkits, *Digital Investigation*, C. 10, Sayı 1, 44–55. doi:10.1016/j.diin.2013.03.004

[27] Husain, M. I.; Baggili, I.; Sridhar, R. (2011). A simple cost-effective framework for iPhone forensic analysis, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. doi:10.1007/978-3-642-19513-6_3

[28] Oladotun, O.; Oladiran Tayo, A.; Ganiyu, R. A.; Oyeleye, C. A. (2014). Mobile Operating Systems and Application Development Platforms: A Survey, *Int. J*, C. 2201, 2195–2201

[29] Palm OS | işletim sistemi | Britannica. https://www.britannica.com/technology/Palm-OS, erişim 18-5-2020

[30] Casey, E.; Cheval, A.; Lee, J. Y.; Oxley, D.; Song, Y. J. (2011). Forensic acquisition and analysis of palm webOS on mobile devices, *Digital Investigation*, C. 8, Sayı 1, 37–47. doi:10.1016/j.diin.2011.04.003

[31] Windows Mobile - Vikipedi. https://tr.wikipedia.org/wiki/Windows_Mobile, erişim 18-5-2020

[32] Canlar, E. S.; Conti, M.; Crispo, B.; Di Pietro, R. (2013). Windows mobile live SD forensics, *Journal of Network and Computer Applications*. doi:10.1016/j.jnca.2012.12.024

[33] Pooters, I. (2010). Full user data acquisition from Symbian smart phones, *Digital Investigation*. doi:10.1016/j.diin.2010.01.001

[34] Lohrum, M. (2012). Forensic extractions of data from the Nokia N900, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering* (C. 88 LNICST), 89–103. doi:10.1007/978-3-642-35515-8_8

[35] MeeGo İşletim Sistemi: Bilmeniz Gereken Her Şey. https://cellularnews.com/mobile-operating-systems/meego-operating-system-everything-you-have-to-know/, erişim 17-5-2020

[36] LiMo İşletim Sistemi - tanım - GSMArena.com. https://www.gsmarena.com/glossary.php3?term=limo-os, erişim 17-5-2020

[37] Tizen OS: Başlangıç Kılavuzu. https://cellularnews.com/mobile-operating-systems/tizen-os-a-beginners-guide/, erişim 17-5-2020

[38] Sailfish OS: Bilmeniz Gereken Her Şey. https://cellularnews.com/mobile-operating-systems/sailfish-os-everything-you-have-to-know/, erişim 17-5-2020

[39] *Mozilla ve Ortakları İlk Firefox OS Akıllı Telefonlarını Piyasaya Sürmeye Hazırlanıyor! - Mozilla Blogu*. https://blog.mozilla.org/blog/2013/07/01/mozilla-and-partners-prepare-to-launch-first-firefox-os-smartphones/

[40] Samsung BADA Mobile OS - Mobisoft Infotech dosyasına genel bakış. https://mobisoftinfotech.com/resources/blog/other-smart-phone-operating-systems/overview-of-samsung-bada-mobile-os/, erişim 18-5-2020

[41] Android Geliştirme için Kurulum | Android Açık Kaynak Projesi. https://source.android.com/setup/, erişim 18-5-2020

[42] IDC - Akıllı Telefon Pazar Payı - İşletim Sistemi. https://www.idc.com/promo/smartphone-market-share/, erişim 18-5-2020

[43] Vidas, T.; Zhang, C.; Christin, N. (2011). Toward a general collection methodology for

Android devices, *Digital Investigation* (C. 8). doi:10.1016/j.diin.2011.05.003

[44] Android - Mimari - Öğreticiler. https://www.tutorialspoint.com/android/android_architecture.htm, erişim 18-5-2020

[45] Distefano, A.; Me, G.; Pace, F. (2010). Android anti-forensics through a local paradigm, *Digital Investigation*, C. 7, Sayı SUPPL. doi:10.1016/j.diin.2010.05.011

[46] Dijital adli tıp: 4.1 Dijital adli tıp süreci - OpenLearn - Açık Üniversite - M812_1. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1, erişim 18-5-2020

