Android İşletim Sisteminde WhatsApp Uygulamasının Adli Bilişim Açısından İncelenmesi

Erhan AKBAL, Şengül DOĞAN*, İbrahim BALOĞLU

Adli Bilişim Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ, Türkiye
erhanakbal@firat.edu.tr, sdogan@firat.edu.tr, ibrahimbaloglu@yahoo.com
(Geliş/Received: 25.09.2017; Kabul/Accepted: 23.02.2018)
DOI: 10.17671/gazibtd.339802

Özet— Günümüzde pek çok kişinin sahip olduğu sosyal medya hesapları insanların vazgeçilmez iletişim araçları haline gelmiştir. Yaygın kullanılan uygulamalardan biri olan WhatsApp artık akıllı telefon sahibi olan bireylerin birçoğunun telefonunda bulunmaktadır. Uygulama internete sahip tüm akıllı telefonlarda mesajlaşma, görüntülü sohbet gibi pek çok avantajlar sağlamaktadır. Bu kadar yaygın kullanılan bu uygulama adli süreçlere yardımcı olabilecek pek çok delil içerebilmektedir. Bu çalışmada sosyal medya kullanımının büyük bir hızla arttığı günümüzde yaygın kullanılan WhatsApp uygulamasının adli bilişim açısından incelenmesi sunulmuştur. Çalışmada Android tabanlı bir telefon rootlu ve rootsuz olarak incelenerek elde edilebilecek veriler ve konumları gösterilmiştir.

Anahtar Kelimeler— adli bilişim, elektronik delil, WhatsApp, siber güvenlik, mobil adli bilişim

The Investigation of WhatsApp Application in Android Operating System related to Digital Forensics

Abstract— Nowadays, the social media accounts used by many people have become the indispensable means of communication for people. WhatsApp, one of the most widely used applications, is now on the phone of many of the individuals who own smartphones. This application provides many advantages such as send secure unlimited messages, documents, audio, video, location on all smartphones with internet usage. This commonly used application can contain a number of evidences that can help with judicial processes. In this study, an investigation of the WhatsApp application with regards to digital forensics is presented. A phone with Android operating system is examined as rooted and unrooted, and the data and locations available from the phone are shown.

Keywords— digital forensics, digital evidence, WhatsApp, cyber security, mobile forensics

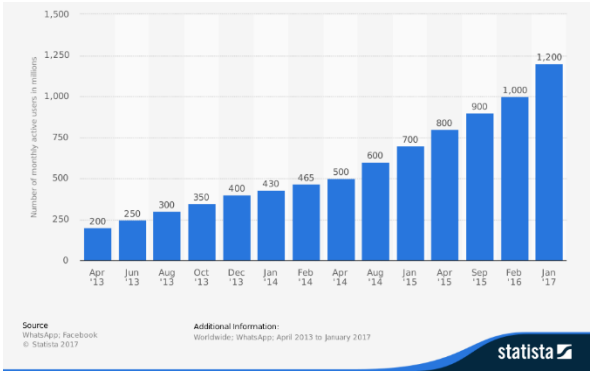
1. GİRİŞ (INTRODUCTION)

WhatsApp günümüzde yaygın kullanılan kişisel mesajlaşma uygulamalarının başında gelmektedir. Bu ve benzeri uygulamalar sayesinde insanlar mesafe kavramı olmaksızın internet alt yapısına sahip telefonlar aracılığıyla ücretsiz bir şekilde telefonlarında kayıtlı olan kişiler ile multimedya verileri paylaşabilirler, mesajlaşıp görüntülü sohbet edebilirler. WhatsApp'ın yaygın kullanılmasının nedenlerinin başında uygulamanın yayınlanması sürecinde iletişimin daha yüksek maliyetle yapılması ve kullanım kolaylığı olarak tanımlanabilir [1,2].

