AJIT-e Academic Journal of Information Technology
10.5824/ajite.2025.04.008.x

2025 . Fall – Güz . Volume – Cilt: 16 . Issue – Sayı: 4

Mobil Cihaz Adli Analizi Sistematik Literatür Taraması

Müge Begüm Dönmez, *Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Doktora Öğrencisi, mbd.dnmez@yandex.com, 0000-0002-2033-1179*

İbrahim Alper Doğru, *Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği, Prof. Dr, iadogru@gazi.edu.tr, 0000-0001-9324-7157*

ÖZ

Günümüzde kullanıcıların işlemlerinin büyük bir kısmını dijital platformlar üzerinden gerçekleştirmesi, mobil cihaz kullanım oranlarını önemli ölçüde artırmıştır. Mobil cihazlar birçok kolaylık ve avantaj sağlarken, beraberinde çeşitli sorunları ortaya çıkarmıştır. Fiziksel ortamda işlenen çoğu suç, artık dijital ortamlara taşınmıştır. Mobil cihazlara erişimin kolaylaşması, bu araçların, suç işleme aracı olarak kullanılmasını da gündeme getirmiştir. Teknolojinin hızla gelişmesi, mobil cihazların sürekli değişen dinamik yapısı ve her geçen gün yeni özellikler kazanması kullanıcılar açısından düşünüldüğünde geniş imkanlar sağlamakta ancak suç soruşturmalarında görev alan adli bilişim uzmanları için ise çeşitli zorluklar oluşturmaktadır. Mobil cihazların suç delili olarak elde edilmesinden, bu delillerin mahkemeye sunulmasına kadar geçen adli bilişim inceleme süreçlerinde birçok zorluklarla karşılaşılmaktadır. Mobil cihazların çok katmanlı yapısı, işletim sistemlerinin cihazdan cihaza farklılık göstermesi, her cihazda farklı uygulamaların bulunması, cihaz ya da cihaz içi bileşenlerin parola ile korunuyor olması bu zorluklar arasında yer almaktadır. Sürekli değişen ve gelişen mobil cihaz teknolojisinin yakından takip edilmesi adli bilişim inceleme süreçlerinin sağlıklı bir şekilde yürütülebilmesi açısından büyük önem taşımaktadır. Belirtilen sorunlar, araştırmanın temel motivasyonunu ve hareket noktasını oluşturmuştur. Araştırmada, 2019-2024 yılları arasında yayınlanan 19 makale üzerinden mobil cihazlarda adli analiz alanındaki gelişmeler sistematik literatür taraması yöntemiyle incelenmiştir. Araştırma kapsamında mobil cihazlarda kullanılan işletim sistemleri, cihaz türleri, kullanılan adli bilişim araçları ve incelenen uygulama türleri detaylı şekilde ele alınmıştır. İncelenen araştırmalar, mobil adli bilişimdeki teknolojik çeşitlilik ve karmaşıklığın, uzmanların çok yönlü bilgi ve becerilere sahip olmasını gerektirdiğini ortaya koymaktadır. Son bölümde, araştırmalara yönelik sonuçlar özetlenmiş ve gelecekte gerçekleştirilebilecek çalışmalara yönelik öneriler sunulmuştur.

Anahtar Kelimeler : Mobil Adli Bilişim, Mobil Adli Analiz, Sosyal Medya Analizi, Mobil Cihazlardan Elde Edilen Adli Kalıntılar

Derleme Makale / ReviewArticle
Date Received: 29.07.2025
Publishing Date: 30.11.2025

AJIT-e Academic Journal of Information Technology
2025 Fall/Güz – Cilt/Vol: 16 - Sayı/Issue: 4
10.5824/ajite.2025.04.008.x

A Systematic Literature Review On Mobile Device Forensic Analysis

ABSRACT

With the increasing tendency of users to perform most of their activities through digital platforms, the use of mobile devices has risen significantly. While mobile devices provide numerous conveniences and advantages, they have also introduced various challenges. Many crimes that were previously committed in physical environments have now shifted to digital spaces. The ease of accessing mobile devices has brought forth their use as instruments of crime. The rapid advancement of technology, the dynamic structure of mobile devices, and the continuous addition of new features offer extensive opportunities for users but pose various challenges for digital forensic experts involved in criminal investigations. Throughout the digital forensic examination process—from obtaining mobile devices as evidence to presenting the findings in court—many difficulties are encountered. The multilayered structure of mobile devices, the variation of operating systems across devices, the diversity of installed applications, and the presence of password-protected components are among the main challenges. Closely following the continuously evolving mobile device technologies is therefore crucial to ensure the effective execution of forensic examination processes. These issues have constituted the main motivation and starting point of the present research. In this study, developments in mobile device forensic analysis were examined through a systematic literature review of 19 articles published between 2019 and 2024. The research extensively addressed operating systems used in mobile devices, device types, forensic tools employed, and types of applications analyzed. The reviewed studies reveal that the technological diversity and complexity within mobile forensics require experts to possess multidisciplinary knowledge and skills. In the final section, the findings of the reviewed studies are summarized, and suggestions are provided for future research directions.

Keywords : Mobile Forensics, Mobile Forensic Analysis, Social Media Analysis, Digital Forensic Artifacts from Mobile Devices

GİRİŞ

Sistemlerin(Eğitim, finans, bankacılık vb.) kullanıcılara sağladığı hizmetleri dijital platformlar üzerinden gerçekleştirmesiyle birlikte toplumun dijitalleşme dönüşümü hız kazanmıştır. Bu dijitalleşme sürecinin bir ögesi konumundaki bireylerin mobil cihaz kullanım oranlarının artması da kaçınılmaz hale gelmiştir. Yapılan araştırmalarda, küresel çapta kullanılan mobil cihaz sayısının 2025 yılında 18 Milyar civarında olması öngörülmektedir (Statista, 2025).

Worldometers (2025), mobil cihaz sayısının dünya nüfusunun neredeyse iki katına ulaşabileceğini öngörmektedir. Bu öngörü, mobil cihaz kullanım oranlarının küresel ölçekteki yaygınlığını ortaya koymaktadır.

Kullanıcılara sağladığı sayısız faydanın yanı sıra bir suç aracı olarak da kullanılabilen mobil cihazların barındırdığı veri miktarı da günden güne artmaktadır (Çakır, Kılıç, Bakan ve

Saluk, 2014, s.238). Suç soruşturmalarına konu olan mobil cihazların içerdiği veri miktarının sayıca ve türce çokluğu incelemeyi gerçekleştiren adli bilişim uzmanlarının işlerini zorlaştırmaktadır. Verilere yönelik bu çıkarımların yanı sıra mobil cihazların dinamik yapılı olması, her mobil cihazın farklı işletim sistemleri, donanım ve özelliklere sahip olması da adli bilişim inceleme süreçlerini zorlaştıran sebepler arasında sayılmaktadır. İnceleme aşamasında; telefon ve bilgisayar bağlantısı için gereken telefona ait bağlantı kablosunun olmamasının çıkarım işlemini imkansız kılabileceği bu zorluklara örnek olarak verilebilir (Henkoğlu, 2014, s.128).

Araştırmada, mobil cihazların sürekli değişen özelliklerinden yola çıkarak, son 6 yılda (2019-2024) çeşitli dergilerde yayımlanan "Mobil Cihazlarda Adli Analiz" konusunu ele alan; yayın dili İngilizce olan 18 makale ele alınmıştır.

Araştırmacılar, mobil cihazlarda çeşitli yollarla elde ettikleri verileri(Programlama yoluyla elde edilen yapay veriler ya da araştırmacılar tarafından oluşturulmuş veri setleri) analiz ederken; ticari ve ticari olmayan yazılımları kullanmışlardır. Mobil cihazlardan elde edilen veriler tür olarak; yerleşik mobil cihaz uygulamaları, mobil cihaz uygulamaları ve sosyal medya uygulamaları olarak sınıflandırılmıştır. Sosyal medya uygulamalarının artan kullanımları mobil cihazlarda oluşturulan veri sayılarındaki artışa yansımıştır. Araştırmalar incelendiğinde sosyal medya popülaritesi dolayısıyla ağırlıklı olarak bu alanda gerçekleştirilmiştir. Yapılan araştırmalar neticesinde Sosyal Medya Analizi şeklinde bir kavramın oluşması bu popülariteyi doğrulamaktadır.

SLR(Systematic Literature Review) niteliğinde ele alınan araştırmada amaç, mobil cihazlarda adli analiz konusunda yayınlanan araştırmaları inceleyerek aşağıdaki soruların (Research Questions) cevaplarını tespit etmektir:

- RQ1: Mobil Cihaz Adli Analiz konulu makalelerin yıl bazında oranları nedir?
- RQ2: Mobil Cihaz Adli Analiz konulu makalelerin yayınlandığı dergiler nelerdir?
- RQ3:Literatür araştırmalarında kullanılan cihaz türleri ve bu cihaz türlerine ait işletim sistemleri nelerdir, hangi işletim sistemine ağırlık verilmiştir?
- RQ4: Literatür araştırmalarında kullanılan ticari ve açık kaynak kodlu yazılımların kullanım oranları nedir?
- RQ5: Literatür araştırmalarında incelenen uygulama türleri nelerdir?

Verilen soruların cevaplanmasıyla birlikte bu alanda araştırma yapan veya yapacak kişilere yönelik detaylı bir inceleme sunulacaktır. Araştırmalara yönelik detaylı incelemeler, literatürdeki eksikliklerin tespit edilmesi ve yeni araştırmalar için yön gösterici olması açısından faydalı olacaktır.

Araştırma aşağıda sıralandığı şekilde düzenlenmiştir. Araştırmalara yönelik teorik kavramlar ve tanımları içeren 2.Bölüm, kullanılan araçlar, teknikler ve yöntemlerin ele alındığı 3. Bölüm, araştırmalardan elde edilen bulguların yer aldığı 4.Bölüm, bulguların değerlendirildiği tartışmanın yer aldığı 5. Bölüm, nihai değerlendirmenin yapıldığı 6.sonuç

10.5824/ajite.2025.04.008.x

bölümü, son olarak gelecekte yapılacak araştırmalara yönelik önerilerin yer aldığı 7.Bölüm ile araştırma sonlandırılmıştır.

1. MOBİL CİHAZ ADLİ BİLİŞİM İNCELEME SÜREÇLERİ

Adli bilişimin beş alt grupta incelenmesine (Veri tabanı, ağ, bilgisayar, mobil cihazlar ve adli analiz) yönelik literatürde birden çok sayıda yayına ulaşmak mümkündür (Jones ve Winster, 2017). Günümüzde artan mobil cihaz kullanımı mobil adli bilişimi bu gruplandırma içerisinde önemli bir konuma getirmiştir. Suç soruşturmaları sırasında suça konu olan mobil cihazlarda bulunan verilerin elde edilmesinden mahkemede sunulmasına kadar geçen sürede gerçekleştirilen işlemler mobil adli bilişim olarak adlandırılmaktadır.

Adli bilişimin alt dallarına ilişkin akademisyenler tarafından sağlanan uzlaşı mobil cihazlar konusunda sağlanamamıştır. Mobil cihazların katmanlı ve dinamik yapıda olması, gelişen teknolojilerin sağladığı imkanlar dahilinde her geçen gün yeni özellikler kazanması (örneğin çeşitlenen mobil uygulamalar vb.), kavram karmaşası yaratmaktadır. Örneğin, mobil cihazlarda mobil uygulama olarak ele alınabilecek durumdaki sosyal medya uygulamaları mobil adli bilişimin altında incelenebilecekken ayrı bir dal olarak karşımıza çıkmaktadır. Sosyal Medya Ağları Bilişimi şeklinde ortaya çıkan kavram, sadece sosyal medya verilerini kapsamaktadır. Suç soruşturmasına konu alan dijital delil depolayıcısı mobil cihazlarda adli bilişim süreçleri farklı metodolojilere bağlıdır.

