Uluslararası Bilişim Sistemleri ve Uygulamaları Dergisi
International Journal of Information Systems and Applications

e-ISSN:3108-4303		https://dergipark.org.tr/pub/ubsud			
Araştırma Makalesi		Cilt No:	2	Sayı No:	1
Geliş Tarihi:	28.01.2026	Kabul Tarihi:	26.03.2026	Yayın Tarihi:	05.06.2026
DOI: 10.71340/ubsud.1874037					

WİNDOWS İŞLETİM SİSTEMİ KURULU BİLGİSAYARLARA BAĞLANAN MOBİL TELEFONLARIN ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Ali ÇETİN [1] Refik SAMET[2]

Özet

Bilişim ve iletişim alanında yaşanan yenilikler sayesinde hayatımıza giren teknolojik ürünlerin başında bilgisayar ve mobil cihazlar gelmektedir. Günümüzde bilgisayar ve mobil cihazlar birbirlerine kablolu ya da kablosuz olarak bağlanabilmekte ve birbirleri arasında sürekli bir veri alışverişi olmaktadır. Windows işletim sistemi, birçok mobil telefon ile uyumlu çalışmakta ve bu telefonların kablolu ya da kablosuz olarak bilgisayara bağlanması halinde yapılan işlemleri kayıt altına almakta ve ardında dijital izler bırakmaktadır. Bu dijital izler, gerek duyulduğunda Windows bünyesinde bulunan araçlar sayesinde incelenebileceği gibi harici bir adli bilişim aracı aracılığıyla da incelenebilmekte, delil elde etme ve analiz sürecinde önemli bir rol oynayabilmektedir. Bu çalışmada, farklı mobil işletim sistemlerine sahip (Android ve iOS) mobil telefonların USB bağlantı kablosu ve kablosuz bağlantı (Wi-Fi) aracılığıyla bilgisayara bağlanması durumunda Windows 11 işletim sistemi üzerinde bıraktıkları dijital izlerin, Windows Kayıt Defteri, Windows Olay Günlükleri kayıtları ve ilgili diğer yazılımlar (USBDeview, DCode, Access Data Registry Viewer vb.) kullanılarak tespit edilmesi amaçlanmıştır. Bu amaç kapsamında bir metodoloji önerilmiş, gerçek verilerle uygulamalar yapılmış, elde edilen sonuçlar değerlendirilmiş ve öneriler sunulmuştur.

Anahtar Kelimeler: Adli Bilişim, Kayıt Defteri, Windows Olay Günlükleri, Adli Bilişim Araçları.

DIGITAL FORENSICS ANALYSIS OF MOBILE PHONES CONNECTED TO COMPUTERS RUNNING WINDOWS OPERATING SYSTEMS

Abstract

Thanks to innovations in the field of information and communication technology, computers and mobile phones are among the leading technological products that have entered our lives. Today, computers and mobile devices can connect to each other via wired or wireless connections, and there is a constant exchange of data between them. The Windows operating system works compatibly with many mobile phones, and when these phones are connected to a computer via wired or wireless connection, it records the actions performed, leaving behind digital traces. These digital traces can be examined using tools within Windows, or through an external forensic tool, playing a significant role in the evidence gathering and analysis process. This study aims to detect the digital traces left on the Windows 11 operating system by mobile phones with different mobile operating systems (Android and iOS) if connected to a computer via USB cable and wireless connection (Wi-Fi), using Windows Registry, Windows Event Log records, and other relevant software (USBDeview, DCode, Access Data Registry Viewer, etc.). Within this scope, a methodology is proposed, applications are carried out with real data, the results obtained are evaluated, and recommendations are presented.

Keywords: Digital Forensics, Registry, Windows Event Logs, Digital Forensic Tools.

[1] Ankara Üniversitesi, Adli Bilimler Enstitüsü, Adli Bilişim Programı, alicetin3442@gmail.com, https://orcid.org/0009-0006-2586-7278

[2] Prof. Dr., Ankara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, samet@eng.ankara.edu.tr, https://orcid.org/0000-0001-8720-6834

1. GİRİŞ

Bilim ve teknolojide yaşanan gelişimler bilgisayarlar, ağlar, internet, akıllı evler, akıllı cihazlar, e-ticaret ve benzeri pek çok teknolojilerin gelişmesine ve bu teknolojilerin hayatımızın birçok alanında giderek daha fazla yer almasına yol açmıştır. İnsanlığın hizmetine sunulan bu teknolojiler günümüzde gelişimine devam etmekte ve gündelik hayatımızı kolaylaştırmaktadır. İletişim ve bilgi işlem teknolojilerinin kullanım alanlarının hızla genişlemesi, bu teknolojileri kullananların sayılarında hatırı sayılır bir artış yaşanmasına yol açmış ve suç işlemek isteyen kişilerin de dikkatlerini bu teknolojilerin üzerine çekmiştir. Bu teknolojilerin sunduğu imkân ve kabiliyetler aracılığıyla suç işlemek amacıyla çeşitli teknik ve yöntemler geliştirme çabası içerisine girmişlerdir (Uçar, 2021).

Geçmişte suç teşkil eden tüm eylemler fiziksel dünyamızda meydana gelirken, günümüzde bilgi işlem ve iletişim teknolojilerinin yaygınlaşmasıyla dijital mecralarda da suç eylemleri veya suça yönelik girişimlerin gerçekleştiği görülmektedir (Tekin, 2017). Bu açıdan, geleneksel adli delil toplama uygulama ve yöntemlerinin dijital ortamda da yapılabilmesi için yeni yöntemlerin geliştirilmesine yol açmıştır. Suç eylemlerin siber dünyaya taşınmasıyla birlikte, adli bilişim adlı yeni bir alan ortaya çıkmıştır. Adli bilişim, elektronik cihazların depolama alanlarında bulunan dijital verilerin toplanması, delil olarak sunulması ve raporlanmasıyla ilgili bir bilim dalıdır (Çakır ve Kılıç, 2013). Bu alandaki araştırmalar sonucunda ortaya konan teknikler, sadece suçun tespit edilmesine ve failin belirlenmesine yardımcı olmakla kalmaz, aynı zamanda suçlanan bireyin masum olması durumunda masumiyetinin kanıtlanmasına da katkı sağlar (Polis Akademisi, 2022)

Dijital adli bilişim, suça konu olan dijital materyallerin elde edilmesi ve incelenmesiyle ilgilenen bilim dalıdır ve geçmişi 1980'lerin sonlarına kadar gitmektedir. Dijital suçun artışı, emniyet teşkilatının soruşturmaların teknik yönlerini incelemek için farklı uzmanlığa sahip gruplar kurmasına yol açmıştır (Sommer, 2004). Elektronik aletlerin hızla artmasıyla, günümüzde ardında dijital iz bırakmayan bir suç eylemi tasarlamak ya da gerçekleştirmek oldukça zordur. Suçlular, suç işleme süreçlerini basitleştirmek ve yakalanmaktan kaçınmak amacıyla teknolojiyi kullanmakta, bu da kolluk kuvvetleri ile adli bilişim uzmanlarına yeni zorluklar meydana getirmektedir (Casey, 2011). Teknolojik aletlerin gelişmesiyle dijital adli bilim de ilerleme kaydetmiştir. Dijital suçlarla ilgili dijital cihaz türleri açısından bilgisayar adli bilimi, mobil adli bilimi, ağ adli bilimi ve bulut adli bilimi gibi ana dallara ayrılabilmektedir. Dijital adli süreç, bir suçun işlenip farkına varılmasının ardından başlar; genellikle bu süreç, hazırlık, potansiyel delillerin tespit edilmesi, ele geçirilmesi ve edinilmesi, analiz edilmesi ve bulguların raporlanması ya da sunulmasını kapsar (Đuranec, 2019).

Bu çalışmada; Windows 11 işletim sistemini kullanan bir bilgisayara USB aracılığıyla bağlanan bir mobil telefonun ve bir bilgisayarın Wi-Fi özelliği aracılığıyla birbirine kablosuz olarak bağlanan bir mobil telefonun Windows 11

işletim sistemi üzerinde bıraktıkları dijital izler araştırılmıştır. Windows işletim sisteminin içerisinde gömülü gelen Windows Kayıt Defteri, Windows Olay Günlükleri ve ilgili diğer ücretsiz yazılım ve donanım araçları vasıtasıyla adli bilişim süreç ve tekniklerine uygun bulguların nasıl elde edileceği araştırılmıştır.

1.1. Problem Durumu

MSC (Mass Storage Class), MTP (Media Transfer Protocol) ve PTP (Picture Transfer Protocol) protokollerinden herhangi birini kullanarak USB kablosu veya Wi-Fi bağlantısı ile bilgisayara bağlanan mobil telefonların Windows işletim sistemi üzerinde bıraktıkları dijital izlerin, Windows işletim sisteminin farklı sürümleri (Windows XP, Windows 7, Windows 8, Windows 10 gibi) için Windows Kayıt Defteri (Registry), Windows Olay Günlükleri ve ticari yazılımlar aracılığıyla incelendiği ancak 2021 yılında piyasaya sürülen Windows 11 işletim sistemi üzerinde konu ile ilgili henüz kapsamlı araştırmaların yapılmadığı belirlenmiştir. Bu boşluğun doldurulmasına katkı sağlamak amacıyla bu çalışmada bir metodoloji önerilmekte, gerçek verilerle uygulamalar yapılmakta, elde edilen sonuçlar değerlendirilmekte ve öneriler sunulmaktadır.