WhatsApp, adres defterini otomatik olarak senkronize edebilen çapraz platform mobil mesajlaşma sağlar. Bu uygulama ile kullanıcılar bir telefonda kolay ve düşük maliyetli ağ kurmuş sayılabilirler. WhatsApp hizmetlerini kullanabilmek için kullanıcı, [telefon numarası] @ s.WhatsApp.net gibi kullanıcı kimliği ile kullanıcı hesabının oluşturulduğu bir telefon numarası sağlamalıdır. Uygulamada mesajların uzunluğu ve sayısı konusunda herhangi bir sınırlama yoktur ve hiçbir servis ücreti gerektirmez. Tek gereksinim, uygulamayı destekleyen bir telefon, internet bağlantısı ve depolama alanıdır [2-4]. Başlangıçta basit bir mesajlaşma uygulaması olarak kullanılan WhatsApp yeni sürümleri yayınlandıkça görüntülü sohbet, WhatsApp durum, gönderilen mesajı geri alma gibi yeni özellikler sağlamaktadır. Bu özelliklerin başında iki aşamalı doğrulama gelmektedir. İki aşamalı doğrulama, hesap güvenliğini artırmaya yönelik olarak eklenmiştir [5,6].

WhatsApp, internet üzerinden veri alışverişi yapmak için açık standart Genişletilebilir Mesajlaşma ve Durum

Protokolünün (XMPP) özelleştirilmiş bir sürümünü kullanır. Mesajlar düz metin, fotoğraf, ses, video, konum, dosya, adres defteri, iletişim kartları ve simgeler şeklinde olabilir. Bu uygulama Android, BlackBerry, iPhone, Bada ve Symbian gibi pek çok işletim sistemlerinin mevcut sürümleri ile çalışabilir [6-8]. Aynı zamanda telefon veya operatöre bağlı çalışan bir uygulama olmaması nedenleri ile Şekil 1'de gösterildiği gibi dünya genelinde 1.2 milyar kullanıcıya ulaşmıştır [9].



Şekil 1. Nisan 2013- Ocak 2017 için WhatsApp kullanım oranları

(WhatsApp usage rates between April 2013 - January 2017)

WhatsApp gibi uygulamaların insanların yaygın kullandığı iletişim aracı haline gelmesi ile beraber elektronik ortamda paylaşılan verilerde büyük oranda artmaktadır. Bu veriler ihtiyaç duyulması durumunda özellikle hukuki süreçlerde önemli bilgiler içerebilmektedir [3].

Elektronik ortamda bulunan her verinin güvenliğinin sağlanması ve gerekli durumlarda hukuki süreçlerde kullanılması amacıyla standart yapıda elde edilmesi Adli bilişimin çalışma alanını oluşturmaktadır. Adli bilişim uzmanları tarafından hukuki süreçte ihtiyaç duyulan verilerin böyle yaygın kullanılan uygulamalardan elde edilmesi sürecinde her uygulamanın dosya yapısının ayrıntılı olarak bilinmesi, delilin hızlı ve zarar görmeden elde edilmesi açısından oldukça önemlidir [2,10,11].

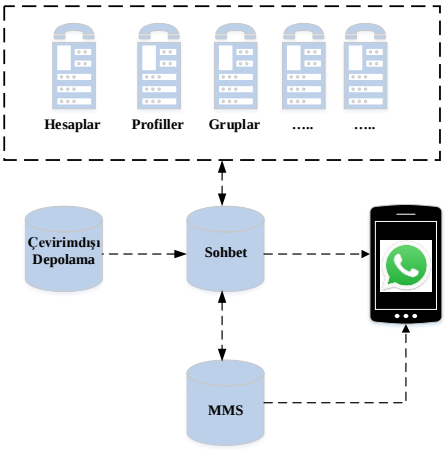
Adli bilişim incelemelerini normal bilişim incelemelerinden ayıran temel özellik yasal mevzuatlar çerçevesinde yapılan inceleme işlemlerini kapsamasıdır. Ülkemizde bilişim suçlarını düzenleyen toplu bir mevzuat ya da kanun bulunmamaktadır. Bilişim suçları ilgili oldukları kanunlara eklenen hükümler ile düzenlenmektedir. Ülkemizde bilişim suçları ile ilgili en kapsamlı durumlar Türk Ceza Kanunu (TCK)'nda belirtilmiştir. 5237 sayılı kanunun 243, 244, 245 ve 246. Maddeleri ile gerekli düzenlemeler yapılmıştır. TCK 124. Madde ile haberleşmenin engellenmesine yönelik suçlar tanımlanmıştır. Ayrıca TCK'da "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığında bulunan madde 135 ile "kişisel verilerin kaydedilmesi" suçu, madde 136 ile "kişisel verileri hukuka aykırı olarak verme ve ele geçirme" suçu, madde 138 ile "verileri yok etme" suçu konularında düzenlemeler bulunmaktadır. Bu kapsam açısından bakıldığında WhatsApp kullanımı, ilgili yasa maddelerini yakından ilgilendirmektedir. Suça konu olabilecek WhatsApp kullanımında inceleme sonucunda yasalara aykırı kullanımlar söz konusu olabilmektedir [12,13].