Literatür incelendiğinde; mobil adli bilişim sürecinin aşağıda verildiği şekilde gerçekleştirildiği konusunda fikir birliği söz konusudur.

- Verilerin muhafazası
- Verilerin elde edilmesi
- Verilerin analizi
- Verilerin raporlanması ve sunulması

1.1. Verilerin muhafazası

Literatür araştırmalarının çoğunda kullanılan ve referans olarak gösterilen çalışmada Casey (2011), dijital delil niteliğindeki verilerin bütünlüğünü korumak amacıyla, herhangi bir değişime maruz bırakılmadan bahsi geçen delillerin korunmasını belirtmiştir. Olayın gerçekleştiği suç mahallinde hangi cihaz ya da nesnenin delil niteliğinde olmasının mümkün olmaması sebebiyle, delilin ispatlanabilirliğini tehlikeye düşürmemek için alan koruma altına alınmalıdır.

NIJ Rehberi' nde, muhafaza aşamasında delilin bütünlüğünü korumak, yetkisiz veya yanlış müdahaleleri engellemek ve delil zincirini doğru yönetmek amacıyla belli ilkeler temelinde durulmuştur(National Institute of Justice, 2007).

Aşağıda bu ilkeler yer almaktadır:

- *Delil Bütünlüğünün Korunması,*
- *Doğru Olay Yeri Yönetimi*
- *Delil Zinciri (Chain of Custody) Oluşturma,*
- *Hızlı ve Uygun Müdahale,*

- *Uzman Desteği Alınması.*

Bu ilkeler, adli bilişim süreçlerinin sağlıklı bir şekilde gerçekleştirilmesi için kritik öneme sahiptir.

1.2. Verilerin elde edilmesi

Suç mahallinde bulunan her türlü nesnenin korumaya alınmasının ardından, delil niteliği taşıyabilecek cihazların tespit edilmesi işlemlerinin gerçekleştirildiği aşamadır. Cihazlar üzerindeki dijital delil olarak nitelendirilebilecek verilerin bozulmadan eksiksiz bir şekilde elde edilmesi amaçlanmaktadır. Bu işlem basamağı cihazlardan veri elde edilmek için uygulanacak teknik yöntem ve prosedürlerden(Örneğin, bit düzeyinde imaj alma, fiziksel ve mantıksal kopyalama, bulut sistemlerinden veri elde etme vb.) oluşmaktadır (Lessard ve Kessler, 2010) .

1.3. Verilerin analizi

Suç mahallinden elde edilen verilerin suça dayanak olması amacıyla anlamlandırılması ve bilgiye dönüştürülmesi sürecini içeren aşamadır. Bu süreçte ticari ya da açık kaynak kodlu yazılımlar kullanılabilirken manuel yöntemlerle de analizler gerçekleştirilebilir. Veriler elde edildikten sonra olayla ilgili olan ile olmayan bilgilerin ayrılması bilgilerin önceliklendirilmesi işlemi gerçekleştirilir (Ayers, Brothers ve Jansen, 2014).

1.4. Verilerin raporlanması ve sunulması

Delillerin suç mahalli ve sonrasında elde edilmesinden mahkemeye sunulmasına kadar geçen süre içerisinde yapılan işlemler doküman haline getirilmelidir. Yapılan her işlemin bilgi dahilinde olması için gereken dokümantasyon işlemi delil niteliğindeki verilerin mahkemeye sunulması ile son bulmaktadır.

NIST Rehberi, raporlama aşaması için yapılması gereken için belli başlı maddeleri belirlemiştir (Kent, Chevalier, Grance ve Dang, 2006).

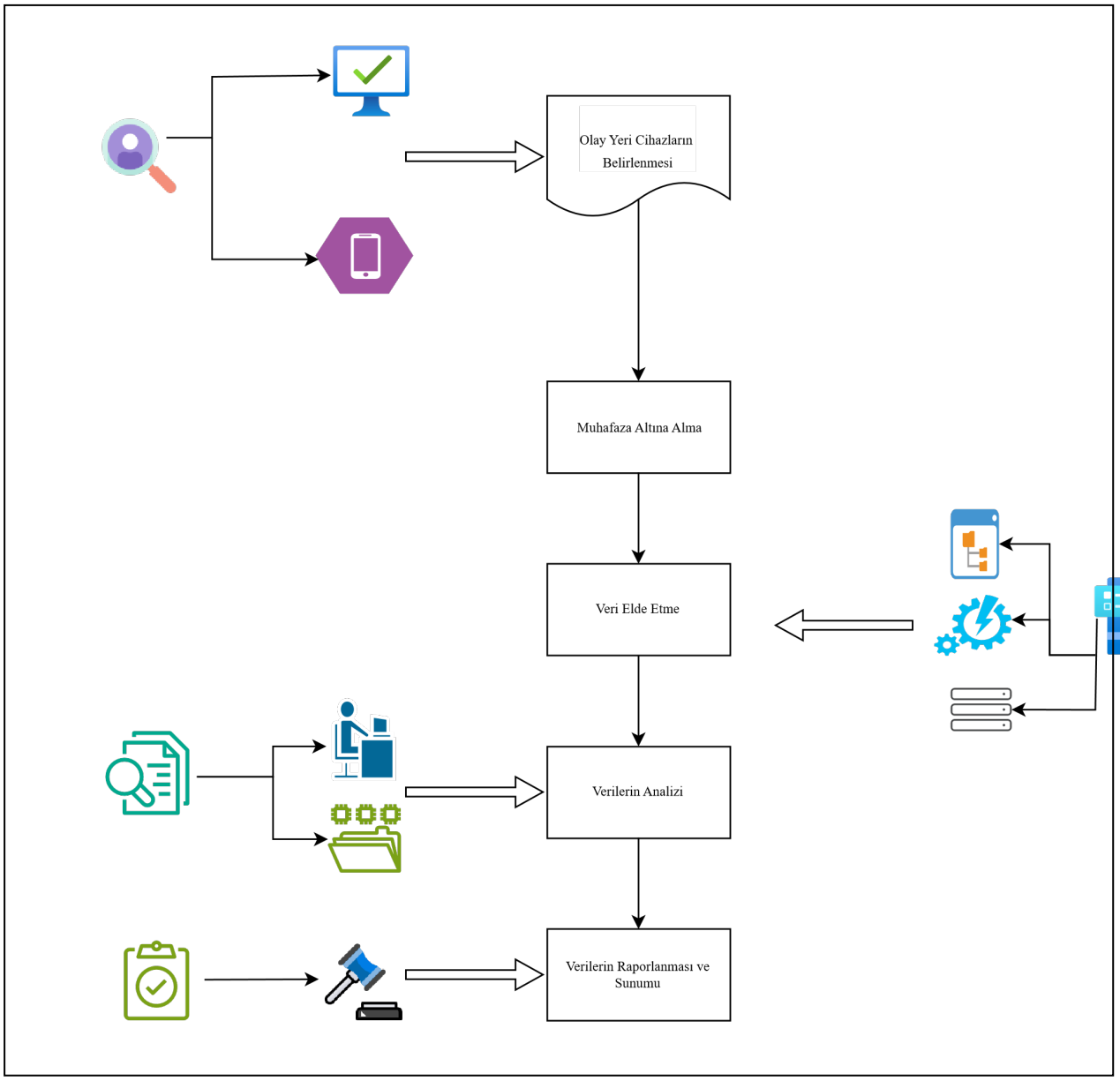
Aşağıda bu maddeler yer almaktadır:

- *Olaya ilişkin farklı senaryolar test edilmeli ve raporda sunulmalıdır.*
- *Raporda yer alan teknik detaylar veya özet bilgiler anlaşılır olmalı ve ihtiyaca göre düzenlenmelidir.*
- *Dokümantasyon süreci içerisinde gerekli olduğu durumlarda güncellemeler gerçekleştirilmelidir.*
- *Analistler güncel kalmak için düzenli eğitim almalıdır, politikalar ve rehberler periyodik olarak gözden geçirilmelidir.*

2.5 Mobil cihaz adli analizi

Mobil cihazlarda adli analiz işlemi, bir mobil cihazda oluşturulan, depolanan ve işleme uğramış verilerin elde edilmesinden sonra suç teşkil eden bir eylem için kullanıp kullanılmadığının tespiti için işleme sokulduğu adımdır. Mobil adli analiz adımında dijital delillerin tespiti için bilimsel yöntemler uygulanmak durumundadır. Yaygın şekilde kullanılan adli bilişim süreç modeli Şekil1'de yer almaktadır.

AJIT-e Academic Journal of Information Technology
2025 Fall/Güz – Cilt/Vol: 16 - Sayı/Issue: 4
10.5824/ajite.2025.04.008.x



Şekil 1: Adli bilişim inceleme süreci

2. METODOLOJİ

Sistematik literatür araştırması(SLR) 5 temel adımda şekillenmiştir. Öncelikle arama yapılacak veri tabanları belirlenmiş ardından veri tabanlarında kullanılacak anahtar kelimeler belirlenmiş ve arama işlemi gerçekleştirilmiştir. Arama işlemlerinde kapsam içine alınan ve kapsam dışında bırakılan araştırmalar belirlenmiş en nihayetinde seçilen araştırmalarla ilgili analiz süreci gerçekleştirilmiştir. Bu bölümde her adımın ayrıntılı bilgileri yer almaktadır.

2.1. Arama sırasında kullanılan veri tabanları

Sistematik literatür taramasının ilk aşaması olan veri tabanları tespiti için Science Direct veri tabanı kullanılmıştır. Science Direct açık erişimli yayınları konusunda sınırlı

imkanlar sunmaktadır; bu sebeple araştırma kapsamının genişletilebilmesi için Google Scholar kaynak olarak kullanılmıştır.

2.2. Arama sırasında kullanılan anahtar kelimeler

Veri tabanı seçiminin ardından aramalar sırasında kullanılacak anahtar kelimeler, araştırma konusunu kapsayacak şekilde belirlenmiştir. Anahtar kelime seçimleri öncellikle kapsamlı olacak şekilde belirlenmiş ardından; kapsam daraltılmıştır. Arama sırasında "mobile device forensic", "mobile digital forensics", "mobile forensic tool", "mobile forensic analysis", "social media analysis", "forensic artifacts from mobile devices" anahtar kelimeleri kullanılmıştır.

2.3. Arama yapılan yayınların kapsamı

Araştırma yayınları belirli ölçütlere göre kapsama alınmış ya da kapsam dışında bırakılmıştır. Yayın dili İngilizce olan, 2019-2024 yılları arasında erişime açık olarak yayınlanan araştırmalar, araştırma kapsamına alınmıştır. Bunun dışında yayın yılı eski tarihli olan ve erişime açık olmayan yayınlar araştırma kapsamına dahil edilmemiştir. Araştırmaların dilinin İngilizce seçilmesinin nedeni uluslararası literatüre katkı sağlama amacından kaynaklanmaktadır.