[47] Pollitt, M. (2016). The key to forensic success: Examination planning is a key determinant of efficient and effective digital forensics, *Digital Forensics: Threatscape and Best Practices*. doi:10.1016/B978-0-12-804526-8.00002-2

[48] Sachowski, J. (2016). *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*. doi:10.1016/C2015-0-00701-8

[49] Kovacich, G.; Jones, A. (2006). *High-Technology Crime Investigator's Handbook*, *High-Technology Crime Investigator's Handbook*. doi:10.1016/B978-0-7506-7929-9.X5038-6

[50] Casey, E. (2011). *Chapter 20 OF Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, *International Journal of Law and Information Technology*

[51] Patil, R. Y.; Devane, S. R. (2019). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime, *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2019.11.016

[52] Dijital adli tıp: 4.3 Farklı dijital adli tıp türleri - OpenLearn - Açık Üniversite - M812_1. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3, erişim 19-5-2020

[53] Schramp, R. (2017). Live transportation and RAM acquisition proficiency test, *Digital Investigation*, C. 20, 44–53. doi:10.1016/j.diin.2017.02.006

[54] Lin, X.; Chen, T.; Zhu, T.; Yang, K.; Wei, F. (2018). Automated forensic analysis of mobile applications on android devices, *Proceedings of the Digital Forensic Research Conference, DFRWS 2018 USA*, S59–S66. doi:10.1016/j.diin.2018.04.012

[55] Scrivens, N.; Lin, X. (2017). Android digital forensics: Data, extraction and analysis, *ACM International Conference Proceeding Series* (C. Part F1277). doi:10.1145/3063955.3063981

[56] Feng, P.; Li, Q.; Zhang, P.; Chen, Z. (2018). Logical acquisition method based on data migration for Android mobile devices, *Digital Investigation*, C. 26, 55–62. doi:10.1016/j.diin.2018.05.003

[57] Ayers, R.; Jansen, W.; Brothers, S. (2014). Guidelines on mobile device forensics (NIST

Special Publication 800-101 Revision 1), *NIST Special Publication*, C. 1, Sayı 1, 85. doi:10.6028/NIST.SP.800-101r1

[58] Daniel, L.; Daniel, L. (2012). *Digital Forensics for Legal Professionals*, *Digital Forensics for Legal Professionals*. doi:10.1016/C2010-0-67122-7

[59] AFLogical™ Open Source Edition Now Available for Download - NowSecure. https://www.nowsecure.com/blog/2012/07/29/aflogical-trade-open-source-edition-now-available-for-download/, erişim 19-5-2020

[60] Android Hata Ayıklama Köprüsü (adb) | Android Geliştiricileri. https://developer.android.com/studio/command-line/adb, erişim 19-5-2020

[61] android-backup-extractor download | SourceForge.net. https://sourceforge.net/projects/adbextractor/, erişim 19-5-2020

[62] Sammons, J. (2012). *The Basics of Digital Forensics*, *The Basics of Digital Forensics*. doi:10.1016/C2010-0-68337-4

[63] Wu, S.; Zhang, Y.; Wang, X.; Xiong, X.; Du, L. (2017). Forensic analysis of WeChat on Android smartphones, *Digital Investigation*, C. 21, 3–10. doi:10.1016/j.diin.2016.11.002

[64] Android 7.0 行为变更 | Android Geliştiricileri | Android Developers. https://developer.android.google.cn/about/versions/nougat/android-7.0-changes, erişim 19-5-2020

[65] Son, N.; Lee, Y.; Kim, D.; James, J. I.; Lee, S.; Lee, K. (2013). A study of user data integrity during acquisition of android devices, *Proceedings of the Digital Forensic Research Conference, DFRWS 2013 USA*, S3–S11. doi:10.1016/j.diin.2013.06.001

[66] Yang, S. J.; Choi, J. H.; Kim, K. B.; Chang, T. (2015). New acquisition method based on firmware update protocols for android smartphones, *Proceedings of the Digital Forensic Research Conference, DFRWS 2015 USA*, S68–S76. doi:10.1016/j.diin.2015.05.008