Literatürde WhatsApp uygulamasının adli bilişim incelenmesi üzerine belirli çalışmalar mevcuttur. Anglano [14] Android işletim sistemine sahip telefonlarda yüklü olan WhatsApp uygulamasını incelemiştir. Çalışmada, kişi listesi ve mesajların depolandığı veritabanında silme ya da değiştirme olması durumundaki farklılaşmanın adli bilişim açısından değerlendirilmesi sunulmuştur. Malekhosseini vd. [15] WhatsApp uygulamasını kullanan kullanıcıların durum ve sesli görüşmelerde bilgi paylaşımındaki kullanıcı gizlilik endişelerini incelemiştir. Sonuçlar yaş, cinsiyet gibi demografik özelliklerine bağlı olmak ile beraber kullanıcıların çoğunluğunda gizlilik kaygısının yüksek olduğunu göstermiştir. Sahu [6] akıllı telefonlar için adli incelemelerde kullanılabilecek verilerin analizi üzerine çalışmıştır. Çalışmada adli verilerin depolandığı veritabanları ve yolları incelenmiş ve sonuçlar sunulmuştur. Shortall ve Azhar [16] WhatsApp uygulamasını IOS, Android ve Windows telefonlar için Encase, UFED ve Oxygen Forensic yazılımları aracılığı ile incelenmiştir. Çalışmada inceleme için seçilen adli inceleme yazılımları ile elde edilen adli veriler değerlendirilmiştir. Sonuçlar incelendiğinde WhatsApp uygulamasından elde edilen yedeklenen mesajlara ulaşılabildiği ancak şifreli dosyaların şifresinin çözülemediği tespit edilmiştir.

Bu çalışmada Android işletim sistemine sahip bir telefon aracılığı ile WhatsApp uygulamasının dosya yapısı incelenerek adli bilişim açısından elde edilebilecek veriler sunulmuştur. Çalışmada, Bölüm 2'de WhatsApp kayıt işlemi, mesaj iletim yöntemi, veritabanı bilgileri, veri depolama alanı, veri edinimi ve analizi başlıkları incelenmiştir. Bölüm 3'de Android tabanlı bir telefonun rootlu ve rootsuz hali göz önüne alınarak telefon numarası, mesajlar, medya dosyaları, iletişim numaraları, konum gibi verilerin elde edilebilme süreci sunulmuştur. Son olarak Bölüm 4'de elde edilen bulgular değerlendirilmiş ve sonuçlar sunulmuştur.

2. WHATSAPP MESAJLAŞMA UYGULAMASI (WHATSAPP MESSENGER APPLICATION)

WhatsApp, Ejabberd (XMPP) sunucusunu kullanan gerçek zamanlı bir mesajlaşma uygulamasıdır. Bu sunucu, belirli bir saniyede iki veya daha fazla kullanıcı arasında anında ileti aktarımını kolaylaştırmaktadır. WhatsApp, Erlang programlama dili ile yazılmıştır. Ejabberd, Erlang dilinde yazılmış, açık kaynak kodlu bir Jabber (eş zamanlı veri aktarımı yapan protokol) sunucusudur [6]. WhatsApp'ın genel işlem yapısı Şekil 2'de verilmiştir.