2.4. Araştırmaların analiz süreci

Sistematik literatür araştırmasında, bütünden parçaya giden şematik araştırma yapısı kullanılmıştır. Öncelikle araştırmaların metodolojik yapıları genel bir çerçevede sunulmuştur; ardından özele inilerek araştırmalar hakkında detaylı bilgiler verilmiştir. Literatür araştırmalarında araştırma sorularını cevaplamaya yönelik adımlar gerçekleştirilmiştir. Literatür araştırmaları, yayınlandıkları yıl, yayın yerleri, kullanılan mobil cihaz marka ve modelleri, işletim sistemleri ve araştırma kapsamında kullanılan araçlara göre sınıflandırılmıştır. Araştırmaların kapsamlı analizi literatürdeki eksiklerin belirlenmesini sağlayacak ve gelecekteki araştırmalara yön verebilecek önerileri sunacaktır.

Tablo 1'de belirtilen 19 makalenin özet bilgileri aşağıda sunulmuş, bulgular bölümünde ise bu bilgiler detaylandırılmıştır.

Tablo1: Literatür araştırmalarına ait genel bilgiler

Yazar(lar) ve Yıl	Yayın Adı	Yayınlanma Yeri	Kullanılan Mobil Cihaz Modelleri	Kullanılan İşletim Sistemleri	Kullanılan Araçlar
(Bays ve Karabiyik, 2019)	Forensic analysis of third party location applications in android and ios	IEEE INFOCOM 2019-CCW	Iphone5 Iphone7 Samsung Galaxy S7	IOS Android	UFED Magnet AXIOM
(Knox, Moghadam, Patrick, Phan ve Choo, 2020)	What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps	Computers & security,	Iphone6 Iphone6S Iphone7 Iphone7 Samsung Galaxy S6 Edge Samsung Galaxy Tab A6 Samsung Galaxy S5	IOS Android	MobilEdit FTK Autopsy Fiddler Db Browser for SQlite MiXplorer

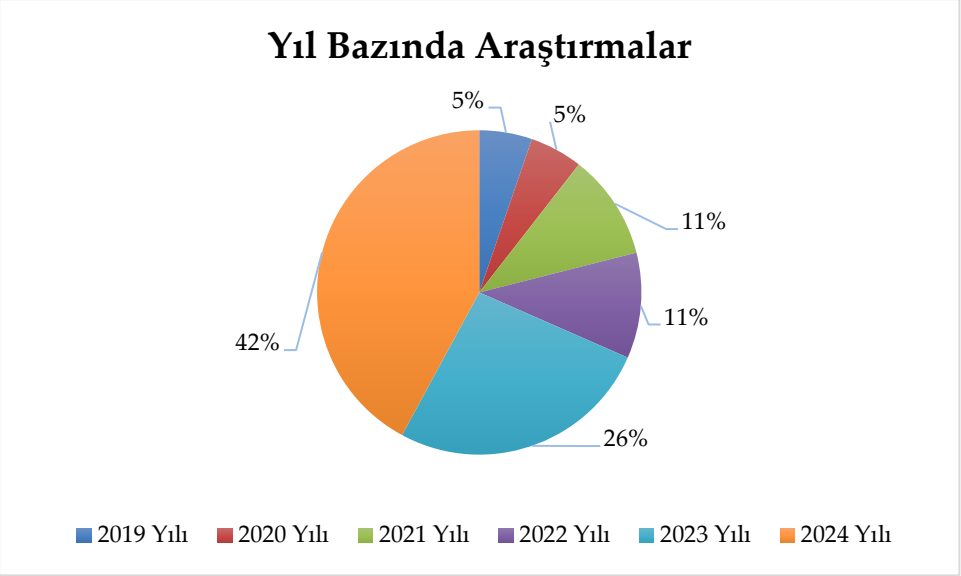
(Cheng, Shi, Gong ve Guan, 2021)	Logextractor: Extracting digital evidence from android log messages via string and taint analysis	Forensic Science International: Digital Investigation	Google Pixel 2	Android	LogExtractor
(Van Zandwijk ve Boztas, 2021	The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones	Forensic science international: digital investigation	Iphone7 plus Iphone 8 Iphone X	IOS	iMazing
(Khalid, Iqbal, Kamoun, Khan ve Shah, 2022)	Forensic investigation of Cisco WebEx desktop client, web, and Android smartphone applications	Annals of Telecommunication	Samsung Galaxy Grand Prime+	Android	AccesData FTK Imager Andriller Autopsy Volatlity ADB RegEdit Db Browser for SQlite MiXplorer Bulk Extractor
(Sumaila ve Bahsi, 2022)	Digital forensic analysis of mobile automotive maintenance applications	Forensic science international: digital investigation	Xiaomi Redmi 9 Samsung Galaxy A20 iPhone XR	IOS Android	Autopy Waze GoFar ve Veepeak OBDCheck, ZUS Smart Vehicle Monitor
(Bowling, Seigfried-Spellar, Karabiyik ve Rogers, 2023)	We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems	Journal of Forensic Sciences	Iphone X Motorola G7	IOS Android	Magnet Axıom Cellebrite UFED 4PC SQlite ChromeCacheView
(Fernández-Fuentes, Pena ve Cabaleiro, 2023)	Digital forensic analysis of the private mode of browsers on Android	Computers & Security	Tablet	Android	AMD AMExtractor Lime AVD
(Murias, Levick ve McKeown, 2023)	A forensic analysis of streaming platforms on Android OS	Forensic Science International: Digital Investigation	BQ Aquaris X Pro	Android	Magnet Axıom Autopsy
(Jennings, Sorell ve Espinosa, 2023)	Interpreting the location data extracted from the Apple Health database	Forensic Science International: Digital Investigation	Apple Watch Iphone 7 Plus	IOS	SQlite
(Blankesteijn, Fukami ve Geradts, 2023)	Assessing data remnants in modern smartphones after factory reset	Forensic Science International: Digital Investigation	Google Pixel Xiaomi Redmi	Android	Ufed Cm2
(Almuqren, Alsuwaelim, Rahman ve Ibrahim, 2024)	A Systematic Literature Review on Digital Forensic Investigation on Android Devices	Procedia Computer Science	-	Android	Andrıller
(Sudiana, Nuruddin, Rizkinia ve Husna, 2024)	Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1.	Journal of Novel Carbon Resource Sciences & Green Asia Strategy	Vıvo V20 SE Oppo A74	Android	SHA256sum Hexdump SQLite DB Browser CherryTree AndroidDebugBridge Whatsapp Key/DatabaseExtractor Whatsapp Crypt Tools

(Çakır ve Karataş, 2024)	Analysis and Comparison of Social Media Applications Using Forensic Software on Mobile Devices	Journal of Forensic Science and Research	Phone SE Samsung A800I Venus V3 5010 Samsung J710FQ	IOS Android	XRY UFED Oxyen Forensic
(Soni, 2024)	Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions	Journal of Forensic Science and Research	-	-	SQlite Viewer SQlite Expert DB Browser for Sqlite
(Patel ve Mann, 2024)	A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges	Security and Privacy	Vivo V2109	Android	MobileEdit MagnetAxiom Balkasoft MD5 SHA1
(Nunes, Domingues ve Frade, 2024)	The Digital Footprints on the Run: A Forensic Examination of Android Running Workout Applications	Future Internet	Vivosmart 4 Samsung A40	Android	ADB ALEAPP Db Browser for Sqlite
(Soni, Kaur ve Aziz, 2024)	Decoding digital interactions: An extensive study of TeamViewer's Forensic Artifacts across Windows and android platforms	Forensic Science International: Digital Investigation	Samsung J2 Redmi Note 5 Samsung J8	Android	Magnet Axıom FTK Imager OS Forensics
(Stanković, Hu, Ozer ve Karabiyik, 2024)	How engaged are you? A forensic analysis of the Oura Ring Gen 3 application across iOS, Android, and Cloud platforms	International Journal of Information Security	Iphone 12 Google Pixel 5a Oura Ring Generation 3	IOS Android	Magnet Axıom Magnet Acquire Magnet Axıom Examine GrayKey

3. BULGULAR

Araştırmanın bu bölümünde, giriş bölümünde yer alan araştırma soruları(Research Questions) cevaplandırılmıştır.

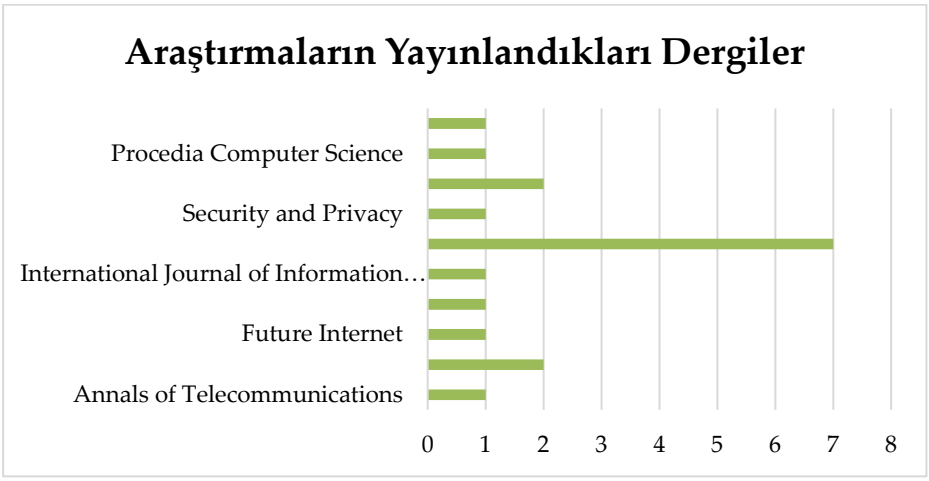
RQ1: Mobil Cihaz Adli Analiz konulu makalelerin yıl bazında oranları nedir?



Şekil 2: Literatür araştırmalarının yıl bazında oranları

Şekil 2 incelendiğinde, literatür araştırmalarının 2024 yılında sayıca en yüksek düzeye ulaştığı görülmektedir. Bununla birlikte, oranların birbirine yakın seyretmesi ve genel artış eğilimi, mobil cihazlardaki adli bilişim ve adli analiz çalışmalarının literatürde giderek önem kazandığını göstermektedir.

RQ2: Mobil Cihaz Adli Analiz konulu makalelerin yayınlandığı dergiler nelerdir?

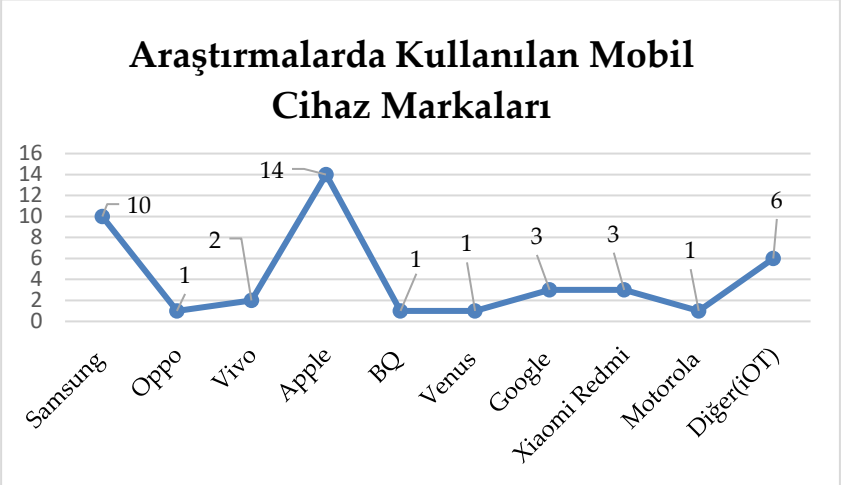


Şekil3: Literatür araştırmalarının yayınlandıkları dergiler

Literatür araştırmaları, yayınlandıkları dergiler bazında sınıflandırıldığında Şekil 3'teki dağılım ortaya çıkmıştır. 19 yayının birisi konferansta sunulmuştur, bu sebeple yukarıda yazılan dergiler içerisinde yer almamaktadır. Yayın sayısı birden fazla olan dergilerde, mobil adli bilişim konusunu ele alan çalışmaların daha önceden yayınlanmış olması, yazarların bu dergileri tercih etmesinde etkili olmuş olabilir.