1.2. Amaçlar

Bu çalışmada, bilgisayarla USB kablosu aracılığıyla kablolu olarak bağlantı kuran iki farklı mobil işletim sistemine (Android ve iOS) sahip telefon ve kendi internetini Wi-Fi özelliği ile bir bilgisayarla paylaşan iki farklı telefonun, Windows 11 işletim sistemi kullanan bir bilgisayar üzerinde bıraktıkları dijital izlerin, Windows Kayıt Defteri, Windows Olay Günlükleri ve ilgili yazılım ve donanım araçları yardımıyla adli bilişim teknik ve süreçlerine uygun bir biçimde tespit edilmesi amaçlanmaktadır.

Makalenin 2. bölümünde çalışmaya konu ile ilgili literatür özetlenmiş, 3. bölümünde çalışmada kullanılan yönteme yer verilmiş, 4. bölümünde elde edilen bulgular sunulmuş ve yorumlar yapılmış, 5. bölümde ise sonuç ve tartışmalara yer verilmiş ve 6. bölümde ileriki çalışmalar için önerilerde bulunulmuştur.

2. LİTERATÜR TARAMASI

Bu bölümde, bilgisayara Wi-Fi ve USB kablosu yardımıyla bağlantı kurulduğunda Windows işletim sisteminde bıraktıkları dijital izlere ilişkin literatürde yer alan benzer çalışmalar incelenmiş ve özetlenmiştir.

Alghafli ve diğerlerinin gerçekleştirdiği araştırma, dijital delillerin saklama ortamlarından elde edilme sürecinin uzamasına işaret etmekte ve bu durumun davaların mahkemeye geç ulaşmasına yol açabileceğini belirtmektedir. Araştırmada, ilk dijital izlerin Windows işletim sistemindeki kayıt defterinden temin edilebileceği ifade edilmiştir. Araştırma, Windows 7 işletim sistemi ile sistem bilgileri, uygulama

bilgileri, bağlı ağlar (Wi-Fi ve kablolu ağlar), USB ve Wi-Fi aracılığıyla bağlı aygıtlar ve geçmiş listeleri gibi bilgilerin nasıl elde edileceğini ortaya koymaktadır. Elde edilen bu verilerin ve sonuçların, dijital delillere ulaşma sürecini hızlandırabileceği ve incelemeleri yönlendirebileceği belirtilmiştir (Alghafli vd., 2011).

Uçar (2021), Windows işletim sisteminin imajını alıp analiz eden araçların ücretli olmasının, incelemeleri yavaşlatabileceği ve engelleyebileceğini ifade etmiştir. Bu nedenle, açık kaynak yazılımlar veya işletim sisteminde mevcut olan uygulamalarla siber suçlarla ilişkili olayların adli bilişim incelemesinin gerçekleştirilebileceği belirtilmiştir. Bu çalışma, Windows işletim sisteminde tutulan kayıtların ve diğer izlerin nasıl toplanıp analiz edileceğini ve olayın zaman çizelgesinin nasıl hazırlanacağını açıklamaktadır.

Dweikat vd. (2021) teknolojinin ilerlemesiyle suçların yalnızca geleneksel yollarla sınırlı olmadığını, elektronik suçlara dönüştüğünü ifade etmiştir. Bu dönüşüm, suçluların belirlenmesi ve kanıt toplama aşamalarında adli bilişimde yeni elektronik araçlar ve uygulamalara olan ihtiyacı artırdığını vurgulamıştır. Araştırma, mevcut adli bilişim uzmanlarının erişimine sunulmuş pek çok ücretsiz ve ücretli uygulamayı analiz ederek bu uygulamaların artı ve eksi yönlerini karşılaştırmıştır. Bu şekilde, adli bilişimdeki araçların etkinliğini değerlendirerek, suçla mücadelede nasıl daha verimli bir şekilde kullanılabileceklerine dair önemli bilgiler sağlanmıştır. Çalışmada, teknolojinin suçlar üzerindeki etkisi üzerinde durulmuş ve adli bilişimin bu yeni suç türleriyle başa çıkabilmesi için atılması gereken önlemler ele alınmıştır.

Neyaz ve Shashidhar (2019) tarafından yapılan araştırmada, bir USB cihazının ürün kimliği, satıcının adı, seri numaraları ve yüklü sürücünün sürümü gibi bilgilere Windows Olay Günlüğü, Windows Kayıt Defteri ve dosya sistemi günlüğü inceleyerek nasıl ulaşılabileceği kapsamlı bir şekilde açıklanmıştır.

Arshad vd. (2017) Windows 8 işletim sistemi üzerinde USB cihazlarının bilgisayara ne kadar süreyle bağlı kaldığını tespit etmek için Windows Kayıt Defteri ve Windows Olay Günlükleri'nin kullanımını araştırmıştır. Araştırma, USB cihazlarının takılıp çıkarıldığı zamanların, belirli kayıt anahtarları ve olay kimlikleri vasıtasıyla takip edilebileceğini göstermektedir. Aynı zamanda, çeşitli türdeki USB cihazları için bu kayıtların da kullanılabileceği belirtilmektedir.

Kurtça ve Samet (2024), macOS işletim sistemini kullanan bir bilgisayara ağ bağlantısı yapan mobil telefonların MAC adresi kayıtlarını incelemiş, olası sorunları belirlemeye çalışmış ve bu sorunların çözüm yollarını araştırmıştır. Adli bilişim süreçlerinde, verilerin toplanması, analizi ve sonuçların değerlendirilmesi aşamalarında kullanılmak üzere bir metodoloji geliştirilmiştir. iOS ve Android işletim sistemine sahip mobil telefonlar, aynı bilgisayara farklı bağlantı yöntemleriyle bağlanarak on farklı uygulama gerçekleştirmiş ve bu çalışmada sunulan metodoloji doğrultusunda bulgular elde edilmiştir. Sonuçlar incelendiğinde, işletim sistemi kayıtlarında tespit edilen MAC adresi bilgilerinin farklılık

gösterebildiği, bağlantı türüne bağlı olarak sonucun değiştiği ve bir telefon için birden fazla MAC adres kaydının kayıtlarda tespit edildiği sonucuna ulaşılmıştır.

Arshad vd. (2017) tarafından yapılan kapsamlı çalışmada, MTP ve PTP protokolünü kullanan kablolu bağlantıya ilişkin cihaz tanıma ve sınıflandırma mantığının temelini Windows 7'den Windows 10'a kadar olan süreçte koruduğu görülmektedir. "DeviceClasses" altındaki GUID dizileri ve 0003, 0064, 0065 gibi temel USB Property Keys altında incelenen alt anahtarlar tüm Windows sürümlerinde istikrarlı şekilde tutulduğu görülmektedir. Ayrıca, cihazın sisteme en son ne zaman takıldığını gösteren "Last insertion time" kaydının her üç sürümde de (Windows 7,8 ve 10) yer alması, işletim sistemi değişse bile temel zaman damgalarının korunmaya devam ettiği tespitini yapmıştır. Diğer taraftan, Windows 7 ile daha güncel sürümler (Windows 8 ve 10) arasında belirgin bir farklılık olduğu belirtilmiştir. Windows 7, "USB Property Key" altında yer alan 0007, 0008, 0009, 000A ve 0066 gibi birçok alt anahtarını kayıt altına almazken, bu veriler Windows 8 ve 10 sürümlerinde tutulmaktadır. Adli bilişim açısından en kritik farklardan biri ise cihazın sistemden son çıkarılma zamanını gösteren 0067 alt anahtarı Windows 7'de bulunmazken, buna karşın diğer iki sürümde de (Windows 8 ve 10) yer almaktadır. Ayrıca Windows 10, "USB Key" altındaki belirli bir GUID dizinine (\e5b3b5ac-9725-4f78-963f-03dfb1d828c7) sahip ilk takılma zamanı kaydıyla Windows 7 ve 8 sürümünden de ayrışarak en spesifik veri takibini yapan sürüm olarak öne çıktığını belirtmiştir. Burada bahsedilen dijital izlere, Windows 11 işletim sistemi kullanan bir sistemde bu çalışmada önerilen metodoloji kapsamında ulaşılmaya çalışılmıştır. Literatür incelendiğinde dijital izlere ait elde edilen bulguların Windows 7, Windows 8 ve Windows 10'da farklılıkların ve benzerliklerin olduğu tespit edilmiştir.

Risto (2011) tarafından yapılan çalışmada, Wi-Fi kayıtlarının Windows 7 kayıt defteri üzerinde dijital izlerin nerede tutulduğu ve nasıl elde edildiği ayrıntılı bir şekilde sunulmaktadır. Windows 11 işletim sistemi kullanılan bu çalışmada, önerilen metodoloji takip edilerek kablosuz bağlantıya dair dijital izlere ulaşılmış ve elde edilen bulguların literatür ile tam uyumlu olduğu tespit edilmiştir.