Şekil 2. WhatsApp genel işlem yapısı
(WhatsApp general process structure)

WhatsApp veri alış verişini sağlayan XMPP kullanmaktadır. Aynı zamanda WhatsApp şebeke güvenliğini sağlamak için DSL olarak bilinen özel veri aktarım protokolünü kullanmaktadır. Bu yapıda mesaj gönderimi aşağıdaki sıra ile yapılır [3,17].

- Mesaj gönderildiğinde sunucuda sıraya girer.
- Mesaj, alıcıda mesajı almak için yeniden bağlanana kadar bekler.
- Mesaj gönderildiğinde, gönderen mesajın yanında çift onay işareti ile bilgilendirilir.
- Teslimattan sonra mesajlar anında sunucu belleğinden silinir.

2.1. WhatsApp Kayıt İşlemi (WhatsApp Registration Process)

WhatsApp, ilk sürümlerinde cep telefonunun IMEI numarasına dayalı olarak, bir posta sistemine kayıt aşamasında kullanılan bir kullanıcı adı ve şifre üretme sürecini izlemiştir. Ancak günümüzde bu yapı değiştirilerek IMEI numarasına bağımlı olmak yerine, mobil telefon numarasına 5 basamaklı bir PIN numarası göndererek gerçekleştirmektedir. Amaç WhatsApp uygulamasının tek telefona bağımlılığını ortadan kaldırmaktır [6,14].

2.2. WhatsApp Mesaj İletim Yöntemi (WhatsApp Message Sending Method)

- WhatsApp veri ağında çalışıp SMS kanalında çalışmadığından, diğer WhatsApp kullanıcılarına bağlanmak için merkezi bir sunucu kullanılır. Bu özellik sayesinde çevrimdışı kullanıcılara da mesaj gönderme yeteneği kazandırılmıştır. WhatsApp uygulaması ile bir mesaj gönderildiğinde sırasıyla aşağıdaki işlem adımları izlenir [18,19].
- WhatsApp çalıştırılınca dinleme ve sunucuya mesaj göndermek olmak üzere iki yuva açılır.
- İlk soket dinlenmeye başlanır.
- Telefon numarası ve dinleme yuvasının bağlantı noktasını içeren bir mesaj sunucuya gönderilir ve bir bildirim beklenir.
- Sunucu, mesajdaki telefon ve port numaralarını ve mesajın geldiği IP adresini kaydeder.
- Sunucu, uygulamaya bir bildirim gönderir.
- Uygulama onay alır ve ileti soketini kapatır.
- Hedef olarak telefon numarasıyla birlikte bir mesaj sunucuya gelir.
- Sunucu, telefon numarasıyla ilişkilendirilmiş IP adresini ve bağlantı noktası numarasını kullanır ve mesajı telefona aktarır.

İşlem genel mantığı *Veri gönderildi->Veri kabul edildi->Onay* şeklindedir.

2.3. WhatsApp Verileri (WhatsApp Data)

Uygulama kurulduktan sonra verileri *com.whatsapp* klasörü içerisinde depolamaktadır. Klasör içerisinde kullanıcı bilgilerinin tutulduğu üç ana dosya yapısı vardır. Bunlar veritabanları, günlük kayıtları ve medya bilgileridir. Adli inceleme açısından kullanıcının bilgilerine erişilebilmek için bu bilgilerin analiz edilmesi önemlidir [6, 18].