RQ3: Literatür araştırmaarında kullanılan cihaz türleri ve bu cihaz türlerine ait işletim sistemleri nelerdir, hangi işletim sistemine ağırlık verilmiştir?

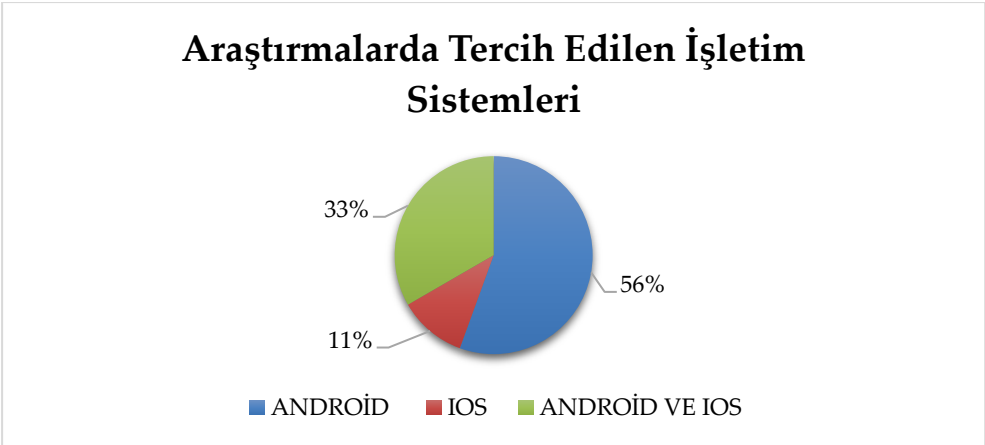
Araştırmalarda kullanılan mobil cihazlar markaları Şekil4' te verildiği gibidir.



Şekil 4: Literatür araştırmalarında kullanılan mobil cihaz markaları

Şekil 4 incelendiğinde, literatürde kullanılan mobil cihazların büyük bir kısmının Apple markasına ait iPhone modeli olduğu görülmektedir. Son yıllarda araştırmalarda iPhone kullanımının artması, kullanıcı sayılarındaki artış ve araştırma gereksinimlerinin bu doğrultuda değişmesiyle açıklanabilir. Araştırmalarda giyilebilir cihaz ve aksesuarlara da (örneğin; Oura Ring Gen 3 akıllı yüzük, Garmin-Vivosmart 4 akıllı saat, Apple Watch) yer verilmiştir. Ayrıca bazı çalışmalarda birden fazla mobil cihazın incelenmiş olması nedeniyle, kullanılan cihaz sayısının incelenen araştırma sayısından fazla olduğu belirlenmiştir. Örneğin, bir araştırmada dört mobil cihaz, başka bir araştırmada ise yalnızca bir adet cihaz kullanılmıştır. Dolayısıyla, markalara yönelimlerin belirlenmesi, bu araştırma sorusunun temel amacını oluşturmaktadır**.**

Araştırmalarda kullanılan mobil cihazlara ait işletim sistemleri Şekil5 'te verildiği gibidir.



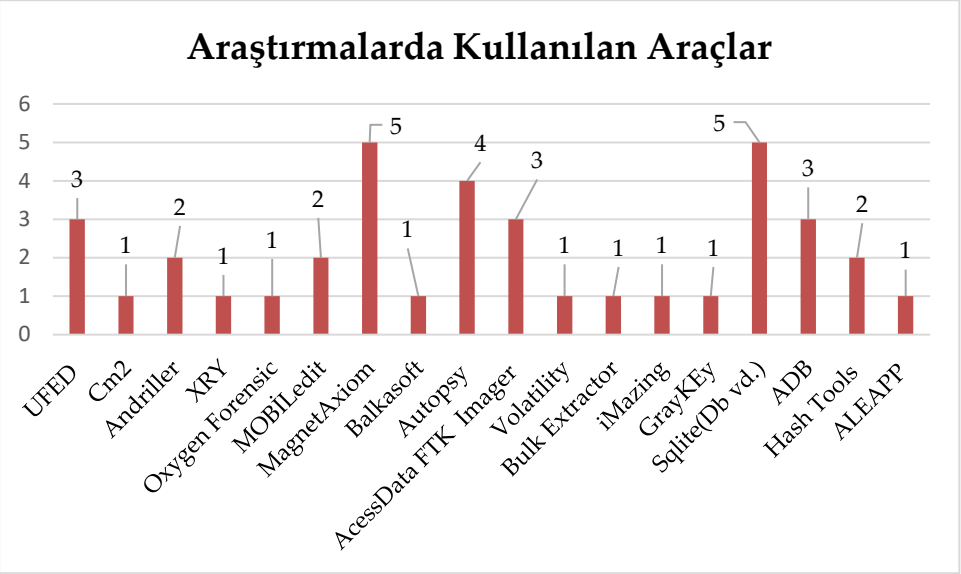
Şekil 5: Literatür araştırmalarında kullanılan cihazlara ait işletim sistemleri

Şekil 5' göre, araştırmalarda en çok Android işletim sistemine sahip mobil cihazlar tercih edilmiştir. Araştırmacılar tarafından genellikle kullanılan mobil cihazlar Android veya

AJIT-e Academic Journal of Information Technology
2025 Fall/Güz – Cilt/Vol: 16 - Sayı/Issue: 4
10.5824/ajite.2025.04.008.x

iOS işletim sistemine sahip düşük fiyatlı ve kolaylıkla erişilebilir alt model cihazlar(Örneğin Iphone 6,7 ve 7 Plus gibi) olarak tespit edilmiştir.

RQ4: Literatür araştırmalarında kullanılan ticari ve ticari olmayan yazılımların oranları nedir?



Şekil 6: Literatür araştırmalarında kullanılan araçlar

İncelemeler kapsamında belirlenen adli bilişim araçları, açık kaynak ve ticari özellikleri temel alınarak aşağıdaki tabloda sınıflandırılmıştır.

Tablo 2: Literatür araştırmalarında kullanılan yazılımların sınıflandırılması

Araç Adı	Ticari Yazılım	Açık Kaynak Kodlu Yazılım
Graykey	X	
İmazing	X	
Bulk Extractor		X
Volatılıty		X
Acessdata Ftk Imager	X	
Autopsy		X
Belkasoft	X	
Magnet Axıom	X	
SQlite		X
Mobıledit	X	
Oxygen Forensıc	X	
Xry	X	
Andrıller	X	
Cm2	X	
Ufed	X	

Şekil 6 ve Tablo 2 birlikte incelendiğinde, literatür araştırmalarında en fazla tercih edilen iki adli bilişim aracının, **ticari bir yazılım olan MAGNET AXIOM**, **açık kaynak kodlu SQLite** (SQLite Expert, SQLite Viewer vb.) aracı olduğu belirlenmiştir.

Bulgular, literatürde ticari araçların açık kaynak kodlu araçlara kıyasla daha yaygın biçimde kullanıldığını, ancak açık kaynaklı **AUTOPSY** yazılımının da araştırmalarda önemli bir kullanım oranına sahip olduğunu göstermektedir.

En dikkat çeken bulgu ise, inceleme sürecinde veri bütünlüğünün korunmasına yönelik gerçekleştirilen **HASH** işlemlerinin (SHA256sum, MD5, SHA1) yalnızca iki çalışmada gözlemlenmesidir (Patel ve Mann, 2024; Sudiana vd.., 2024).

Aşağıda literatür araştırmalarında kullanılan adli bilişim araçlarının işletim sistemlerine göre sınıflandırılması verilmiştir. Üstte yer alan işletim sistemi ve araç ayrımı aşağıda detaylandırılacaktır.

Tablo3. Literatür araştırmalarında kullanılan yazılımların işletim sistemlerine göre sınıflandırılması

Yayın (Yıl)	Platform	Kullanılan Araçlar
Bays ve Karabiyik (2019)	iOS, Android	UFED, Magnet AXIOM
Knox, Moghadam, Patrick, Phan ve Choo (2020)	iOS, Android	MobileEdit, FTK, Autopsy, Fiddler, DB Browser for SQLite, MiXplorer, Bulk Extractor
Cheng, Shi, Gong ve Guan (2021)	Android	LogExtractor
Van Zandwijk ve Boztas (2021)	iOS	iMazing
Khalid, Iqbal, Kamoun, Khan ve Shah (2022)	Android	AccessData FTK Imager, Andriller, Autopsy, Volatility, ADB, RegEdit, DB Browser for SQLite, MiXplorer
Sumaila ve Bahsi (2022)	iOS, Android	Autopsy, Waze, GoFar, Veepeak OBDCheck, ZUS Smart Vehicle Monitor M
Bowling, Seigfried-Spellar, Karabiyik ve Rogers (2023)	iOS, Android	Magnet AXIOM, Cellebrite UFED 4PC, SQLite, Tableau Forensic USB 3.0 Bridge, ChromeCacheView
Fernández-Fuentes, Pena ve Cabaleiro (2023)	Android	AMD, AMExtractor, Lime, AVD
Murias, Levick ve McKeown (2023)	Android	Magnet AXIOM, Autopsy, Android Analyzer Ingest
Jennings, Sorell ve Espinosa (2023)	iOS	SQLite
Blankesteijn, Fukami ve Geradts (2023)	Android	UFED, CM2
Almuqren, Alsuwaelim, Rahman ve Ibrahim (2024)	Android	Andriller
Sudiana, Nuruddin, Rizkinia ve Husna (2024)	Android	SHA256sum, Hexdump, SQLite DB Browser, CherryTree, Android Debug Bridge, WhatsApp Key/Database Extractor, WhatsApp Crypt Tools
Çakır ve Karataş (2024)	iOS, Android	XRY, UFED, Oxygen Forensic

Yayın (Yıl)	Platform	Kullanılan Araçlar
Soni (2024)	-	SQLite Viewer, SQLite Expert, DB Browser for SQLite
Patel ve Mann (2024)	Android	MobileEdit, Magnet AXIOM, Balkasoft, MD5, SHA1
Nunes, Domingues ve Frade (2024)	Android	ADB, ALEAPP, DB Browser for SQLite
Soni, Kaur ve Aziz (2024)	Android	Magnet AXIOM, FTK Imager, OS Forensics
Stanković, Hu, Ozer ve Karabiyik (2024)	iOS, Android	Magnet AXIOM, Magnet Acquire, Magnet AXIOM Examine, GrayKey

Tablo 3 incelendiğinde; iOS ve Android işletim sistemlerine sahip mobil cihazlar için kullanılan araçlar arasında belirgin bir farklılaşma ve aynı zamanda bazı ortak eğilimler olduğu görülmektedir. Mobil adli bilişim araçları seçimi işletim sisteminin çok katmanlı yapısal özelliklerinin yanı sıra erişim kısıtlamalarına bağlı olarak şekillenmektedir.