[67] iOS Atılımı, Tam Dosya Sistemi Çıkarma için Yasal Erişimi Sağlıyor - Cellebrite.https://www.cellebrite.com/en/blog/ios-breakthrough-enables-lawful-access-for-full-file-system-extraction/, erişim 19-5-2020

[68] Sunde, N.; Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward, *Digital Investigation*, C. 29, 101–108. doi:10.1016/j.diin.2019.03.011

[69] Horsman, G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework, *Digital Investigation*, C. 28, 146–151. doi:10.1016/j.diin.2019.01.007

[70] Casey, E. (2018). Clearly conveying digital forensic results, *Digital Investigation*, 1–3. doi:10.1016/j.diin.2018.03.001

[71] Akalın, U. (2016). Mobil Cihazlarda Adli Bilişim Çalişmalarina Yönelik Bir Model Önerisi, 139

[72] Officers, C. P. (2008). Good Practice Guide for Computer-Based Electronic Evidence, *Director*, C. 67, Sayı 5, 72. doi:10.1016/j.jad.2011.08.001

[73] Dimitriadis, A.; Ivezic, N.; Kulvatunyou, B.; Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks, *Array*, C. 5, 100015. doi:10.1016/j.array.2019.100015

[74] O., K.; Quayson, E.; Agyei, O.; Danso, E. (2017). Survey of Digital Forensic Models and Proposed Thematic Scheme, *International Journal of Computer Applications*, C. 169, Sayı 11, 41–45. doi:10.5120/ijca2017914782

[75] Polymeropoulou, P. (2014). Book Review: Graves, Michael W. Digital Archaeology: The Art and Science of Digital Forensics , *Information Security Journal: A Global Perspective*, C. 23, Sayı 1–2, 45–45. doi:10.1080/19393555.2013.877542

[76] Mushtaque, K. (2015). Digital Forensic Investigation Models, an Evolution study, *Journal of Information Systems and Technology Management*, C. 12, Sayı 2. doi:10.4301/s1807-17752015000200003

[77] Lutui, R. (2016). A multidisciplinary digital forensic investigation process model, *Business Horizons*, C. 59, Sayı 6, 593–604. doi:10.1016/j.bushor.2016.08.001

[78] Bryant, R.; Bryant, S. (2014). *Policing digital crime*, *Policing Digital Crime*

[79] Du, X.; Le-Khac, N. A.; Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service, *European Conference on Information Warfare and Security, ECCWS*, 573–581

[80] Rogers, M. K.; Goldman, J.; Mislan, R.; Wedge, T.; Debrota, S.; Rogers, M. K.; Goldman, J.; Wedge, T.; Debrota, S. (2006). Journal of Digital Forensics , Security and Law Computer Forensics Field Triage Process Model Computer Forensics Field Triage Process Model, C. 1, Sayı 2, 1–21

[81] Martini, B.; Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing, *Digital Investigation*, 71–80. doi:10.1016/j.diin.2012.07.001

[82] Quick, D.; Choo, K. W. R. (2014). Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive, *Trends and Issues in Crime and Criminal Justice*, 1–11

[83] Perumal, S.; Md Norwawi, N.; Raman, V. (2015). Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology, *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 19–23. doi:10.1109/ICDIPC.2015.7323000

[84] Hitchcock, B.; Le-Khac, N. A.; Scanlon, M. (2016). Tiered forensic methodology model for

digital field triage by non-digital evidence specialists, *DFRWS 2016 EU - Proceedings of the 3rd Annual DFRWS Europe*, S75–S85. doi:10.1016/j.diin.2016.01.010

[85] Ibrahim, T. M.; Abdulhamid, S. M.; Alarood, A. A.; Chiroma, H.; Al-garadi, M. A.; Rana, N.; Muhammad, A. N.; Abubakar, A.; Haruna, K.; Gabralla, L. A. (2019). Recent advances in mobile touch screen security authentication methods: A systematic literature review, *Computers and Security*, 1–24. doi:10.1016/j.cose.2019.04.008