2.3.1. WhatsApp Veritabanı Bilgileri (WhatsApp Database Information)

WhatsApp gönderilen ve alınan mesajları kullanılan telefon üzerinde ya da bulut sistemlerde depolamaktadır. Veritabanı bilgilerine ancak telefon üzerinden ulaşmamız mümkündür, veritabanı dosyalarına ulaşabilmek için Android telefonlarda ROOT, IOS cihazlarında ise JAILBREAK işlemi yapılmalıdır aksi durumda bu bilgilere ulaşmak için SD kartta yer alan şifreli veritabanlarının kırılması gerekmektedir. Bu işlemlerden sonra elde edilecek verilerin kaynak adresleri Tablo 1'deki gibidir. Bu dizinler altındaki veriler kullanılarak kullanıcı etkileşimine ulaşılabilmektedir.

Tablo 1. İşletim sistemlerine göre verilerin veritabanı bilgilerinin konumu
(Location of database information of data according to operating systems)

İşletim Sistemi	Kaynak Adresleri
IOS	*/root/var/mobile/Applications/net.whatsap.WhatsApp/Documents/*
Android	*/ data / data / com.whatsapp/ databases / /sdcard/WhatsApp/Databases/*

Android cihazlarda, adli veri elde edilebilecek şekilde WhatsApp verilerini barındıran üç veritabanı mevcuttur, Bunlar *msgstore.db, wa.db* ve *web_sessions.db* veritabanlarıdır. *Msgstore.db* bir kullanıcı ve kişiler arasındaki sohbet görüşmeleri hakkında ayrıntılı bilgi içerir. *Wa.db* tüm WhatsApp kullanıcılarının kişileri hakkındaki bilgileri depolar. *Web_sessions.db* ise en son ne

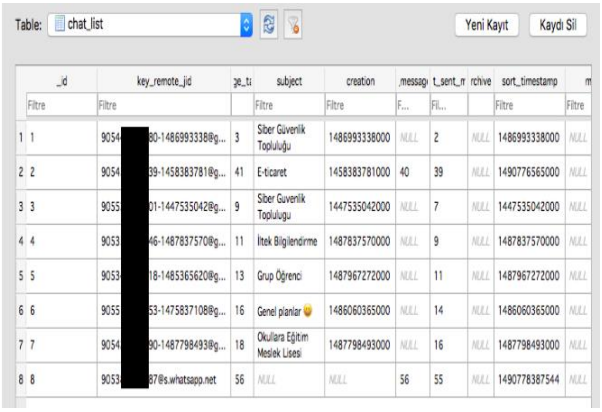
zaman oturum açıldığı, tarayıcı bilgileri, hangi işletim sistemi ile giriş yapıldığı gibi bilgileri içerir.

Msgstore.db veritabanı içerisinde yer alan *chat_list* ve mesajlar tabloları basit bir SQLite veritabanıdır. Mesajlar tablosu, bir kullanıcının gönderdiği veya aldığı tüm iletilerin bir listesini içerir.

WhatsApp kullanıcısının telefon numarasını hem kullanıcı hem de kişileri için benzersiz bir tanımlayıcı olarak kullanır. Bu tanımlayıcı ile:

- Kişinin telefon numarası,
- Mesaj içeriği,
- Mesaj durumu,
- Zaman damgaları
- Mesajın ekleri ile ilgili ayrıntılar gibi temel bilgilere ulaşılabilmektedir.

WhatsApp aracılığıyla gönderilen eklerin kendi tablo girişi vardır ve ileti içeriği paylaşılan fotoğraf/resim ile ilgili küçük resim ve bağlantı içeren bir girdi içerir. Bu ek doğrudan *msgstore.db* dosyasında saklanır. Buna ek olarak Şekil 3'de gösterildiği gibi, gönderilen iletiler enlem ve boylam koordinatları gibi konum bilgileri içerebilir, böylece denetleyicinin bir kullanıcının coğrafi konum bilgilerini haritalaması sağlanır.



Şekil 3. Msgstore.db yer alan chat_list ekran görüntüsü
(Chat_list screenshot in msgstore.db)

Chat_list tablosu, bir kullanıcının ilettiği tüm telefon numaralarının bir listesini içerir. Ancak kullanıcı kişilerinin tam listesi için *wa.db*'ye bakılması gereklidir. *Wa.db* telefon numarası, zaman damgası ve bir WhatsApp kullanıcısının kişilerinin tam listesi barındırır. Android'de veritabanlarına eriştiğinizde WhatsApp kişileri, mesajlar ve eklere ulaşmak mümkündür [6,8].