Aşağıda işletim sistemlerine göre seçilen araçlara yönelik,

i. Android işletim sistemine sahip mobil cihazlar için tercih edilen araçlar
ii. İos için Tercih Edilen Araçlar
iii. Android ve iOS için Tercih Edilen Ortak Araçlar

olarak ayrım yapılmıştır.

i.Android işletim sistemine sahip mobil cihazlar için tercih edilen araçlar

Tablo3 'e göre Android cihazlar üzerinde sıklıkla tercih edilen adli bilişim araçları aşağıda yer almaktadır:

Android işletim sistemine yönelik adli bilişim çalışmalarında, veri elde etme ve analiz süreçlerinde en sık kullanılan araçlar arasında **Magnet AXIOM**, **SQLite , Autopsy**, **Cellebrite UFED**, **XRY**, **Andriller**, **Android Debug Bridge (ADB)**, **Wireshark**, **OSForensics** ve **CM2 (Infinity Chinese Miracle II)** yer almaktadır. Bu araçlar, cihazlardan **mantıksal, fiziksel ve dosya sistemi düzeyinde veri çıkarımı**, **uygulama kalıntılarının tespiti ve analizi**, **silinmiş verilerin kurtarılması** amacıyla kullanılmıştır.

Araştırmalar özelinde kullanılan araçlardan bahsedilecek olursa; **Bays ve Karabıyık (2019)** tarafından gerçekleştirilen araştırmada, **Cellebrite UFED** ve **Magnet AXIOM** araçları kullanılarak Life360 ve iSharing uygulamalarına ait **GPS koordinatları, kullanıcı kimlik bilgileri, mesaj içerikleri** ve **uygulama veritabanı kalıntıları** elde edilmiştir. Benzer şekilde **Knox vd. (2020)**, Happn uygulamasının adli analizinde **Packet Capture** aracını kullanarak ağ trafiğini izlemiş, **MOBILedit Forensic Express** ile iTunes yedeklerinden elde edilen verileri incelemiştir.

Cheng vd. (2021) tarafından geliştirilen **LogExtractor** aracı, Android cihazların sistem loglarından otomatik olarak delili tespit etme ve çıkarma sürecini optimize etmiş; bu kapsamda **cihaz kimliği, konum** gibi hassas bilgileri tespit etmiştir. **Murias vd. (2023)** ise

Twitch, Facebook, Reddit, Instagram ve YouTube Live uygulamalarını inceleyerek **Autopsy** aracıyla Android cihazlardaki kalıntıları analiz etmiştir.

Nunes vd. (2024) tarafından yürütülen çalışmada, altı farklı Android fitness uygulamasından **ADB** ve **DB Browser for SQLite** araçları kullanılarak **egzersiz kayıtları, konum ve sağlık bilgileri** çıkarılmıştır. **Almuqren vd. (2024)** ise **Andriller CE** aracının performansını değerlendirerek Android cihazlarda adli veri kurtarma süreçlerinin standardizasyonunu amaçlamıştır.

Genel olarak, Android ekosisteminde kullanılan adli araçların temel işlevi; **dosya sistemi düzeyinde veri elde etmek**, **uygulamalardan elde edilen verilerin analizini gerçekleştirmek** ve **şifreli veri tabanlarından anlamlı deliller elde etmektir.**

ii.İos için Tercih Edilen Araçlar

iOS işletim sistemine yönelik adli analizlerde sıklıkla kullanılan araçlar arasında, **Magnet AXIOM**, **Cellebrite UFED**, **XRY**, **MOBILedit Forensic Express**, **iTunes yedekleme altyapısı**, **GrayKey**, iMazing ve **DB Browser for SQLite** gibi yazılımlar yer almaktadır. Bu araçlar, iOS cihazlarda bulunan **kullanıcı etkinliklerinin, konum geçmişinin, sağlık verilerinin ve uygulama kalıntılarının** çıkarılması amacıyla kullanılmaktadır.

Araştırmalar özelinde kullanılan araçlardan bahsedilecek olursa; **Bays ve Karabıyık (2019)** çalışmasında, iOS cihazlardan elde edilen Life360 ve iSharing uygulama veritabanları (**L360Model.sqlite**, **iSharing.db**) üzerinde yapılan incelemeler sonucunda **konum, kişi bilgileri ve parola verileri** tespit edilmiştir. **Knox vd. (2020)** ise iOS cihazlarda Happn uygulamasının analizini gerçekleştirmiş; **MOBILedit** ile mantıksal yedeklerden kullanıcı verilerini çıkarmıştır.

Zandwijk vd. (2021) tarafından yürütülen araştırmada, iPhone cihazlarda **WhatsApp log dosyaları analizi** yapılmıştır. **Jennings vd. (2023)**, **Apple Health** verilerini inceleyerek **healthdb_secure.sqlite** veri tabanındaki egzersiz kayıtlarını elde etmiştir.

Stankovic vd. (2024), **GrayKey** aracını kullanarak cihazın **tam dosya sistemi görüntüsünü** elde etmiş ve bu imajı **Magnet AXIOM Examine** aracılığıyla analiz etmiştir. Çalışmada, **Oura Ring** verilerinin iOS cihazlarda adli olarak incelenebileceği sonucuna varılmıştır.

Bu bağlamda iOS çalışmalarında kullanılan araçların amacı, **adli veri elde etmek**, **sağlık, konum ve uygulama verilerini analiz etmek**tir.

iii.Android ve iOS için Tercih Edilen Ortak Araçlar

Birçok araştırma, hem Android hem de iOS işletim sistemlerinde gerçekleştirilen adli incelemeleri karşılaştırmalı olarak ele almıştır. Bu kapsamda, **Cellebrite UFED**, **Magnet AXIOM**, **XRY**, **MOBILedit**, **Autopsy**, **Wireshark** ve **iLEAPP/ALEAPP** gibi araçlar her iki platformda da yaygın biçimde kullanılmıştır.

Bays vd. (2019) ve **Knox vd. (2020)** çalışmalarında, her iki işletim sisteminde de **Cellebrite UFED**, **Magnet AXIOM** ve **MOBILedit** kullanılarak **konum, mesaj ve ağ trafiği** verileri analiz edilmiştir. **Bowling vd. (2023)**, Microsoft Teams uygulamasını Android ve iOS

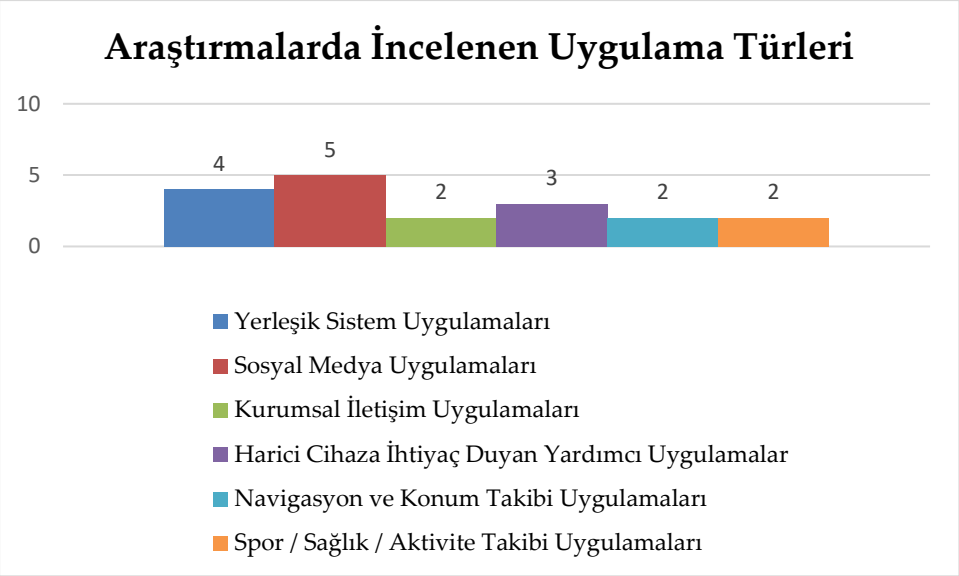
cihazlarda incelemiş; **Cellebrite UFED** ve **Magnet AXIOM Examine** araçlarıyla **uygulama veritabanlarını, önbellek kalıntılarını** karşılaştırmıştır.

Çakır ve Karataş (2024), Android ve iOS cihazlarda sosyal medya uygulamalarının analizini gerçekleştirerek **Cellebrite UFED**, **XRY** ve **Oxygen Forensic Suite** araçlarının performanslarını değerlendirmiştir. Çalışma sonuçları, **Cellebrite UFED**'in her iki platformda da **silinmiş verilerin kurtarılması** açısından en başarılı araç olduğunu göstermiştir. Benzer şekilde **Sudiana vd. (2024)**, WhatsApp uygulamasında kaybolan mesajların kurtarılabilirliğini incelemiş; Android ve iOS cihazlarda **Cellebrite UFED** ve **XRY** kullanarak karşılaştırmalı testler yürütmüştür. Elde edilen bulgular, **Cellebrite** aracının mesajların %75'ine kadarını kurtarabildiğini, önerilen yeni yöntemin ise **%83,33 başarı oranı** ile kök erişimi gerektirmeden veri kurtarabildiğini ortaya koymuştur.

Nunes vd. (2024) tarafından geliştirilen **ALEAPP** modülleri, Android uygulama analizine uyarlanmış; bu araç ailesinin iOS versiyonu olan **iLEAPP** ise **Jennings vd. (2023)** tarafından sağlık verisi analizlerinde kullanılmıştır. Bu durum, aynı araç ailesinin her iki işletim sisteminde **benzer yapılar üzerinde uyumlu biçimde çalışabildiğini** göstermektedir.

Android ve iOS platformlarını birlikte ele alan araştırmalarda, veri inceleme araçları, mantıksal ve fiziksel veri çıkarımı yöntemleri, silinmiş içeriklerin kurtarılması teknikleri ve uygulama veri tabanlarının çözümlemesi, karşılaştırma amacıyla kullanılmıştır.

RQ5: Literatür araştırmalarında incelenen uygulama türleri nelerdir?



Şekil 7: Literatür araştırmalarında incelenen yapılar

Literatür araştırmalarında, özellikle ele alınan mobil cihaz uygulama türleri incelenmiş; öne çıkan yönelimler altı ana tema altında değerlendirilmiştir. Şekil 7 literatür araştırmalarında ele alınan mobil uygulama türlerini göstermektedir. Şekil incelendiğinde literatürde sosyal medya uygulamaları ve yerleşik sistem uygulamalarının özellikle ön plana çıktığı gözlemlenmektedir.

Aşağıda her bir kategoriye ilişkin tanımlar ve örnekler sunulmaktadır.

- Yerleşik Sistem Uygulamaları ile telefonda hali hazırda yüklü olarak gelen uygulamalar kast edilmiştir. Örneğin, SMS uygulaması, kamera, takvim, e-posta uygulaması, dosya yöneticisi…vb
- Sosyal Medya Uygulamaları ile günümüzde yoğun bir şekilde kullanılan örneğin Facebook, Instagram, Twitter, TikTok,WhatsApp…vb gibi uygulamalar belirtilmiştir.
- Kurumsal İletişim Uygulamaları ile Örneğin Microsoft Teams, Cisco Webex, Google Meet …vb ifade edilmiştir.
- Harici Cihaza İhtiyaç Duyan Yardımcı Uygulamalar ile kastedilen uygulamalar, mobil cihazın dışındaki başka bir donanım ile etkileşim kurmak üzere tasarlanmıştır.
- Navigasyon ve Konum Takibi Uygulamaları konum ve navigasyon amaçlı kullanılan uygulamalardır. Google Maps, Waze, Apple Maps, Strava örnek olarak gösterilebilir.
- Spor / Sağlık / Aktivite Takibi Uygulamaları Spor-etkinlik takibi amacıyla kullanılan uygulamalardır. Fitbit, Apple Health, örnek olarak gösterilebilir.