Literatürdeki mevcut çalışmalar ağırlıklı olarak Windows'un eski sürümlerinde dijital izlerin incelenmesi ile ilgili olup Windows 11 işletim sistemiyle ilgili çalışmalara rastlanmamıştır. Bu boşluğu doldurmaya katkı sağlamak amacıyla bu çalışmada Windows 11 işletim sistemiyle çalışan bilgisayarlara kablolu ve/veya kablosuz bağlanan farklı mobil işletim sistemleri ile çalışan mobil telefonların bıraktıkları dijital izlerin incelenmesi, uygulamaların yapılması, sonuçların değerlendirilmesi ve önerilerde bulunulması hedeflenmektedir.

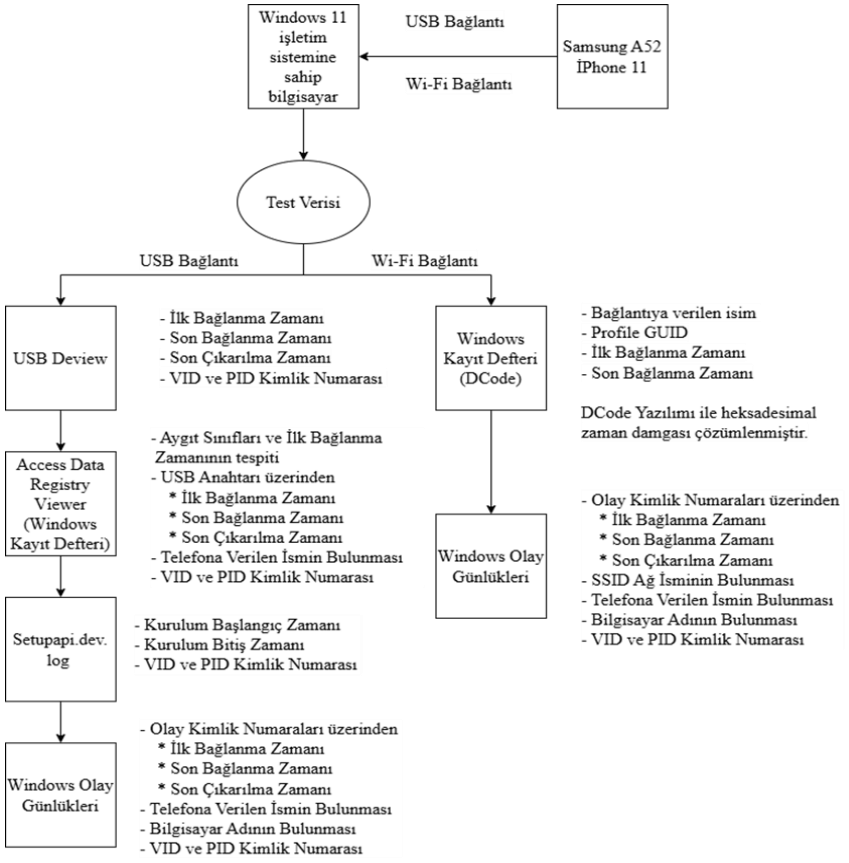
3. YÖNTEM

Bu bölüm, Windows 11 işletim sistemine USB ve Wi-Fi aracılığıyla bağlanan iki farklı mobil işletim sistemine sahip telefonların Windows 11 kayıtları üzerinde bıraktıkları dijital izlerin araştırılmasında kullanılan donanım ve yazılım araçları

hakkında bilgi sunarken izlenen yöntemi de açıklamaktadır. Mevcut adli bilişim yazılımlarının pahalı olması nedeniyle bu çalışmada ücretsiz yazılımların kullanılması hedeflenmektedir. Geçmişte bilgisayara bağlanmış ya da hâlâ bağlı olan tüm USB aygıtlarını listeleyebilen ücretsiz bir yardımcı yazılım aracı olan USBDeview (Nirsoft, t.y.), mobil cihazlarda heksadesimal sayı formatında tutulan tarih ve zaman verilerini çözümlemek için DCode (Digital Detective, t.y.) ve Windows Kayıt Defteri kayıtlarını görüntülemek için Access Data Registry Viewer (Accessdata, 2014) yazılım araçları tercih edilmiştir. Ayrıca, Windows işletim sisteminde halihazırda olan Windows Kayıt Defteri, Windows Olay Günlükleri ve Setupapi.dev.log metin günlüğü içeriğinde gerçekleştirilen bağlantıya dair dijital izlerin bulunması hedeflenmiştir.

Çalışma için Windows 11 Home 21H2 sürümünü kullanan bir bilgisayar ve Android OS 14. sürümünü kullanan Samsung Galaxy A52 mobil telefonu ile iOS 18.6.2 sürümünü kullanan Apple iPhone 11 mobil telefonu temin edilmiştir. Test verilerinin oluşturulması öncesinde bilgisayara daha önce takılan USB cihazlarının olup olmadığı USBDeview yazılım aracı ile kontrol edilmiş ve geçmiş bağlantılara dair bilgilerin ekran görüntüsü alınmıştır. Ayrıca bu mobil telefonlar USB ve Wi-Fi aracılığıyla bilgisayara bağlanmış ve bağlantıya dair zaman bilgileri kayıt altına alınarak test verileri oluşturulmuştur (Çetin, 2025).

Çalışma kapsamında belirtilen hedeflere ulaşabilmek için ihtiyaç duyulan araçlar ve bu araçlar ile elde edilebilecek verilere ait bilgiler Şekil 1'de verilmiş ve çalışma kapsamında önerilen metodolojiye ait iş akış süreci belirtilmiştir.



Şekil 1. Önerilen metodolojinin iş akış diyagramı (Çetin, 2025)

Şekil 1'de ortaya konan iş akış diyagramı takip edilerek çalışma kapsamındaki araştırmalar gerçekleştirilmiş ve elde edilen bulgular bir sonraki bölümde ayrıntılı olarak sunulmaktadır.

4. BULGULAR VE YORUMLAR

Windows 11 Home 21H2 sürümünü kullanan bir bilgisayar ile Android OS 14. sürümünü kullanan Samsung Galaxy A52 mobil telefon ve iOS 18.6.2 sürümünü kullanan Apple iPhone 11 mobil telefon ile test ortamı oluşturulmuştur (Çetin, 2025).

Windows 11 işletim sistemine sahip bir bilgisayara iki farklı mobil işletim sistemi kullanan telefonlar, USB kablosu ve Wi-Fi özelliği aracılığıyla bağlanmış ve bağlanma zamanı bağlantının sonlandırılma zamanları not edilmiştir. Elde edilen test verileri Tablo 1'de sunulmuştur (Çetin, 2025).

Tablo 1. Oluşturulan test verileri (Çetin, 2025)

Cihaz Adı	Bağlantı Türü	Sisteme Bağlanma Zamanı	Sistemden Çıkarılma Zamanı
Samsung Galaxy A52	USB	14.10.2025 23:46:06	14.10.2025 23:56:46
	Wi-Fi	15.10.2025 00:03:32	15.10.2025 00:13:42
Apple iPhone 11	USB	17.10.2025 23:30:41	17.10.2025 23:37:58
	Wi-Fi	28.08.2025 15:32:25	28.08.2025 15:34:23

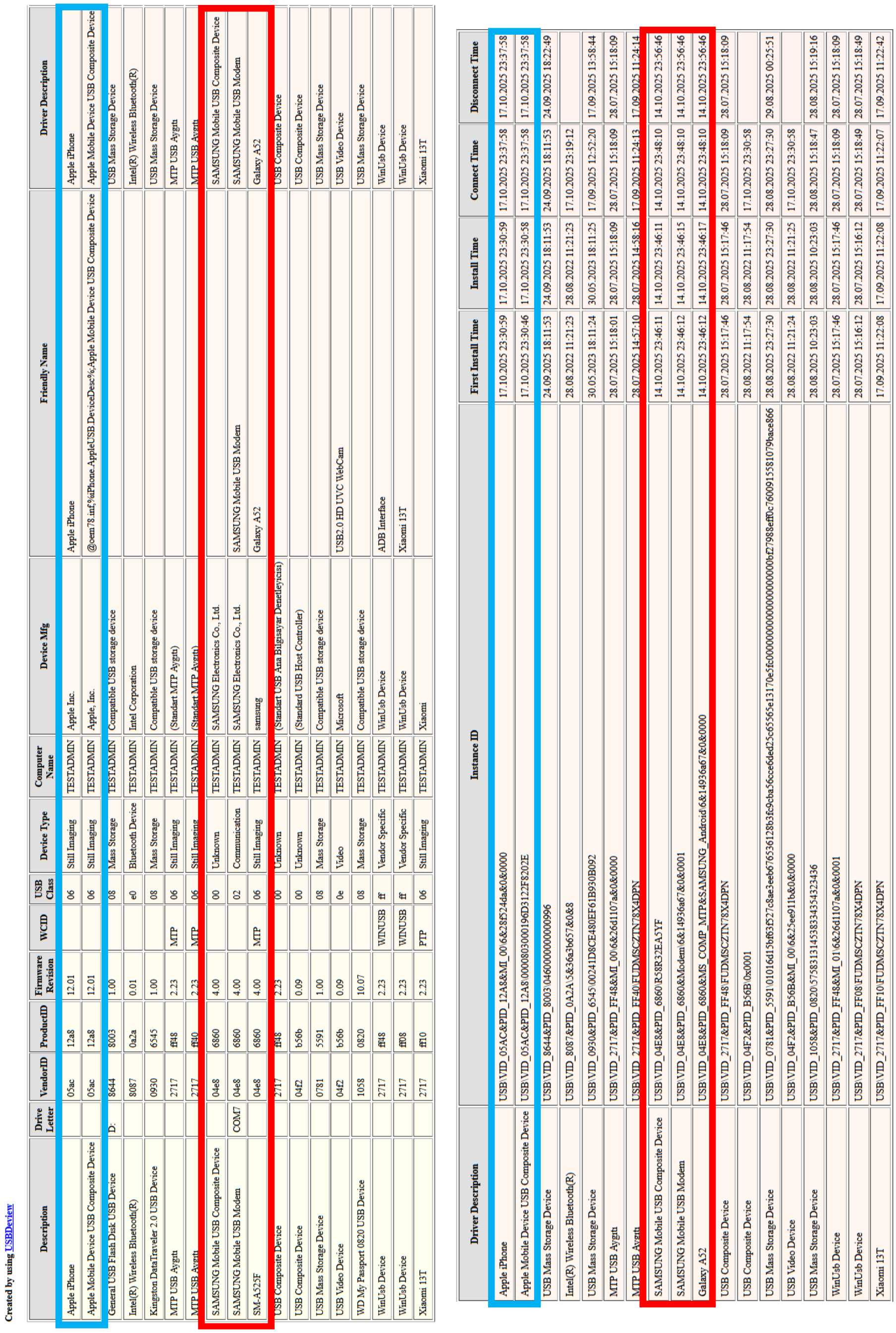
Test ortamının ve test verilerinin oluşturulmasının ardından Şekil 1'de ortaya konan iş akış diyagramı takip edilerek çalışma kapsamındaki araştırmalar gerçekleştirilmiştir.