[86] Feng, T.; Liu, Z.; Kwon, K. A.; Shi, W.; Carbunar, B.; Jiang, Y.; Nguyen, N. (2012). Continuous mobile authentication using touchscreen gestures, *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*. doi:10.1109/THS.2012.6459891

[87] Abdulhamid, S. M.; Waziri, V. O.; Idris, I.; Gbolahan, A.; Alhassan, J. K. (2018). A forensic evidence recovery from mobile device applications, *International Journal of Digital Enterprise Technology*. doi:10.1504/ijdet.2018.10013745

[88] Jain, A.; Kanhangad, V. (2015). Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures, *Pattern Recognition Letters*. doi:10.1016/j.patrec.2015.07.004

[89] Chen, S.; Pande, A.; Mohapatra, P. (2014). Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones, *MobiSys 2014 - Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*. doi:10.1145/2594368.2594373

[90] Kunz, M.; Kasper, K.; Reininger, H.; Möbius, M.; Ohms, J. (2011). Continuous speaker verification in realtime, *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, 79–87

[91] Derawi, M. O.; Yang, B.; Busch, C. (2012). Fingerprint recognition with embedded cameras on mobile phones, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*. doi:10.1007/978-3-642-30244-2_12

[92] Campisi, P.; Maiorana, E.; Lo Bosco, M.; Neri, A. (2009). User authentication using keystroke dynamics for cellular phones, *IET Signal Processing*. doi:10.1049/iet-spr.2008.0171

[93] Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, *IEEE Transactions on Information Forensics and Security*. doi:10.1109/TIFS.2012.2225048

[94] Shahzad, M.; Liu, A. X.; Samuel, A. (2013). Secure unlocking of mobile touch screen devices by simple gestures - You can see it but you can not do it, *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*.

doi:10.1145/2500423.2500434

[95] Meng, W.; Wong, D. S.; Furnell, S.; Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones, *IEEE Communications Surveys and Tutorials*. doi:10.1109/COMST.2014.2386915

[96] Murao, K.; Tobise, H.; Terada, T.; Iso, T.; Tsukamoto, M.; Horikoshi, T. (2014). Mobile phone user authentication with grip gestures using pressure sensors, *12th International Conference on Advances in Mobile Computing and Multimedia, MoMM 2014*. doi:10.1145/2684103.2684116

[97] Nader, J.; Alsadoon, A.; Prasad, P. W. C.; Singh, A. K.; Elchouemi, A. (2015). Designing Touch-Based Hybrid Authentication Method for Smartphones, *Procedia Computer Science*. doi:10.1016/j.procs.2015.10.072

[98] Antal, M.; Szabó, L. Z. (2016). Biometric Authentication Based on Touchscreen Swipe Patterns, *Procedia Technology*. doi:10.1016/j.protcy.2016.01.061

[99] LeCun, Y.; Kavukcuoglu, K.; Farabet, C. (2010). Convolutional networks and applications in vision, *ISCAS 2010 - 2010 IEEE International Symposium on Circuits and Systems: Nano-Bio Circuit Fabrics and Systems*. doi:10.1109/ISCAS.2010.5537907

[100] Jadhav, P.; Rajguru, G.; Datta, D.; Mukhopadhyay, S. (2020). Automatic sleep stage classification using time–frequency images of CWT and transfer learning using convolution neural network, *Biocybernetics and Biomedical Engineering*. doi:10.1016/j.bbe.2020.01.010

[101] Anand, R.; Shanthi, T.; Sabeenian, R. S.; Veni, S. (2020). Real time noisy dataset implementation of optical character identification using CNN, *International Journal of Intelligent Enterprise*, C. 7, Sayı 1/2/3, 67. doi:10.1504/IJIE.2020.104646

[102] Kokalis, C. C. A.; Tasakos, T.; Kontargyri, V. T.; Siolas, G.; Gonos, I. F. (2020). Hydrophobicity classification of composite insulators based on convolutional neural networks, *Engineering Applications of Artificial Intelligence*. doi:10.1016/j.engappai.2020.103613