Uygulama türlerine ilişkin ana tablo sunulduktan sonra, her uygulama türüne ait tablolar ayrı olarak verilmiştir. Böylelikle, her defasında ana tabloya dönme gereksinimi ortadan kaldırılmıştır.

Aşağıda literatür araştırmalarında tercih edilen uygulama türlerine ait genel tablo verilmiştir.

Tablo 4: Literatür araştırmalarında tercih edilen uygulama türleri

Uygulama Türü	Yazarlar ve Yıl	İncelenen Uygulamalar
Yerleşik Sistem Uygulamaları	Cheng, Shi, Gong ve Guan (2021)	Android log mesajları
	Van Zandwijk ve Boztas (2021)	iPhone hareket ve aktivite kayıtları
	Blankesteijn, Fukami ve Geradts (2023)	Mobil cihaz sistemi
	Fernández-Fuentes, Pena ve Cabaleiro (2023)	Web Tarayıcıları
	Patel ve Mann (2024)	Mobil cihaz depolama verileri
Sosyal Medya Uygulamaları	Knox, Moghadam, Patrick, Phan ve Choo (2020)	Happn
	Murias, Levick ve McKeown (2023)	Video Akış Platformları(Twitch, Instagram, Periscope...vb)
	Sudiana, Nuruddin, Rizkinia ve Husna (2024)	WhatsApp
	Çakır ve Karataş (2024)	Facebook, Instagram, Twitter, TikTok
	Soni (2024)	WhatsApp
Kurumsal İletişim Uygulamaları	Bowling, Seigfried-Spellar, Karabiyik ve Rogers (2023)	Microsoft Teams
	Khalid, Iqbal, Kamoun, Khan ve Shah (2023)	Cisco WebEx

Uygulama Türü	Yazarlar ve Yıl	İncelenen Uygulamalar
	Soni, Kaur ve Aziz (2024)	TeamViewer
Harici Cihaza İhtiyaç Duyan Yardımcı Uygulamalar	Sumaila ve Bahsi (2022)	OBDCheck, ZUS Smart Vehicle Monitor
	Stanković, Hu, Ozer ve Karabiyik (2024)	Oura Ring Gen 3
Navigasyon ve Konum Takibi Uygulamaları	Bays ve Karabıyık (2019)	Google Maps, Apple Maps, Waze
Spor / Sağlık / Aktivite Takibi Uygulamaları	Jennings, Sorell ve Espinosa (2023)	Apple Health
	Nunes, Domingues ve Frade (2024)	Fitbit, Android Running/Workout Apps

i. Yerleşik Sistem Uygulamaları

Yerleşik sistem uygulamaları, mobil cihazların temel işlevlerini ve sistem loglarını analiz ederek veri toplama ve sınıflandırma yöntemlerini araştırmaktadır.

Cheng vd. (2021), Android log verilerinin toplanması ve analiz edilmesi yoluyla cihaz aktivitelerinin detaylı şekilde izlenebileceğini göstermiştir. Geliştirilen araç sayesinde, yüksek doğruluk ve hassasiyet ile delil çıkarımı gerçekleştirilmiştir.

Van Zandwijk ve Boztas (2021) Iphone sensörleri üzerinden kullanıcı aktivite verilerini incelemiştir. Çalışma sonucunda, dijital izlerin, telefon kullanım durumu ve cihazın modeline bağlı olarak değişkenlik gösterdiğini, bunun yanı sıra, hareket tespitinde başlangıç ve bitiş zamanlarının yürüyüş, koşu ve sürüş için doğruluğunun değiştiğini tespit etmişlerdir.

Blankesteijn vd. (2023) modern Android sürümlerinde fabrika ayarlarına döndürülen bir cihazda yer alan kullanıcı verilerine erişimin neredeyse imkânsız hale geldiğini ve veri güvenliğinin önceki sürümlere kıyasla önemli ölçüde arttığını(Örneğin cihazdaki, şifreleme anahtarları desen vb. geri döndürülememiştir.) tespit etmişlerdir.

Fernández-Fuentes vd. (2023) Web tarayıcılarında gerçekleştirilen özel mod kullanımı ve bu kullanımın veri gizliliğine etkilerini incelemiştir. Tarayacılarda özel modun ne ölçüde gizlilik sağlayacağının tespiti araştırmanın ana amacıdır. Araştırma sonuçlarına göre, Mozilla Firefox en az iz bırakırken en fazla Google Chrome iz bırakmaktadır.

Patel ve Mann (2024) Depolama verilerini analiz ederek sistem etkinliğini sistematik literatür çalışmalarıyla ortaya koymuşlardır. Mobil adli bilişim alanında Android ve iOS cihazlardan veri toplama, analiz ve raporlama süreçlerini incelemiş mantıksal ve fiziksel yedekleme yöntemleriyle **cihaz içi uygulama verilerini** elde etmiştir.

Yerleşik sistem uygulamaları, cihaz içi aktivitelerin ayrıntılı şekilde izlenmesini sağlayarak kullanıcı davranışlarını anlamlandırmakta adli bilişim inceleme süreci içerisinde önemli bir veri kaynağı sunmaktadır.

Tablo: Literatür araştırmalarında yerleşik sistem uygulamaları

Yazarlar ve Yıl	İncelenen Uygulamalar	Açıklama
Cheng, Shi, Gong ve Guan (2021)	Android Log Mesajları	Android işletim sistemindeki log mesajları üzerinden veri çıkarımı yapılmıştır.
Van Zandwijk ve Boztas (2021)	iPhone hareket ve aktivite kayıtları	iOS cihazlarda hareket, yürüme, sürüş gibi aktivitelere ait dijital izlerin tespiti amaçlanmıştır.
Blankesteijn, Fukami ve Geradts (2023)	Mobil cihaz sistemi	Fabrika ayarlarına döndürme sonrası hangi verilere ulaşılabileceği test edilmiştir.
Fernández-Fuentes, Pena ve Cabaleiro (2023)	Android Tarayıcı Özel Modu	Gizli modda yapılan internet gezintilerinde kalan dijital izler incelenmiştir.
Patel ve Mann (2024)	Mobil sistem fonksiyonları,	Mobil adli bilişimde kullanılan araçlar, süreçler sistematik biçimde incelenmiştir.

ii. Sosyal Medya Uygulamaları

Knox vd. (2020), Happn flört uygulamasında hem iOS hem de Android cihazlarda yapılan adli inceleme, kullanıcıların konum, mesaj, profil bilgileri ve etkileşim geçmişi gibi hassas verilerinin uygulama ve ağ trafiği üzerinden kolayca açığa çıkarılabileceğini göstermiştir.

Murias, Levick ve McKeown (2023) Android uygulamalarında (Twitch, Facebook, Reddit, Instagram, Periscope) video akışlarının adli incelemesini yapmıştır. Araştırma bulgularına göre; Android video akış uygulamaları, adli incelemeye çok az veri bırakmakta ve önbellek temizleme işlemi adli izleri büyük ölçüde ortadan kaldırmaktadır.

Sudiana, Nuruddin, Rizkinia ve Husna (2024) WhatsApp mesaj silme ve veri kurtarma süreçlerinin analizini yapmıştır. Araştırma, kök erişimi olmadan yapılan WhatsApp mobil adli bilişim incelemelerinde kaybolan mesajların %83,33'ünün yedek dosyalar ve bildirim günlüğü kullanılarak kurtarılabildiğini göstermiştir.

Çakır ve Karataş (2024) Facebook, Instagram, Twitter, TikTok gibi platformlar arası veri işleme farklılıklarını analiz etmenin yanı sıra, **Android** işletim sistemine sahip cihazlarda veri çıkarımının daha geniş çapta gerçekleştirilebildiği, buna karşılık **iOS** işletim sistemine sahip cihazlarda veri erişiminin daha sınırlı olduğunu tespit etmiştir.

Soni (2024), WhatsApp'a yönelik adli bilişim süreçlerini inceleyen uzmanların karşılaşabileceği zorluklara odaklanmış ve WhatsApp verilerinin, kullanıcılar tarafından silinmesi, kaybolan mesajlar özelliği ve cihazın sıfırlanması gibi durumlar nedeniyle uçucu olduğuna dair tespitlerde bulunmuştur.

Sosyal medya uygulamaları, kullanıcı davranışlarını anlamada ve suça kanıt olabilecek delilleri tespit etmede adli bilişim için önemli bir inceleme alanıdır.

Tablo 6: Literatür araştırmalarında sosyal medya uygulamaları

Yazarlar ve Yıl	İncelenen Uygulamalar	Açıklama
Knox, Moghadam, Patrick, Phan ve Choo (2020)	Happn (flört uygulaması)	Android ve iOS platformlarında Happn uygulamasından elde edilen kişisel veriler analiz edilmiştir.
Murias, Levick ve McKeown (2023)	Video Akış Platformları(Twitch, Instagram, Periscope...vb)	Akış platformlarının veri saklama yöntemleri, video akış uygulamalarının adli incelemesi gerçekleştirilmiştir.
Sudiana, Nuruddin, Rizkinia ve Husna (2024)	WhatsApp	Silinen mesajların geri getirilebilirliği test edilmiştir.
Çakır ve Karataş (2024)	Facebook, Instagram, Twitter, TikTok	Sosyal medya uygulamaları arasında adli veri çıkarım araçlarının başarı oranları karşılaştırılmıştır.
Soni (2024)	WhatsApp	WhatsApp verilerinin adli bilişim açısından analizi ve karşılaşılan zorluklar incelenmiştir.

iii. Kurumsal İletişim Uygulamaları

Bowling, Seigfried-Spellar, Karabiyik ve Rogers (2023) Microsoft Teams'in Windows, iOS ve Android kalıntılarını incelediğinde, manuel incelemenin(%77.6), adli yazılımlara(%13.8) göre çok daha etkili olduğu, kullanıcı aktivitelerinin platforma bağımlı olduğu sonucuna ulaşmışlardır.

Khalid, Iqbal, Kamoun, Khan ve Shah (2023), Cisco WebEx'in masaüstü, web ve Android uygulamaları üzerinde yapılan adli analiz, bellek, disk ve ağ kaynaklarından kullanıcı kimlik bilgileri, sohbet ve medya içerikleri, toplantı detayları, şifreler ve zaman damgaları gibi dijital delillerin çıkarılabileceğini göstermiştir.

Soni, Kaur ve Aziz (2024) TeamViewer, Uzaktan erişim uygulamalarının performansı ve güvenliğini incelemiştir. Disk analizi sayesinde TeamViewer' a yönelik log dosyaları, yapılandırma ayarları ve geçici dosyalardan kullanıcı aktiviteleri ve zaman haritalandırılmasının yapılabileceğini bulmuşlardır.

Kurumsal iletişim uygulamaları, kullanıcı kimlik bilgileri, sohbet ve medya içerikleri, toplantı detayları, şifreler, log dosyaları, yapılandırma ayarları ve zaman damgaları gibi verileri sağlayarak adli soruşturmalarda delil niteliği taşıyabilecek kritik bilgiler sunabilmektedir.