4.1. USB Bağlantısı Yapan Mobil Telefonlara Dair Bulgular

Çalışma kapsamında Android ve iOS mobil işletim sistemlerine sahip telefonların USB bağlantı kablosu yardımıyla bilgisayara farklı zamanlarda bağlanması ve bağlantısının sonlandırılmasına ait zaman damgaları araştırılmış olup elde edilen bulgular ilerleyen bölümlerde ayrıntılı bir biçimde sunulmaktadır.

4.1.1. USBDeview Yazılım Aracı ile ilk Takılma ve Çıkarılma Zamanlarının Tespit Edilmesi

Mobil telefonlar bilgisayara bağlandıktan sonra, USBDeview yazılım aracı yönetici yetkisiyle çalıştırılmıştır. Şekil 2'de belirtildiği üzere test sonrasında bilgisayara USB bağlantı kablosu aracılığıyla bağlanan tüm cihazlara ilişkin bilgiler elde edilmiştir.



Created by using USBDeview

Description	Drive Letter	VendorID	ProductID	Firmware Revision	WCID	USB Class	Device Type	Computer Name	Device Mfg	Friendly Name	Driver Description
Apple iPhone		05ac	12a8	12.01		06	Still Imaging	TESTADMIN	Apple Inc.	Apple iPhone	Apple iPhone
Apple Mobile Device USB Composite Device		05ac	12a8	12.01		06	Still Imaging	TESTADMIN	Apple, Inc.	@oem78.inf,%iPhone.AppleUSB.DeviceDesc%;Apple Mobile Device USB Composite Device	Apple Mobile Device USB Composite Device
General USB Flash Disk USB Device	D:	8644	8003	1.00		08	Mass Storage	TESTADMIN	Compatible USB storage device		USB Mass Storage Device
Intel(R) Wireless Bluetooth(R)		8087	0a2a	0.01		e0	Bluetooth Device	TESTADMIN	Intel Corporation		Intel(R) Wireless Bluetooth(R)
Kingston DataTraveler 2.0 USB Device		0930	6545	1.00		08	Mass Storage	TESTADMIN	Compatible USB storage device		USB Mass Storage Device
MTP USB Aygıtı		2717	ff48	2.23	MTP	06	Still Imaging	TESTADMIN	(Standart MTP Aygıtı)		MTP USB Aygıtı
MTP USB Aygıtı		2717	ff40	2.23	MTP	06	Still Imaging	TESTADMIN	(Standart MTP Aygıtı)		MTP USB Aygıtı
SAMSUNG Mobile USB Composite Device		04e8	6860	4.00		00	Unknown	TESTADMIN	SAMSUNG Electronics Co., Ltd.		SAMSUNG Mobile USB Composite Device
SAMSUNG Mobile USB Modem	COM7	04e8	6860	4.00		02	Communication	TESTADMIN	SAMSUNG Electronics Co., Ltd.	SAMSUNG Mobile USB Modem	SAMSUNG Mobile USB Modem
SM-A525F		04e8	6860	4.00	MTP	06	Still Imaging	TESTADMIN	samsung	Galaxy A52	Galaxy A52
USB Composite Device		2717	ff48	2.23		00	Unknown	TESTADMIN	(Standart USB Ana Bilgisayar Denetleyicisi)		USB Composite Device
USB Composite Device		04f2	b56b	0.09		00	Unknown	TESTADMIN	(Standard USB Host Controller)		USB Composite Device
USB Mass Storage Device		0781	5591	1.00		08	Mass Storage	TESTADMIN	Compatible USB storage device		USB Mass Storage Device
USB Video Device		04f2	b56b	0.09		0e	Video	TESTADMIN	Microsoft	USB2.0 HD UVC WebCam	USB Video Device
WD My Passport 0820 USB Device		1058	0820	10.07		08	Mass Storage	TESTADMIN	Compatible USB storage device		USB Mass Storage Device
WinUsb Device		2717	ff48	2.23	WINUSB	ff	Vendor Specific	TESTADMIN	WinUsb Device	ADB Interface	WinUsb Device
WinUsb Device		2717	ff08	2.23	WINUSB	ff	Vendor Specific	TESTADMIN	WinUsb Device	Xiaomi 13T	WinUsb Device
Xiaomi 13T		2717	ff10	2.23	PTP	06	Still Imaging	TESTADMIN	Xiaomi		Xiaomi 13T

Driver Description	Instance ID	First Install Time	Install Time	Connect Time	Disconnect Time
Apple iPhone	USB\VID_05AC&PID_12A8&MI_00\6&28f524da&0&0000	17.10.2025 23:30:59	17.10.2025 23:30:59	17.10.2025 23:37:58	17.10.2025 23:37:58
Apple Mobile Device USB Composite Device	USB\VID_05AC&PID_12A8\0000803000196D3122F8202E	17.10.2025 23:30:46	17.10.2025 23:30:58	17.10.2025 23:37:58	17.10.2025 23:37:58
USB Mass Storage Device	USB\VID_8644&PID_8003\0460000000000996	24.09.2025 18:11:53	24.09.2025 18:11:53	24.09.2025 18:11:53	24.09.2025 18:22:49
Intel(R) Wireless Bluetooth(R)	USB\VID_8087&PID_0A2A\5&36a3b657&0&8	28.08.2022 11:21:23	28.08.2022 11:21:23	17.10.2025 23:19:12	
USB Mass Storage Device	USB\VID_0930&PID_6545\00241D8CE480EF61B930B092	30.05.2023 18:11:24	30.05.2023 18:11:25	17.09.2025 12:52:20	17.09.2025 13:58:44
MTP USB Aygıtı	USB\VID_2717&PID_FF48&MI_00\6&26d1107a&0&0000	28.07.2025 15:18:01	28.07.2025 15:18:09	28.07.2025 15:18:09	28.07.2025 15:18:09
MTP USB Aygıtı	USB\VID_2717&PID_FF40\FUDMSCZTN78X4DPN	28.07.2025 14:57:10	28.07.2025 14:58:16	17.09.2025 11:24:13	17.09.2025 11:24:14
SAMSUNG Mobile USB Composite Device	USB\VID_04E8&PID_6860\R58R32EA5YF	14.10.2025 23:46:11	14.10.2025 23:46:11	14.10.2025 23:48:10	14.10.2025 23:56:46
SAMSUNG Mobile USB Modem	USB\VID_04E8&PID_6860&Modem\6&14936a67&0&0001	14.10.2025 23:46:12	14.10.2025 23:46:15	14.10.2025 23:48:10	14.10.2025 23:56:46
Galaxy A52	USB\VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android\6&14936a67&0&0000	14.10.2025 23:46:12	14.10.2025 23:46:17	14.10.2025 23:48:10	14.10.2025 23:56:46
USB Composite Device	USB\VID_2717&PID_FF48\FUDMSCZTN78X4DPN	28.07.2025 15:17:46	28.07.2025 15:17:46	28.07.2025 15:18:09	28.07.2025 15:18:09
USB Composite Device	USB\VID_04F2&PID_B56B\0x0001	28.08.2022 11:17:54	28.08.2022 11:17:54	17.10.2025 23:30:58	
USB Mass Storage Device	USB\VID_0781&PID_5591\01016d15bf63f527c8ae3eeb676536128b3fc9cba56cce6ded25c65565e13170e5fc00000000000000000000bf27988eff0c7600915581079bace866	28.08.2025 23:27:30	28.08.2025 23:27:30	28.08.2025 23:27:30	29.08.2025 00:25:51
USB Video Device	USB\VID_04F2&PID_B56B&MI_00\6&25ee911b&0&0000	28.08.2022 11:21:24	28.08.2022 11:21:25	17.10.2025 23:30:58	
USB Mass Storage Device	USB\VID_1058&PID_0820\575831314538334354323436	28.08.2025 10:23:03	28.08.2025 10:23:03	28.08.2025 15:18:47	28.08.2025 15:19:16
WinUsb Device	USB\VID_2717&PID_FF48&MI_01\6&26d1107a&0&0001	28.07.2025 15:17:46	28.07.2025 15:17:46	28.07.2025 15:18:09	28.07.2025 15:18:09
WinUsb Device	USB\VID_2717&PID_FF08\FUDMSCZTN78X4DPN	28.07.2025 15:16:12	28.07.2025 15:16:12	28.07.2025 15:18:49	28.07.2025 15:18:49
Xiaomi 13T	USB\VID_2717&PID_FF10\FUDMSCZTN78X4DPN	17.09.2025 11:22:08	17.09.2025 11:22:08	17.09.2025 11:22:07	17.09.2025 11:22:42