[103] Szegedy, C.; Vanhoucke, V.; Ioffe, S.; Shlens, J.; Wojna, Z. (2016). Rethinking the Inception Architecture for Computer Vision, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. doi:10.1109/CVPR.2016.308

[104] Lecun, Y.; Bottou, L.; Bengio, Y.; Ha, P. (1998). LeNet, *Proceedings of the IEEE*. doi:10.1109/5.726791

[105] Krizhevsky, A.; Sutskever, I.; Hinton, G. E. (2012). 2012 AlexNet, *Advances In Neural Information Processing Systems*. doi:http://dx.doi.org/10.1016/j.protcy.2014.09.007

[106] Szegedy, C.; Liu, W.; Jia, Y.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. (2015). Going deeper with convolutions, *Proceedings of the IEEE*

Computer Society Conference on Computer Vision and Pattern Recognition, C. 07-12-June, 1–9. doi:10.1109/CVPR.2015.7298594

[107] Liu, Z.; Li, J.; Shen, Z.; Huang, G.; Yan, S.; Zhang, C. (2017). Learning Efficient Convolutional Networks through Network Slimming, *Proceedings of the IEEE International Conference on Computer Vision*. doi:10.1109/ICCV.2017.298

[108] Fu, R.; Li, B.; Gao, Y.; Wang, P. (2018). Visualizing and analyzing convolution neural networks with gradient information, *Neurocomputing*, C. 293, 12–17. doi:10.1016/j.neucom.2018.02.080

[109] Gadde, R.; Jampani, V.; Kiefel, M.; Kappler, D.; Gehler, P. V. (2016). Superpixel convolutional networks using bilateral inceptions, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. doi:10.1007/978-3-319-46448-0_36

[110] Szegedy, C.; Ioffe, S.; Vanhoucke, V.; Alemi, A. A. (2017). Inception-v4, inception-ResNet and the impact of residual connections on learning, *31st AAAI Conference on Artificial Intelligence, AAAI 2017*

[111] He, K.; Zhang, X.; Ren, S.; Sun, J. (2016). ResNet, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. doi:10.1109/CVPR.2016.90

[112] Singh, B.; Toshniwal, D.; Allur, S. K. (2019). Shunt connection: An intelligent skipping of contiguous blocks for optimizing MobileNet-V2, *Neural Networks*. doi:10.1016/j.neunet.2019.06.006

[113] Sandler, M.; Howard, A.; Zhu, M.; Zhmoginov, A.; Chen, L. C. (2018). MobileNetV2: Inverted Residuals and Linear Bottlenecks, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. doi:10.1109/CVPR.2018.00474

[114] Zhang, X.; Zhou, X.; Lin, M.; Sun, J. (2018). ShuffleNet: An Extremely Efficient Convolutional Neural Network for Mobile Devices, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. doi:10.1109/CVPR.2018.00716

[115] Özyurt, F.; Sert, E.; Avcı, D. (2020). An expert system for brain tumor detection: Fuzzy C-means with super resolution and convolutional neural network with extreme learning machine, *Medical Hypotheses*. doi:10.1016/j.mehy.2019.109433

[116] Iandola, F. N.; Han, S.; Moskewicz, M. W.; Ashraf, K.; Dally, W. J.; Keutzer, K. (2016). SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size, 1–13

[117] Toğaçar, M.; Ergen, B.; Cömert, Z. (2020). Detection of lung cancer on chest CT images using minimum redundancy maximum relevance feature selection method with

convolutional neural networks, *Biocybernetics and Biomedical Engineering*. doi:10.1016/j.bbe.2019.11.004

[118] Oufaida, H.; Nouali, O.; Blache, P. (2014). Minimum redundancy and maximum relevance for single and multi-document Arabic text summarization, *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2014.06.008

[119] Horsman, G.; Page, H.; Beveridge, P. (2018). A preliminary assessment of latent fingerprint evidence damage on mobile device screens caused by digital forensic extractions, *Digital Investigation*, C. 27, 47–56. doi:10.1016/j.diin.2018.10.002