Tablo 7: Literatür araştırmalarında kurumsal iletişim uygulamaları

Yazarlar ve Yıl	İncelenen Uygulamalar	Açıklama
Bowling, Seigfried-Spellar, Karabiyik ve Rogers (2023)	Microsoft Teams	Mesaj, dosya paylaşımı ve takvim etkinlikleri gibi verilerin adli incelemesi yapılmıştır.
Khalid, Iqbal, Kamoun, Khan ve Shah (2023)	Cisco WebEx	Android platformunda oturum logları, kullanıcı hesapları ve medya paylaşımları analiz edilmiştir.
Soni, Kaur ve Aziz (2024)	TeamViewer	Farklı platformlarda TeamViewer log dosyalarının adli açıdan içeriği incelenmiştir.

iv. Harici Cihaza İhtiyaç Duyan Yardımcı Uygulamalar

Mobil cihaz haricinde çalışan ve bu cihazlarla senkronize olarak veri toplayan uygulamalardır. Akıllı saatler, akıllı yüzükler ve fitness bileklikleri bu grubun içerisinde yer almaktadır. Harici cihazlarla entegre çalışan uygulamalar, kullanıcıların sağlık ve araç verilerini izleyip analiz etmektedir.

Sumaila ve Bahsi (2022) araç performans verilerini analiz etmiştir. Çalışma, GoFar'ın en zengin veri setine sahip olduğunu vurgulamaktadır. Mantıksal çıkarım teknikleri, GPS, VIN, hız ve seyahat bilgilerini güvenilir biçimde elde etmek için kritiktir sonucuna ulaşılmıştır.

Stanković, Hu, Ozer ve Karabiyik (2024) Giyilebilir cihazlar üzerinden sağlık ve aktivite takibi yapmıştır. Android ve iOS cihazlarda %80 oranında aktivite verisi, kalp atış hızı, uyku ve kullanıcı bilgilerinin adli soruşturmalarda kanıt olabileceğini vurgulamıştır.

Harici cihazlarla senkronize çalışan yardımcı uygulamalar, kullanıcıların sağlık durumu, aktivite seviyeleri, uyku düzeni, kalp atış hızı ve araç kullanım verileri gibi bilgilerini izleyip analiz ederek adli bilişim incelemelerinde değerli veriler sağlayabilmektedir.

Tablo 8: Literatür araştırmalarında Harici Cihaza İhtiyaç Duyan Yardımcı Uygulamalar

Yazarlar ve Yıl	İncelenen Uygulamalar	Kısa Açıklama
Sumaila ve Bahsi (2022)	OBDCheck, ZUS Smart Vehicle Monitor M, GoFar	Araç bakım uygulamalarından elde edilebilen GPS ve araç kimlik (VIN) verileri analiz edilmiştir.
Stanković, Hu, Ozer ve Karabiyik (2024)	Oura Ring Gen 3	Akıllı yüzükten toplanan sağlık, uyku ve aktivite

Yazarlar ve Yıl	İncelenen Uygulamalar	Kısa Açıklama
		verilerinin iOS, Android ve bulut ortamındaki izleri incelenmiştir.

v. Navigasyon ve Konum Takibi Uygulamaları

Bays ve Karabıyık (2019) Google Maps, Apple Maps, Waze: konum tabanlı uygulamalarda veri kullanımını incelemiştir. *"Elde edilen veri miktarı **işletim sistemi ve cihazın tam dosya sistemine erişim durumuna** bağlıdır."* sonucuna ulaşmışlardır.

Navigasyon uygulamalarına ait kullanıcı konum verileri, yönlendirme ve davranış analizine yönelik bilgiler sağlayarak adli bilişim incelemelerinde değerli veriler sunabilmektedir.

Tablo 9: Literatür araştırmalarında navigasyon ve konum takibi uygulamaları

Yazarlar ve Yıl	İncelenen Uygulamalar	Açıklama
Bays ve Karabıyık (2019)	Google Maps, Waze, Apple Maps	Konum paylaşım uygulamalarındaki GPS verilerinin tespiti yapılmıştır.

vi. Spor / Sağlık / Aktivite Takibi Uygulamaları

Jennings, Sorell ve Espinosa (2023) Apple Health, veritabanından konum bilgisi çıkarılabileceğini ve soruşturmalarda destekleyici delil niteliği taşıyabileceği; bunun yanı sıra GPS doğruluğunun değişken olduğu sonucuna ulaşmışlardır.

Nunes, Domingues ve Frade (2024) Fitbit, Android Running/Workout Apps,Koşu ve aktivite takibi için veri analizi gerçekleştirmiştir. Veri tabanları ve dosya formatlarını inceleyerek GPS, zaman damgası ve aktivite verilerini çıkarabilen modül oluşturmuşlardır.

Sağlık ve spor uygulamalarına ait GPS konumu, zaman damgaları ve aktivite verileri, adli bilişim incelemelerinde kullanıcıya ilişkin değerli bilgiler sağlayabilmektedir.

Tablo 10: Literatür araştırmalarında spor, sağlık ve aktivite takibi uygulamaları

Yazarlar ve Yıl	İncelenen Uygulamalar	Açıklama
Jennings, Sorell ve Espinosa (2023)	Apple Health	Apple Watch ve iPhone üzerinden elde edilen konum ve sağlık verilerinin doğruluğu analiz edilmiştir.
Nunes, Dominguesve Frade (2024)	Android Running/Workout Apps, Fitbit	Koşu uygulamalarında GPS ve zaman damgaları gibi dijital izlerin adli olarak kullanılabilirliği değerlendirilmiştir.

4. TARTIŞMA

Bu bölümde, mobil adli bilişim alanında Android ve iOS platformları arasındaki farklar, kullanılan adli araçlar ile veri elde etme yöntemleri ve uygulama türlerine göre gerçekleştirilen analizler değerlendirilmektedir.

Mobil adli bilişim çalışmalarında, Android ve iOS işletim sistemleri arasında belirgin farklar gözlemlenmektedir. Analizler, Android cihazların açık kaynaklı yapısı sayesinde adli araç çeşitliliği açısından daha avantajlı olduğunu göstermektedir (Cheng, Shi, Gong ve Guan, 2021; Nunes, Domingues ve Frade, 2024). Tablo 3'te de görüldüğü üzere, Magnet AXIOM, Autopsy, Cellebrite UFED, XRY ve Andriller gibi araçlar Android platformunda yaygın olarak kullanılmakta; veri çıkarımı ile uygulama verilerinin analizi gibi kritik adli süreçlerin yürütülmesini sağlamaktadır (Bays ve Karabıyık., 2019; Knox vd., 2020). Örneğin, Bays ve Karabıyık (2019) tarafından Samsung Galaxy S7 üzerinde yapılan çalışmada, Life360 ve iSharing uygulamalarına ait GPS koordinatları, kullanıcı kimlik bilgileri ve mesaj içeriklerinin bu araçlar aracılığıyla başarıyla elde edilebildiği raporlanmıştır. Bu durum, Android cihazların esnek yapısının adli veri toplama süreçlerini desteklediğini ve analiz süreçlerinde avantaj sağladığını ortaya koymaktadır. Buna karşın iOS cihazları, kapalı kaynak mimarisi ve katı güvenlik katmanları nedeniyle sınırlı araç desteğine sahiptir ve adli analizlerde genellikle ticari yazılımlar tercih edilmektedir (Van Zandwijk ve Boztas, 2021; Stanković vd., 2024). Örneğin, Zandwijk vd. (2021) tarafından gerçekleştirilen çalışmada, iPhone cihazlardaki WhatsApp logları ve sağlık veritabanları incelenerek kullanıcı hareketleri ortaya çıkarılmıştır. Jennings vd. (2023), Apple Health veritabanındaki egzersiz kayıtları ve sağlık verilerinin delil potansiyeli taşıdığını vurgulamıştır.

Her iki işletim sistemi için ortak kullanılan araçlar da bulunmaktadır. Magnet AXIOM, Cellebrite UFED,XRY, MOBILedit gibi araçlar, hem Android hem de iOS platformlarında mantıksal ve fiziksel veri çıkarımı, silinmiş içeriklerin kurtarılması ve uygulama veritabanlarının çözümlemesi amacıyla yaygın şekilde kullanılmıştır (Bays ve Karabıyık., 2019; Knox vd., 2020; Çakır ve Karataş., 2024). Sudiana vd. (2024), WhatsApp uygulamasında kaybolan mesajların kurtarılabilirliğini değerlendirerek, bu araçların platformlar arası karşılaştırmalı veri analizinde güvenilir sonuçlar sunduğunu ortaya koymuştur.

Tüm bunların dışında veri çıkarım ve analiz süreçlerinde veri bütünlüğünün korunmasına yönelik HASH (SHA256sum, MD5, SHA1) işlemlerine yalnızca iki çalışmada rastlanmıştır (Sudiana vd., 2024; Patel ve Mann, 2024). Bu tür bilgilerin diğer çalışmalarda yer almaması, elde edilen bulguların geçerliliğini ve güvenilirliğini riske atmaktadır ve literatürde önemli bir boşluk olarak değerlendirilmiştir.

Gerçekleştirilen çalışmalar uygulama türüne göre incelendiğinde, yerleşik sistem uygulamaları, sosyal medya uygulamaları, kurumsal iletişim uygulamaları, harici cihaz destekli yardımcı uygulamalar, navigasyon/konum takibi ve spor/sağlık uygulamaları öne çıkmaktadır. Yerleşik uygulamalarda, sistem logları ve cihaza ait aktiviteler, kullanıcı

hareketlerinin ve cihaz performansının anlaşılmasında kritik veriler sunmaktadır (Cheng vd., 2021; Patel ve Mann, 2024).

Uygulama türlerine göre yapılan incelemelerde, sosyal medya uygulamaları (özellikle WhatsApp) yaygın olarak tercih edilmiştir. WhatsApp'ın sunduğu kaybolan mesajlar, veri kurtarma sürecinde önemli zorluklar yaratmakta ve UFED ile XRY gibi araçların performansı değişkenlik göstermektedir. Sosyal medya uygulamaları kullanıcı iletişimi ve veri güvenliği açısından değerlidir; Knox vd. (2020) ve Çakır ve Karataş (2024) sosyal medya platformlarında veri çıkarım yöntemlerini karşılaştırmalı olarak incelemişlerdir.

Kurumsal iletişim uygulamalarında ise, Bowling vd. (2023) ve Khalid vd. (2023) mesaj, dosya paylaşımı ve toplantı verilerinin adli olarak analiz edilmesinin, süreçlerin güvenliği ve etkinliği açısından önemli olduğunu göstermiştir.

Harici cihazlarla entegre çalışan uygulamalar, mobil cihaz ve IoT cihazları arasındaki veri akışını analiz ederek kullanıcıların sağlık ve araç performans verilerini değerlendirmede kritik rol oynamaktadır (Sumaila ve Bahsi, 2022; Stanković vd., 2024).

Benzer şekilde, navigasyon ve konum takibi uygulamaları kullanıcı aktivitelerinin izlenmesi ve destekleyici delil niteliğinde değerli veriler sunarken (Bays ve Karabıyık, 2019), spor/sağlık takip uygulamaları sağlık ve egzersiz verilerinin adli olarak analiz edilmesine olanak tanımaktadır (Jennings vd., 2023; Nunes vd., 2024).