Şekil 2. USBDeview aracılığıyla bilgisayara bağlanan telefonlara dair bulgular

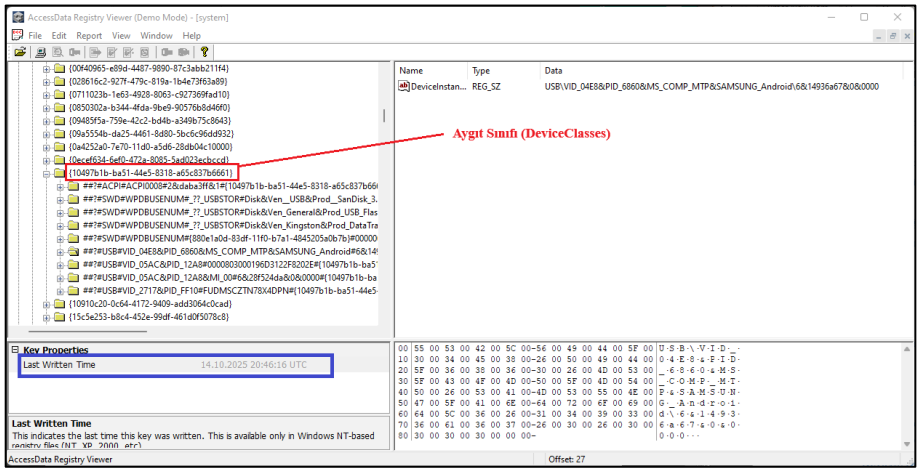
Test öncesi ve test sonrasında oluşan veriler birbirleri ile kıyaslanmıştır. Tespit edilen farklar Şekil 2'de Android işletim sistemine sahip telefon için kırmızı renk ve

iOS işletim sistemine sahip telefon için mavi renk ile kutu içerisine alınarak gösterilmiştir.

4.1.2. USB Bağlantısına Dair Zaman Damgalarının Windows Kayıt Defteri Kayıtlardan Elde Edilmesi

4.1.2.1. İlk Takılma Zamanın Aygıt Sınıfları (DeviceClasses) Kayıtlarından Bulunması

İşletim sisteminden bağımsız olarak bir mobil telefon, USB kablosu aracılığıyla bilgisayara bağlandığında bilgisayara bağlanmak ve bilgisayar ile iletişim kurabilmek için gerekli tüm sürücüleri bünyesinde barındırmaktadır. Sürücülerin başarılı bir şekilde kurulup ilk bağlantının gerçekleştirilmesi sonrasında Windows Kayıt Defteri kayıt sisteminde kurulan bağlantıya dair bilgileri aygıt sınıflarına göre anahtarlar atamak suretiyle kayıt altına almaktadır. Oluşturulan kayıtlar, Windows Kayıt Defteri kayıt sisteminin "SYSTEM\ControlSet001\Control\DeviceClasses" dizininin altında yer almaktadır (Şekil 3).



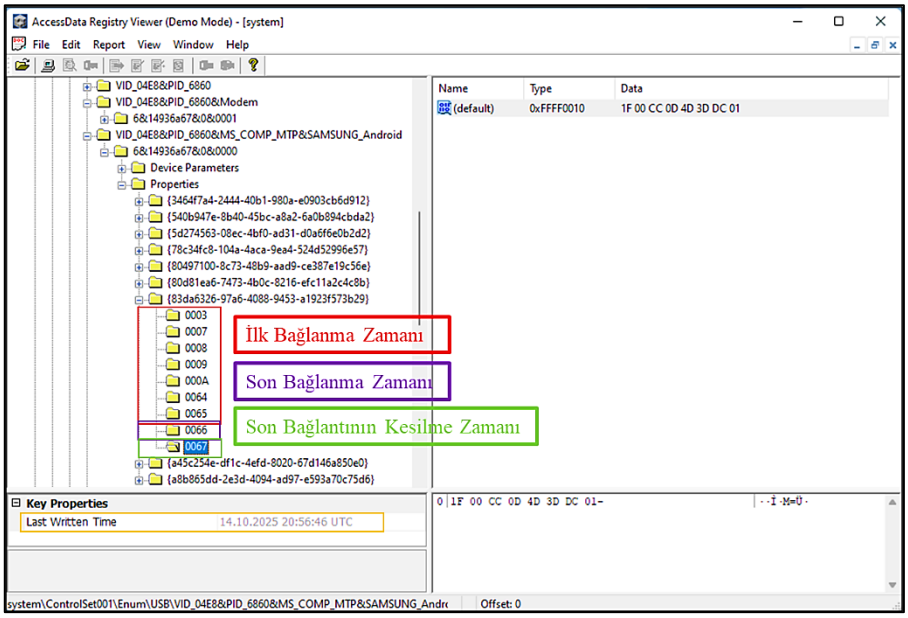
Şekil 3. DeviceClasses Anahtarlarına dair ekran görüntüsü

Android ve iOS işletim sistemine sahip iki mobil telefon için Windows Kayıt Defteri'nde oluşturulan Aygıt Sınıfları Access Data Registry Viewer yazılımı aracılığıyla alt anahtar incelenmiştir. Last Written Time başlığı altında ilgili mobil telefonun sisteme ilk bağlanma zamanı tespit edilmiştir. Elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

4.1.2.2. Çıkarılma Zamanlarının USB Anahtarı Aracılığıyla Elde Edilmesi

Bir mobil telefon USB kablosu ile bilgisayara bağlandığında veya bağlantısı kesildiğinde, bağlantının Medya Aktarım Protokolü (MTP) veya Resim Aktarım Protokolü (PTP) kullanıp kullanmadığına bakılmaksızın ilgili bilgiler Windows

Kayıt Defteri sistemi kovanında tutulmaktadır. Alt anahtar, her bir bağlantı için "SYSTEM\ControlSet001\Enum\USB\VID_vvvv&PID_pppp\ UUID\Properties\(83da6326-97a6-4088-9453-aI923f573b29)" dizininde oluşturulmaktadır (Arshad vd., 2017). Burada 0003, 000A, 0064 ve 0065 anahtarları, ilk bağlantı zamanıyla ilgili bilgileri depolarken 0066 ve 0067 anahtarları sırasıyla son bağlantı zamanı ve son bağlantının sonlandırılma zamanı hakkında bilgileri saklamaktadır (Şekil 4).



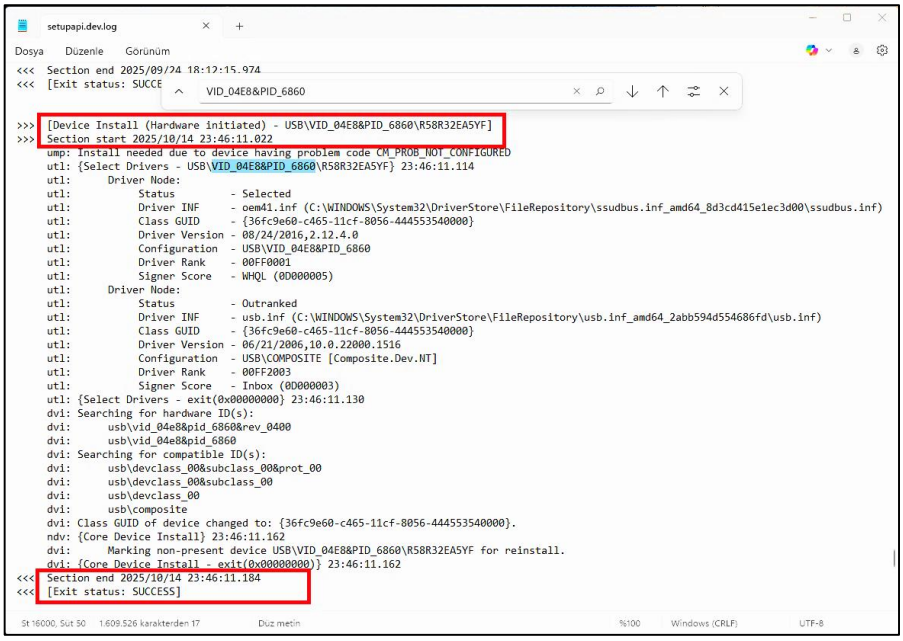
Şekil 4. Samsung A52 mobil telefonunun sistemden çıkarılma zamanına dair ekran görüntüsü

Android ve iOS işletim sistemine sahip iki mobil telefon için Windows Kayıt Defteri'nde oluşturulan USB anahtarları Access Data Registry Viewer yazılımı aracılığıyla USB anahtarları incelenmiştir. İlk bağlanma zamanı, son bağlanma zamanı ve son bağlantının kesilme zamanına ait ilgili anahtarın işaretlenmesiyle Last Written Time başlığı altında incelenen zaman damgası tespit edilmiştir. Elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

4.1.3. Setupapi.dev.log Kayıtlarından İlk Takılma Zamanlarının Tespit Edilmesi

Günümüzde tak-çalıştır (Plug-and-Play) özelliğine sahip cihazlar, gerekli sürücü dosyalarını hafızalarında bulundurarak bilgisayara bağlandıklarında otomatik kurulum işlemleri gerçekleştirmektedir. USB kablosu ile bağlanan telefonlar da bu özelliğe sahiptirler. Bağlantı sağlandığında, PnP yöneticisi tarafından cihazın tanımlama bilgileri alınır ve Windows Kayıt Defteri'nde ilgili kayıtlar oluşturulur.