[120] Leetcode 351: Android Kilit Açma Desenleri. https://baihuqian.github.io/2018-08-12-android-unlock-patterns/, erişim 20-5-2020

[121] IDC - Akıllı Telefon Pazar Payı - İşletim Sistemi. https://www.idc.com/promo/smartphone-market-share/os, erişim 20-5-2020

[122] • Uygulama mağazaları: önde gelen uygulama mağazalarındaki uygulama sayısı 2020 | statista. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, erişim 20-5-2020

[123] Opasiak, K.; Mazurczyk, W. (2019). (In)Secure Android Debugging: Security analysis and lessons learned, *Computers and Security*, C. 82, 80–98. doi:10.1016/j.cose.2018.12.010

[124] Løge, M. D. (2015). *Tell Me Who You Are and I Will Tell You Your Unlock Pattern*, *Master thesis*

[125] Bana kim olduğunu söyle sana ekran kilidi açma desenini söyleyeyim.https://www.kaspersky.com.tr/blog/bana-kim-oldugunu-soyle-sana-ekran-kilidi-acma-desenini-soyleyeyim/1799/, erişim 22-5-2020

[126] Samsung Exynos 7 Octa 7870 Chipset Kullanan Telefonlar - Epey. https://www.epey.com/akilli-telefonlar/yonga-seti-chipset/samsung-exynos-7-octa-7870/, erişim 23-5-2020

[127] MSAB Hakkında - MSAB. https://www.msab.com/company/, erişim 23-5-2020

[128] Oksijen Adli Tıp - Mobil adli tıp çözümleri: yazılım ve donanım. https://www.oxygen-forensic.com/en/company, erişim 23-5-2020

[129] Cellebrite UFED - Cellebrite. https://www.cellebrite.com/en/ufed/#, erişim 23-5-2020

[130] Koordinat Bulma - HESAPLAMA.NET. https://koordinat.hesaplama.net/hesaplama.do, erişim 28-5-2020

[131] WhatsApp Plus APK İndir (Official) Son Sürüm v8.50 | Anti-Ban. https://gbapps.net/, erişim 27-5-2020

[132] Android'in UID / GID'lerle izin eşlemesi nasıl çalışır? - Android Meraklıları Stack Exchange. https://android.stackexchange.com/questions/208523/how-androids-permissions-mapping-with-uids-gids-works, erişim 25-5-2020

[133] *The Mobile Application Hacker's Handbook*. (2014). *The Mobile Application Hacker's Handbook*. doi:10.1002/9781119183655

ÖZGEÇMİŞ

Ömer Faruk YAKUT

KİŞİSEL BİLGİLER

Doğum Yeri	**:** Hamur
Doğum Yılı	**:** 1986
Uyruğu	**:** T.C
Adres	**:** Bostanbaşı Mah. Çiftlik Cad. Payitaht Sit. D Blok No:36 Yeşilyurt/Malatya
E-posta	**:** .omerfaruk.yakut@egm.gov.tr
Yabancı Diller	**:** -

EĞİTİM BİLGİLERİ

Lisans	**:** Muğla Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 2007
Önlisans	**:** Andolu Üniversitesi, Açıköğretim Fakültesi, Adalet, 2015
Lise	**:** Hamur Lisesi, Ağrı, 2003

ARAŞTIRMA DENEYİMİ

- ✓ Cellebrite, XRY, Oxyeen Forensic, Hashcat, Pasware Forensic Tool Kit, FTK, Encase, FEX, MOBILedit, Autops Forensic,

İŞ DENEYİMİ

B. YIL – 2009 **:**Emniyet Genel Müdürlüğü

AKADEMİK FAALİYETLER

Makaleler:

1. ERTAM, F.; YAKUT, Ö. F. (2020). Android Cihazların Adli Bilişim Analizlerinde Parola Tespitine Bağlı Yeni Süreç Tanımlama Modelinin Geliştirilmesi, Fırat Üniversitesi Mühendislik Bilimleri Dergisi, C. 32, Sayı 1, 147–156. doi:10.35234/fumbd.613879

Projeler:

2. Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından TEKF.20.06 protokol numaralı proje