Sonuç olarak, mobil adli bilişimde işletim sistemi ve uygulama türüne göre araç seçimi kritik bir öneme sahiptir. Android cihazların esnek yapısı geniş araç desteği sağlarken, iOS cihazları daha sınırlı ve ticari araçlar üzerinden veri analizi imkânı sunmaktadır. Yerleşik sistemlerden sosyal medya, kurumsal ve sağlık uygulamalarına kadar farklı kategorilerde gerçekleştirilen analizler, kullanıcı davranışlarını, veri güvenliğini ve cihaz performansını değerlendirmede önemli bulgular sağlamaktadır. Bu bağlamda, adli analiz süreçlerinde hem platform özellikleri hem de uygulama türlerinin dikkate alınması, veri bütünlüğü ve analiz başarısı açısından kritik bir strateji olarak öne çıkmaktadır.

SONUÇ

Bu bölümde, sistematik literatür taraması sonucunda elde edilen bulgular özetlenmiş ve mobil adli bilişim alanındaki genel eğilimler ile karşılaşılan zorluklar değerlendirilmiştir."

Sistematik literatür araştırmasında, son altı yılda yayınlanan 19 çalışma derinlemesine incelenmiştir. İncelenen araştırmalar, hızla değişen ve gelişen teknolojilerin yanı sıra cihaz modelleri, işletim sistemleri ve uygulama çeşitliliğinin mobil adli bilişim süreçlerini giderek daha karmaşık, yönetilmesi zor ve dinamik bir hâle getirdiğini ortaya koymaktadır.

Araştırmacıların tercih ettikleri işletim sistemleri incelendiğinde; iOS işletim sistemlerine sahip mobil cihazların kullanımının son yıllarda belirgin şekilde arttığı görülmektedir. Bu artış, kullanıcı sayılarındaki artış ve adli analiz gereksinimlerindeki değişimle ilişkilendirilebilir. Bununla birlikte Android cihazlar, daha erişilebilir olmaları ve dünya genelindeki yüksek pazar payları nedeniyle çalışmaların önemli bir kısmını oluşturmaktadır.

Araştırmalar, mobil adli bilişimde kullanılan araçların çeşitliliğini ortaya koymaktadır. Araç seçimi, cihazın işletim sistemine bağlı olarak değişmekte; iOS ve Android cihazlarda farklı yazılımlar etkinlik göstermektedir. Farklı cihaz ve işletim sistemleri, veri elde etme ve analiz süreçlerinde araç seçimini belirleyici kılmaktadır. Çoğu araştırmacı, tek bir araç yerine farklı araç kombinasyonlarını kullanarak veri bütünlüğünü artırmayı hedeflemektedir. 2019 sonrası yapılan çalışmalarda, Magnet AXIOM ve UFED araçlarının her iki işletim sistemi için standart hâle geldiği gözlenmiştir. Android analizlerinde Autopsy, ADB ve DB Browser gibi açık kaynak araçlar tercih edilirken, iOS cihazlarda GrayKey ve XRY gibi ticari araçlar daha sık kullanılmaktadır.

Araştırmacıların incelemeyi tercih ettiği mobil uygulama türleri açısından değerlendirildiğinde; giyilebilir cihazlar, fitness uygulamaları ve otomobil bakım uygulamaları yeni dijital delil kaynakları olarak ön plana çıkmaktadır. Ayrıca, mobil uygulamalar arasında sosyal medya uygulamaları önemli bir yer tutmakta, ancak Telegram ve Discord gibi popüler platformların literatürde yeterince incelenmediği ve bu alanda bir boşluk olduğu belirlenmiştir.

Son olarak, mobil cihazlarda kullanılan işletim sistemlerinin çeşitliliği, cihazların çok katmanlı yapısı ve kullanıcı arayüzlerindeki farklılıklar, adli bilişim inceleme sürecini yürüten kişiler için çok yönlü bilgi ve beceri gerektirmektedir. Bu süreçte, araştırmacıların elde edilen verileri analiz edebilmek için birden fazla adli bilişim aracına, tekniğe ve prosedüre hâkim olmaları gerekmektedir.

ÖNERİLER

Bu bölümde, gelecekte gerçekleştirilecek araştırmalar için öneriler sunulmaktadır:

- Mobil cihaz uygulamalarına düzenli olarak eklenen yeni özellikler, örneğin WhatsApp uygulamasının sunduğu süreli mesajlar, kritik delil niteliği taşıyabilir. Bu tür yeniliklerin takip edilmemesi, geri döndürülemez veri kayıplarına yol açabilir. Bu nedenle, adli bilişim süreçlerinin değişen teknolojileri yakından izleyen uzmanlar tarafından yürütülmesi önemlidir.
- Literatürde birçok mobil cihazın adli analizi gerçekleştirilmiş olmasına rağmen, aynı cihazın kök erişimi olan ve olmayan durumlarda veri edinimi karşılaştırılmış bir çalışma bulunmamaktadır. Bu bağlamda, söz konusu konu üzerine yapılacak araştırmalar literatüre önemli katkı sağlayabilir.
- Yapılan Araştırmaların büyük çoğunluğu akıllı telefonlar üzerine odaklanmıştır. Tabletler, akıllı saatler veya benzeri taşınabilir cihazlar yalnızca sınırlı sayıda çalışmada incelenmiştir. Günlük yaşamda yoğun olarak kullanılan bu cihazlar, dijital delil potansiyeli taşımaktadır. Bu nedenle, giyilebilir teknolojilerin adli analizi üzerine gerçekleştirilebilecek çalışmaların sayısının artırılması önerilmektedir.
- Sosyal medya uygulamaları üzerine odaklanan çalışmalar, bu alanın önemini göstermektedir. Bu kapsamda, sosyal medya uygulamaları üzerine yapılan araştırma sayısının artırılması önerilmektedir; örneğin Discord, Telegram gibi platformlar ele alınabilir.
- İncelenen araştırmaların bazılarında adli araçların veri çıkarım başarıları sayısal olarak ölçülmüş; buna karşın veri çıkarım süreleri üzerine bilgi

sunulmamıştır. Adli soruşturmaların zamana duyarlı doğası dikkate alındığında, gelecekte farklı araçların veri çıkarım sürelerini karşılaştıran araştırmaların yapılması önerilmektedir.

KAYNAKLAR

Almuqren, A., Alsuwaelim, H., Rahman, M. H., & Ibrahim, A. A. (2024). A systematic literature review on digital forensic investigation on Android devices. *Procedia Computer Science, 235*, 1332–1352.

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST Special Publication 800-101, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Bays, J., & Karabiyik, U. (2019, April). Forensic analysis of third party location applications in Android and iOS. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1–6). IEEE.

Blankesteijn, M. B., Fukami, A., & Geradts, Z. J. (2023). Assessing data remnants in modern smartphones after factory reset. *Forensic Science International: Digital Investigation, 46*, 301587. https://doi.org/10.1016/j.fsidi.2023.301587

Bowling, H., Seigfried-Spellar, K., Karabiyik, U., & Rogers, M. (2023). We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems. *Journal of Forensic Sciences, 68*(2), 434–460. https://doi.org/10.1007/s10207-024-00936-7

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Çakır, H., & Karataş, M. (2024). Analysis and comparison of social media applications using forensic software on mobile devices. *Journal of Forensic Science and Research, 8*(1).

Çakır, H., Kılıç, M., Bakan, M., & Saluk, A. (2014). *Mobil cihaz incelemelerinde kullanılan ekipmanlar*. In *Adli Bilişim ve Elektronik Deliller* (p. 238). Seçkin Yayıncılık.

Cheng, C. C. C., Shi, C., Gong, N. Z., & Guan, Y. (2021). LogExtractor: Extracting digital evidence from Android log messages via string and taint analysis. *Forensic Science International: Digital Investigation, 37*, 301193. https://doi.org/10.1016/j.fsidi.2021.301193

Fernández-Fuentes, X., Pena, T. F., & Cabaleiro, J. C. (2023). Digital forensic analysis of the private mode of browsers on Android. *Computers & Security, 134*, 103425. https://doi.org/10.1016/j.cose.2023.103425

Henkoğlu, T. (2014). Cep bilgisayarı/cep telefonu analizi neden ve nasıl yapılır? In *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (pp. 127–128). Pusula Yayıncılık.

Jennings, L., Sorell, M., & Espinosa, H. G. (2023). Interpreting the location data extracted from the Apple Health database. *Forensic Science International: Digital Investigation, 44*, 301504. https://doi.org/10.1016/j.fsidi.2023.301504

Jones, G. M., & Winster, S. G. (2017). Forensics analysis on smart phones using mobile forensics tools. *International Journal of Computational Intelligence Research, 13*(8), 1859–1869.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Khalid, Z., Iqbal, F., Kamoun, F., Khan, L. A., & Shah, B. (2022). Forensic investigation of Cisco WebEx desktop client, web, and Android smartphone applications. *Annals of Telecommunications, 78*(3), 183–208. https://doi.org/10.1007/s12243-022-00919-6

Knox, S., Moghadam, S., Patrick, K., Phan, A., & Choo, K. K. R. (2020). What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps. *Computers & Security, 94*, 101833. https://doi.org/10.1016/j.cose.2020.101833

Lessard, J., & Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. *Small Scale Digital Device Forensics Journal, 4*(1).

Murias, J. G., Levick, D., & McKeown, S. (2023). A forensic analysis of streaming platforms on Android OS. *Forensic Science International: Digital Investigation, 44*, 301485. https://doi.org/10.1016/j.fsidi.2022.301485

National Institute of Justice. (2007). *Electronic crime scene investigation: A guide for first responders* (2nd ed.).

Nunes, F., Domingues, P., & Frade, M. (2024). The digital footprints on the run: A forensic examination of Android running workout applications. *Future Internet, 16*(9), 304. https://doi.org/10.3390/fi16090304

Patel, B., & Mann, P. S. (2024). A survey on mobile digital forensic: Taxonomy, tools, and challenges. *Security & Privacy, 8*(2), 1–27. https://doi.org/10.1002/spy2.470

Soni, N. (2024). Forensic analysis of WhatsApp: A review of techniques, challenges, and future directions.

Soni, N., Kaur, M., & Aziz, K. (2024). Decoding digital interactions: An extensive study of TeamViewer's forensic artifacts across Windows and Android platforms. *Forensic Science International: Digital Investigation, 51*, 301838. https://doi.org/10.1016/j.fsidi.2024.301838

Statista. (2025, January 2). *Multiple mobile device ownership worldwide.* Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

Stanković, M., Hu, X., Ozer, A. A., & Karabiyik, U. (2024). How engaged are you? A forensic analysis of the Oura Ring Gen 3 application across iOS, Android, and cloud platforms. *International Journal of Information Security, 24*(1), 1–15. https://doi.org/10.1007/s10207-024-00936-7

10.5824/ajite.2025.04.008.x

Sudiana, D., Nuruddin, C. H., Rizkinia, M., & Husna, D. (2024). Forensic analysis of WhatsApp disappearing message on unrooted Android using mobile device forensics methodology NIST SP 800-101r1.

Sumaila, F., & Bahsi, H. (2022). Digital forensic analysis of mobile automotive maintenance applications. *Forensic Science International: Digital Investigation, 43*, 301440. https://doi.org/10.1016/j.fsidi.2022.301440

Van Zandwijk, J. P., & Boztas, A. (2021). The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones. *Forensic Science International: Digital Investigation, 37*, 301170. https://doi.org/10.1016/j.fsidi.2021.301170

Worldometers. (2025, January 2). *World population projections.* Worldometers. https://www.worldometers.info/world-population/world-population-projections/