Bu kayıtlar "setupapi.dev.log" dosyasında saklanır ve C:\WINDOWS\INF\setupapi.dev.log yoluyla erişilebilir (Neyaz ve Shashidhar, 2019) (Şekil 5).



Şekil 5. Bilgisayara USB ile bağlanan telefonun kurulumuna ait ekran görüntüsü

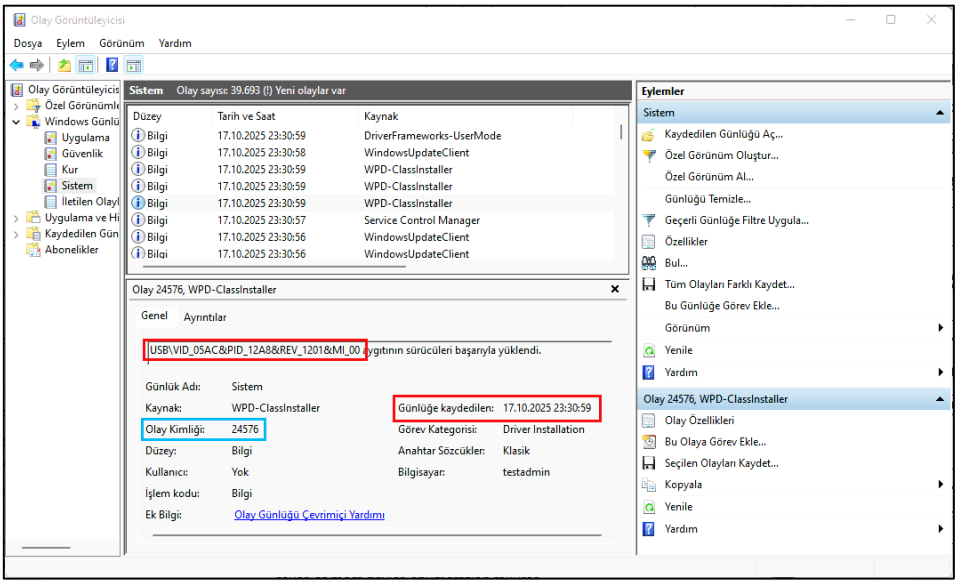
Windows/INF dizini altında yer alan 'Setupapi.dev.log' metin günlüğündeki kayıtlar Not Defteri ile açılarak incelenmiştir. Mobil telefonların ürün kimlik numarası (PID) ve üretici kimlik numarası (VID) aracılığıyla arama yapılmış ve Şekil 5'te görüldüğü üzere ilk kuruluma dair zaman bilgileri elde edilmiştir. Elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

4.1.4. USB Bağlantısına Dair Zaman Damgalarının Windows Olay Günlüklerinden Elde Edilmesi

Windows işletim sistemi, bünyesinde yer alan olay günlükleri içerisinde sistem etkinliği ve kullanıcı faaliyetlerine dair tüm uyarı ve bildirimlerin kaydını tutmaktadır. Windows işletim sistemi, bilgisayarda gerçekleştirilen her işlem için bir olay adı ve buna bağlı olarak olay kimliği belirlemektedir. Windows Olay Günlüğü dosyaları C:\Windows\System32\winevt\Logs dizininde yer almaktadır (Kondapally, t.y.).

Bir mobil telefonun USB kablosu aracılığıyla Windows sistemine bağlanması ve bağlantısının sonlandırılması ile ilgili kayıtların, Windows Olay Günlükleri'nde

belirli olay kimlik numaraları ile ilgili tuttuğu belirlenmiştir. 1000, 1001, 1002, 1003, 1005, 10000, 10100, 20001, 20003, 24576, 24577 ve 24578 olay kimlik numaraları ile MTP ve PTP protokollerini kullanarak bağlantı sağlayan cihazlar için kayıt tutulmaktadır. 1000 ve 1001 olay kimlik numaraları ile sisteme son bağlantı zamanına ulaşılabilirken 1002 ve 1005 olay kimlik numaraları ile de son bağlantının sonlandırılma zaman bilgisine erişilebilmektedir (Şekil 6).



Şekil 6. Bilgisayara bağlanan telefonun Windows Olay Günlüğü kayıtlarının görüntüsü

Android ve iOS işletim sistemine sahip iki mobil telefon için Windows Olay Günlükleri'nde tutulan kayıtlar yukarıda belirtilen olay kimlik numaraları aracılığıyla incelenmiştir. Şekil 6'da bilgisayara bağlanan bir mobil telefonun bağlanma zamanlarına ait görsel sunulmaktadır. Benzer şekilde bağlantının sonlandırılmasına dair zaman bilgileri ilgili olay kimliği numarası ile araştırılmış olup elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

4.2. Kablosuz (Wi-Fi) Bağlantısı Yapan Mobil Telefonlara Dair Bulgular

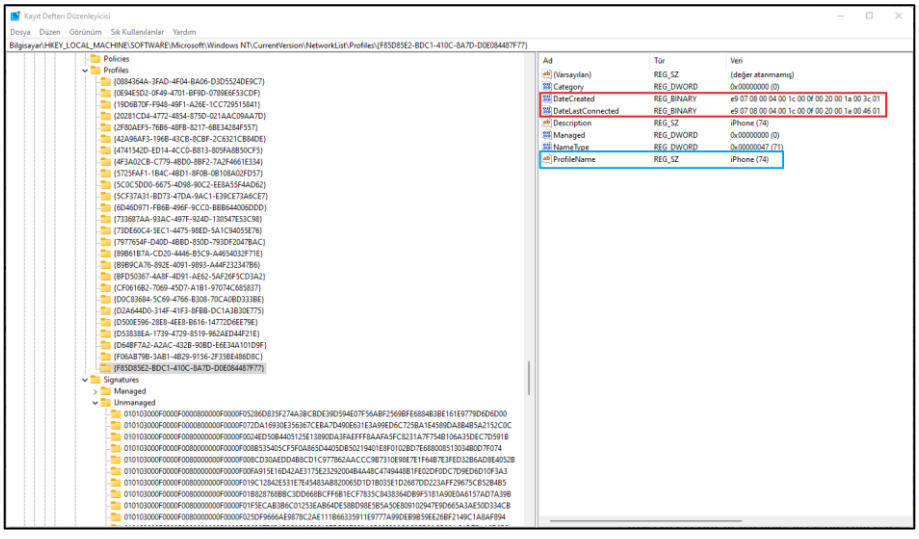
Çalışma kapsamında Android ve iOS mobil işletim sistemlerine sahip telefonların Wi-Fi aracılığıyla bilgisayara farklı zamanlarda bağlanması ve bağlantısının sonlandırılmasına ait zaman damgaları araştırılmıştır. Elde edilen bulgular ilerleyen bölümlerde ayrıntılı bir biçimde sunulmaktadır.

4.2.1. Wi-Fi Bağlantısına Dair Zaman Damgalarının Windows Kayıt Defteri Kayıtlardan Elde Edilmesi

Windows işletim sistemi, kablosuz bağlantı ayarlarını ve bağlantı ile ilgili yapılandırma bilgilerini çeşitli yerlerde depolamaktadır. Windows Defteri içerisinde yer alan "NetworkList", bir cihazın bağlı olduğu kablosuz ağ profilleri hakkında bilgileri içeren bir kayıt defteri anahtarıdır. Ağ profilinin ismi, ağ profilinin GUID (Globally Unique Identifier) değeri, DNS uzantısı, kablosuz ağ cihazının fiziksel adresi (MAC), profilin oluşturulma tarihi, en son bağlantı zamanı ve bağlantının güncellenme süresi gibi veriler bu anahtar altında tutulmaktadır. Genel olarak, "NetworkList" kayıtlarının kayıt defterindeki konumu aşağıdaki yol izlenerek ulaşılabilmektedir (Risto, 2011) (Alghafli vd., 2011).