2.3.2. Veritabanı Dosyalarının Analizi (Database File Analaysis)

Veritabanı dosyalarını 'SQLite tarayıcısı' ile okunabilse de zaman damgaları ve verilerin gösterimi açık şekilde görülememektedir. Bu yüzden WhatsApp Xtract aracı kullanılmaktadır ve bu aracın önemli bir avantajı, değiş tokuş edilen medya içeriğinin HTML sayfasında görüntülenmesi ve medya klasörüne ayrı ayrı bakılmasının gerekmemesidir. Analiz edilen verileri karşılaştırmak için bu araç oldukça yararlı olabilmektedir. Bu aracın tüm özellikleri kullanışlı bir ara yüzde toplanır ancak mesajlar veritabanından silindikten sonra araç bunları geri alamaz. WhatsApp Xtract aracı yalnızca veritabanında bulunan statik bilgileri temsil edebilir.

Android güvenlik modelinin önemli bir kısmı, kurulumda her uygulamaya benzersiz bir Linux kullanıcısı ve grup kimliği atar. Yükleme sırasında işletim sistemi, uygulama için belirli bir dizin oluşturur ve yalnızca bu uygulamanın o dizinde depolanan tüm verilere erişmesine izin verir. Bu mekanizmalar, uygulamalar, bellek, izinler veya disk depolamayı paylaşmadığından, veri güvenliğini düşük seviyede sağlar.

Bununla birlikte, adli bilişim inceleme uzmanları öncelikle insan etkileşimiyle ilgili verilerle ilgilenir. Bu veriler farklı veri depolama ortamlarının incelenmesi ile çıkarılabilir ve analiz edilebilir. Android uygulamaları, verileri genellikle harici depolama ve dâhili depolama şeklinde iki konumda depolar. Harici depolama ortamında, veriler herhangi bir yerde saklanabilir ve yönetilebilir. Dâhili depolama alanında ise veri depolama Android API'leri tarafından kontrol edilir. Kalıcı veriler, NAND flaş belleğine, SD karta veya ağa depolanır. Uygulama yüklendiğinde, uygulama ile ilgili veriler aşağıda yolu belirtilen alanda yer alırlar.

- */Data/data/<paket_adı>*
- */data/data/com.whatsapp*

Bu alt dizinde pek çok uygulamada bulunan bir dizi standart alt dizin vardır. Uygulama geliştiricileri genellikle bu dizinde depolanan verileri kontrol eder. En yaygın alt dizinler *lib*, dosyalar, önbellek ve veritabanlarıdır. Uygulama, telefonun dâhili belleğinde saklanır. Uygulama otomatik olarak, WhatsApp kullanan kişileri gösteren telefon rehberleriyle senkronize olur. WhatsApp yüklü bir telefon açıldığında, '*com.WhatsApp*" işlemi, telefon açık olduğu sürece arka planda çalışan '*ExternalMediaManage*' ve '*MessageService*' hizmetlerini başlatmak için bir sinyal alır. Değiştirilen tüm mesajlar SQLite veritabanları olan *msgstore.db* ve *wa.db*'de saklanır. Veritabanları daha hızlı veri erişimi için RAM'e yüklenir. Genellikle RAM'de takas nedeniyle tüm içerik kalıcı olmayabilir veya üzerine yazılabilir durumdadır.

Mesajlar alındığında kullanıcılar mesajlar hakkında push mekanizması aracılığıyla haberdar olur, böylece WhatsApp hafızada, özellikle görünür bir süreçte, yüksek bir önceliği korur. Bu kullanıcıya bir e-posta hizmeti gibi tipik bir web sunucusundan onları indirmek zorunda kalmadan arka planda iletileri sürekli almaya olanak tanır. WhatsApp kullanıcı verilerini bir SQLite veritabanında (*msgstore.db, wa.db ve web_sessions.db*) saklar. Veritabanının konumu ve yapısı, platformdan platforma değişir. Cihazda sistemin bulunduğu kök dizin seçildiğinde

aşağıda yolu verilen alanda düz veritabanı dosyaları *wa.db* ve *msgstore.db* dosyaları bulunabilir.