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList

Kablosuz ağ tanımlayıcı tarafından tutulan kayıtların, Windows Kayıt Defteri "İmzalar (Signatures)" kayıtlarıyla eşleşmesi gerçekleştirilmiş, buradan bağlantı için belirlenen DefautGatewayMac adresi ile Profil GUID değeri ve ayrıca kablosuz ağ için kullanıcı tarafından kullanılan isim tespit edilmiştir. Ardından elde edilen Profil GUID değeri, Windows Kayıt Defteri "Profiller (Profiles)" kayıtları ile eşleştirilmiştir. Eşleştirme sonrası ilgili profil incelenerek ilk bağlanma ve son bağlanma zamanları belirlenmiştir (Şekil 7).



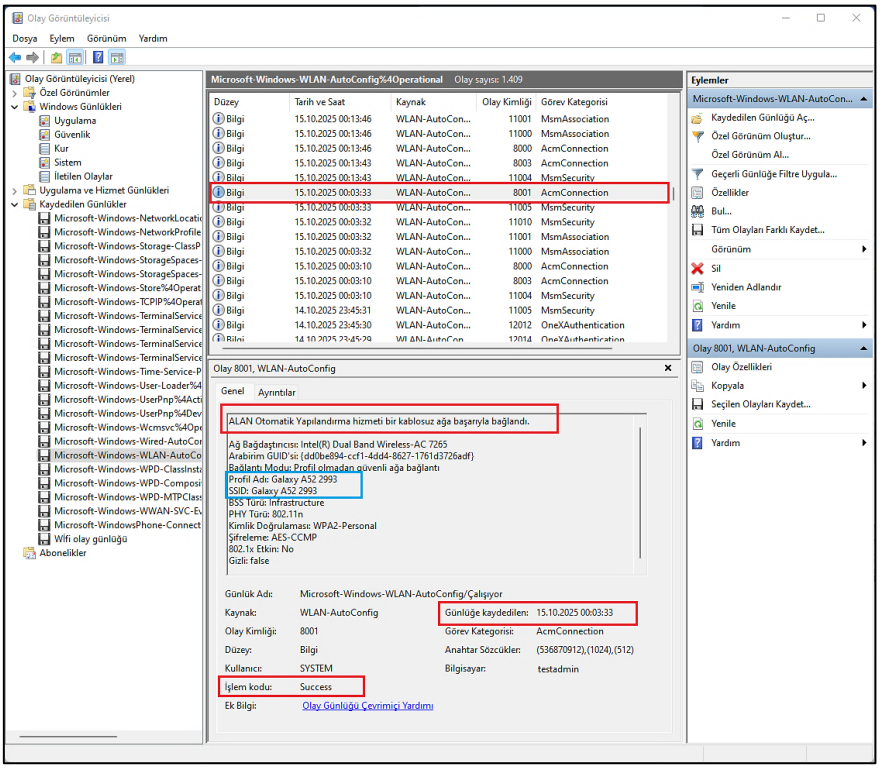
Şekil 7. Windows Kayıt Defteri kayıtlarından kablosuz bağlantının oluşturulma ve son bağlantı zamanının tespiti

Şekil 7'de görüldüğü üzere, elde edilen DataCreated ve DateLastConnected bilgileri Hexadecimal (16 tabanlı sayı) yapıda olup, bu bilgiler DCode yazılımı yardımıyla

çözümlenerek zaman bilgileri tespit edilmiştir. Elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

4.2.2. Wi-Fi Bağlantısına Dair Zaman Damgalarının Windows Olay Günlüklerinden Elde Edilmesi

Bir mobil telefonun kablosuz bağlantı aracılığıyla Windows sistemine bağlanma zamanı ve sistemden bağlantısının kesilme zamanına ait bilgiler, Windows Olay Günlükleri'nde belirli olay kimlik numaraları ile kaydedildiği bilinmektedir. Bilgisayara kablosuz (Wi-Fi üzerinden) bağlantı kuran cihazlarla ilgili veriler, 8001 olay kimlik numarası ile Windows Olay Günlükleri'ne kaydedilirken bilgisayarla kablosuz bağlantını sonlandıran cihazlara dair bilgilerin ise 8003 olay kimlik numarası ile kaydı tutulmaktadır. Bu olay kimlikleri yardımıyla kablosuz bağlantı yapan telefonların profil adları, bağlanma ve bağlantının kesilme zamanları ve bağlandıkları bilgisayarın adı gibi önemli verilere erişilebilmektedir (Şekil 8).



Şekil 8. Windows Olay Günlükleri'nden kablosuz bağlantı kuran telefona ait zaman bulgusu

Android ve iOS işletim sistemine sahip iki mobil telefon için Windows Olay Günlükleri'nde tutulan kayıtlar yukarıda belirtilen olay kimlik numaraları aracılığıyla incelenmiştir. Şekil 8'de bilgisayara Wi-Fi aracılığıyla bağlanan bir

mobil telefonun bağlanma zamanlarına ait görsel sunulmaktadır. Benzer şekilde bağlantının sonlandırılmasına dair zaman bilgileri ilgili olay kimliği numarası ile araştırılmış elde edilen bulgular, sonuçlar ve tartışma bölümde ayrıntılı olarak sunulmuştur.

Çalışma kapsamında ele alınan araştırma konuları için çeşitli veri kaynaklarından zaman bulguları tespit edilmiştir. Bir sonraki bölümde farklı kaynaklardan elde edilen zaman bulguları birbirleri ile kıyaslanarak tartışılmış ve karşılaşılan problemlere yönelik çözüm önerileri sunulmuştur.

5. SONUÇLAR ve TARTIŞMA

Bu çalışmada, bilgisayarla USB kablosu aracılığıyla bağlantı kuran iki farklı mobil işletim sistemine (Android ve iOS) sahip telefon ve kendi internetini Wi-Fi özelliği ile bir bilgisayara paylaşan iki farklı telefonun, Windows 11 işletim sistemi kurulu bir bilgisayar üzerinde bıraktıkları dijital izler, Windows Kayıt Defteri, Windows Olay Günlükleri ve ilgili yazılım ve donanım araçları aracılığıyla adli bilişim teknik ve süreçlerine uygun bir biçimde tespit edilmiştir.

Önerilen metodoloji ile USBDeview yazılım aracı kullanılarak bilgisayara bağlı veya hâlâ bağlantıda olan USB cihazlarının türü, seri numarası, üretici, ürün kimlik numarası, sınıf kodu ve benzeri birçok değerli bilgiye ulaşılması mümkün olduğu gözlenmiştir. Ayrıca USB kablosu ile bilgisayara bağlanan telefonlara dair bağlantı türü, cihaza verilen isim, üretici ve ürün kimlik numarası, ilk yüklenme zamanı, son bağlantı zamanı ve bağlantıyı kesme zamanı gibi adli bilişim araştırmacısı için önemli verilere ulaşılabildiği görülmüştür. Bunlara ilave olarak, yazılım aracı sayesinde tüm kullanıcı hesaplarında bilgisayara bağlı USB cihazlarını listeleyebildiği ancak yönetici yetkisi olmadan çalıştırıldığında sisteme bağlanma zamanı ve bağlantının kesildiği zamanı gösteremediği belirlenmiştir.

USB kablosu ile bilgisayara bağlanan ve bir müddet sonra bağlantısı sonlandırılan mobil telefonlar için farklı veri kaynaklarından ulaşılan zaman damgaları Tablo 2'de sunulmaktadır.

Tablo 2. USB bağlantısı yapan mobil telefonlarına ait zaman bulguları

Kaynak	**Bulgular**	**Samsung (Galaxy A52)**	**iPhone 11**
Test verisi	Bağlanma zamanı:	14.10.2025 **23:46:06**	17.10.2025 **23:30:41**
	Çıkarılma zamanı:	14.10.2025 23:56:46	17.10.2025 23:37:58
USBDeview	İlk bağlanma zamanı:	14.10.2025 **23:46:12**	17.10.2025 **23:30:46**
	Son bağlanma zamanı:	14.10.2025 23:48:10	17.10.2025 23:37:58
	Son çıkarılma zamanı:	14.10.2025 23:56:46	17.10.2025 23:37:58

Access Data Registry Viewer (Windows Kayıt Defteri)	Bağlanma zamanı:	14.10.2025 **23:46:12**	17.10.2025 **23:30:45**
	Çıkarılma zamanı:	14.10.2025 23:56:46	17.10.2025 23:37:58
Windows Olay Günlükleri	Bağlanma zamanı:	14.10.2025 **23:46:11**	17.10.2025 **23:30:46**
	Çıkarılma zamanı:	14.10.2025 23:56:46	17.10.2025 23:37:58
Setupapi.dev.log	İlk bağlanma zamanı:	14.10.2025 **23:46:11.022**	17.10.2025 **23:30:45.836**
	Son bağlanma zamanı:	14.10.2025 23:46:11.184	17.10.2025 23:30:46.853
	Çıkarılma zamanı:	İze rastlanılmamıştır.	İze rastlanılmamıştır.

Tablo 2'den görüldüğü gibi, USB ile bilgisayara bağlanan telefonun bağlantı zamanına ilişkin bilgiler, USBDeview yazılım aracı, Windows Kayıt Defteri'ni incelemek için kullanılan Access Data Registry Viewer yazılımı, Windows Olay Günlükleri ve Setupapi.dev.log metin kayıtlarından elde edilebilmektedir. Ancak bilgisayar ile bağlantısı kesilen telefona ait zaman damgalarına Access Data Registry Viewer yazılımı, USBDeview yazılım aracı ve Windows Olay Günlükleri ile erişim sağlandığı gözlemlenmiştir. Elde edilen bulguların test verileri ile uyumlu olduğu ancak test verisi ile dijital izler arasında yaklaşık 5 saniyelik bir farkın olduğu gözlenmiştir. Bu farkın ise telefona bağlanan USB kablosunun bilgisayarın soketine tam oturtulması için geçirilen süre olabileceği düşünülmektedir. Dijital kayıtlar arasındaki birkaç saniyelik farklılıkların, gerçekleştirilen işlemlerin sıralanmasından kaynaklandığı düşünülmektedir.

Bilgisayara USB bağlantısıyla bağlı telefonlara ilişkin Windows Kayıt Defteri kayıtlarında USBSTOR anahtarının altında yapılan incelemede, sistemin herhangi bir alt anahtar oluşturmadığı görülmüştür. Fakat USB anahtarının altında ilgili kayıtların bulunduğu ve bu kayıtlardan ilk bağlantı, son bağlantı ve bağlantının kesildiği zaman bilgilerine ulaşılabileceği anlaşılmıştır.

Wi-Fi üzerinden bilgisayara bağlanan telefonların bağlantı oluşturma ve bağlantıyı kesme sürelerine dair elde edilen veriler Tablo 3'de gösterilmektedir.

Tablo 3. Wi-Fi bağlantısı yapan mobil telefonlarına ait zaman bulguları

Kaynak	**Bulgular**	**Samsung (Galaxy A52)**	**iPhone 11**
Test verisi	Sisteme bağlanma zamanı:	15.10.2025 **00:03:32**	28.08.2025 **15:32:25**
	Sistemden çıkarılma zamanı:	15.10.2025 **00:13:42**	28.08.2025 15:34:23
Access Data Registry Viewer	Sisteme bağlanma zamanı:	15.10.2025 **00:03:34**	28.08.2025 **15:32:26**
	Sistemden çıkarılma zamanı:	İze rastlanılmamıştır.	İze rastlanılmamıştır.

Windows Kayıt Defteri (DCode yardımıyla)	Sisteme bağlanma zamanı:	15.10.2025 **00:03:34.232**	28.08.2025 **15:32:26.316**
	Sisteme en son bağlanma zamanı:	15.10.2025 00:03:34.247	28.08.2025 15:32:26.326
	Sistemden çıkarılma zamanı:	İze rastlanılmamıştır.	İze rastlanılmamıştır.
Windows Olay Günlükleri	Sisteme bağlanma zamanı:	15.10.2025 **00:03:33**	28.08.2025 **15:32:25**
	Bağlantının kesilme zamanı:	15.10.2025 **00:13:43**	28.08.2025 15:34:23

Elde edilen sonuçlar test verisi ile karşılaştırıldığında, verilerin birbirleriyle uyumlu olduğu görülmüştür. Çizelgeden görüleceği üzere, bilgisayar ile Wi-Fi üzerinden kablosuz bağlantı kuran telefonlara ait bağlanma bilgileri Windows Olay Günlükleri ve Access Data Registry Viewer kullanılarak Windows Kayıt Defteri kayıtları aracılığıyla elde edilebilmektedir. Ancak bağlantının sona erdiği zamana dair bilgiye yalnızca Windows Olay Günlükleri kayıtlarının incelenmesiyle ulaşılabileceği belirlenmiştir.

Tablo 3'deki verilerin test verisiyle örtüştüğü, test verisi ile dijital izler arasında sisteme bağlanma süresi ve bağlantının kesilme süresi arasında yaklaşık 1 saniyelik bir fark bulunduğu, bu farkın telefonun Wi-Fi ile bağlanmaya başladığı anda bilgisayar sisteminde gerçekleştirilen işlemlerin sıralanmasından kaynaklandığı öngörülmektedir.

Çalışma kapsamında incelenen, Android ya da iOS işletim sistemine sahip şüpheli bir telefonun bilgisayara USB bağlantı kablosu aracılığıyla ya da kablosuz (Wi-Fi) olarak herhangi bir bağlantı kurup kurmadığına dair bilgilerin kolaylıkla elde edilebileceği görülmüştür. Şüpheli cihazın çok kısa süreliğine dahi USB kablosu ya da Wi-Fi aracılığıyla bir bilgisayar ile bağlantı kurması halinde kurulan bağlantının türü ve zamanı ile bağlantının kesildiği zamana dair bilgiler kolaylıkla tespit edilebilmektedir. Tespit edilen zaman bilgilerinin farklı veri kaynaklarından da teyit edilebileceği görülmüştür.

6. ÖNERİLER

- Linux ya da MacOS gibi farklı işletim sistemleri kullanan bilgisayarlarda çalışmanın tekrarlanmasının adli bilişim araştırmalarına katkı sağlayacağı değerlendirilmektedir.

- Windows işletim sisteminin imajının alınması esnasında ya da imaj alınması sonrasında veri kaybı olup olmadığının araştırılmasının faydalı olacağı düşünülmektedir.

- Sanal makine kullanılarak çalışmanın tekrarlanarak işletim sistemi üzerinde ne tür dijital izler bıraktığının irdelenmesinin literatüre katkı sağlayacağı ve bu alanda çalışanlara kolaylık sağlayacağı değerlendirilmektedir.

- Bilgisayara USB veya Wi-Fi ile bağlanan telefonların bağlı kaldıkları süre zarfında yaptıkları işlemlerin (dosya transferi, dosya açılması vb.) Windows işletim sisteminde bıraktığı izlerin adli bilişim açısından incelenmesinin yararlı olacağı düşünülmektedir.

KAYNAKÇA

AccessData. (2014). *Registry Viewer*. https://d1kpmuwb7gvu1i.cloudfront.net/RegistryViewer_UG.pdf

Alghafli, K. A., Jones, A., & Martin, T. A. (2011). Forensic analysis of the Windows 7 registry. *Journal of Digital Forensics, Security and Law, 5*(4), 5–30. https://doi.org/10.15394/jdfsl.2010.1081

Arshad, A., Iqbal, W., & Abbas, H. (2018). USB storage device forensics for Windows 10. *Journal of Forensic Sciences, 63*, 856–867. https://doi.org/10.1111/1556-4029.13596

Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Elsevier.

Çakır, H., & Kılıç, M. S. (2013). Bilişim suçlarına ilişkin delil elde etme yöntemlerine genel bir bakış. *Polis Bilimleri Dergisi, 15*(3), 23–44.

Çetin, A. (2025). *Windows işletim sistemi kurulu bilgisayarlara bağlanan telefonların adli bilişim açısından incelenmesi* [Yayımlanmamış yüksek lisans tezi]. Ankara Üniversitesi.

Digital Detective. (t.y.). *DCode™ – Timestamp decoder*. https://www.digital-detective.net/dcode/

Đuranec, A., Topolčić, D., Hausknecht, K., & Delija, D. (2019, Mayıs 20–24). Investigating file use and knowledge with Windows 10 artifacts. In *42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (ss. 1213–1218). IEEE. https://ieeexplore.ieee.org/document/8756877

Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital forensic tools used in analyzing cybercrime. *Journal of University of Shanghai for Science and Technology, 23*(3), 367–379. https://doi.org/10.51201/Jusst12621

Kondapally, B. P. (t.y.). *Forensically important artifacts in Windows operating systems*. https://www.academia.edu/29746363/Forensically_Important_Artifacts_in_Windows_Operating_systems

Kurtca, T., & Samet, R. (2024). MacOS bilgisayara bağlanan telefonların MAC adresi kayıtlarının incelenmesi. *Journal of the Faculty of Engineering and Architecture of Gazi University, 39*(3), 1637–1647. https://doi.org/10.17341/gazimmfd.1140690

Neyaz, A., & Shashidhar, N. (2019). USB artifact analysis using Windows event viewer, registry and file system logs. *Electronics, 8*(11), 1322. https://doi.org/10.3390/electronics8111322

Nirsoft. (t.y.). *USBDeview v3.07*. https://www.nirsoft.net/utils/usb_devices_view.html

Polis Akademisi. (2022). *Adli bilişim: Güncel yaklaşım ve uygulamalar*. https://cdn2.pa.edu.tr/Upload/Rapor/Dosya/adli-bilisim-raporu.pdf

Risto, J. (2010). *Wireless networks and the Windows registry: Just where has your computer been?* Global Information Assurance Certification. https://www.giac.org/paper/gawn/1623/wireless-networks-windows-registry-computer-been/121403

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security*, 8–12. https://doi.org/10.1016/S1361-3723(04)00017-X

Tekin, E. (2017). *Adli bilişimde açık kaynak kullanımı* (Yayın No. 481806) [Yüksek lisans tezi, Polis Akademisi]. YÖK Ulusal Tez Merkezi.

Uçar, A. H. (2021). *Windows işletim sistemi kalıntılarının analizini gerçekleştiren siber olay müdahale aracının geliştirilmesi ve olay zaman çizelgesinin çıkarılması* (Yayın No. 688951) [Yüksek lisans tezi, Fırat Üniversitesi]. YÖK Ulusal Tez Merkezi.