- */data/data/com.whatsapp/databases/ msgstore.db and wa.db*

Web_sessions.db veritabanı içeriğine ise *web.whatsapp.com* aracılığı ile bilgisayar tarayıcısı üzerinden girilebilir.

Kök dizin seçilmediğinde SD karttaki yedeklenmiş WhatsApp klasörüne erişebilir. Bu klasör esas olarak üç alt klasörü içerir:

- */sdcard/WhatsApp/Databases*
- */sdcard/WhatsApp/Media*
- */sdcard/WhatsApp/ProfilePictures*

Veritabanı, SD kart üzerindeki şifreli bir dosya biçimindedir.

- */sdcard/WhatsApp/Databases/msgstore.db.crypt*

WhatsApp Xtract, şifreli bir *db* dosyasını (*msgstore.db.crypt*) girdi olarak alan ve çıktı olarak şifresi çözülmüş bir db dosyası (*msgstore.plain.db*) veren basit bir Python komut dosyası geliştirmiştir. Bu kod kullanılarak *db* dosyası extract edilir.

Çıktı dosyası, SQLite tarayıcı yazılımı kullanılarak okunabilir. WhatsApp Xtract aracıyla medya dosyalarını açabilir ve mesajları doğrudan HTML dosyasından görebiliriz. Dosyaların cihazdan SD karta yedeklenmesi her gün belirlenen saatte ya da kullanıcı seçimi ile yapılmaktadır. Şifresiz veritabanından veya medya klasöründen en yeni verilerin olmaması yalnızca o gün için uygulamanın en yeni veriyi SD karttaki veritabanında yedeklemediği anlamına gelmektedir [6,8,17].

3. WHATSAPP ANALİZİ VE ELDE EDİLEN BULGULAR (ANALYSIS OF WHATSAPP AND FINDINGS)

Bu çalışmada Android işletim sistemine sahip bir telefonun WhatsApp 2.17.106 sürümünün incelemeleri sunulmuştur. İnceleme yapılan telefon Android v.4.4.2 işletim sistemli, Samsung Galaxy Note 2, 2 GB RAM, 16 GB dâhili hafızaya sahiptir. Telefonun incelendiği bilgisayar ise MacBookAir 1.3 GHz Intel Core i5, 4 GB 1600 MHz DDR3 özelliğindedir. Telefon root yapılmadan ve rootlu haliyle incelenmiştir. İnceleme yapmak için SQLite DB Browser v.3.9.99, Kingo Root, File Explorer Mobil uygulamaları kullanılmıştır.

Bu çalışma ile SQLite programı yardımıyla rootlanmış telefondaki *wa.db*, *msgstore.db* ve *web_sessions.db* veritabanları incelenerek bu veritabanlarının içerisinde yer alan veriler değerlendirilmiştir.

Telefonda var olan WhatsApp verileri rootlu ve rootsuz olarak 2 biçimde elde edilmektedir.

Root işlemi, Android sistemlerde kullanıcıya sistem dosyalarına erişme, değiştirme gibi işlemleri yapma yetkisi tanımaktadır. Bu sayede kullanıcı, telefon üzerinde üretici firmanın yetkisi kadar bir yetki hakkına erişmiş olur.

Rootsuz telefonlarda, WhatsApp verileri SD kart ya da dâhili hafızada WhatsApp klasörü altında barındırılmaktadır. Barındırılan verilerin başkalarının eline geçme ihtimaline karşın WhatsApp tarafından *.crypt** uzantılı olarak şifreli bir biçimde telefonun içerisinde depolanmaktadır. Şifreli verilere erişebilmek için WhatsApp uygulamasının kullanıcı için tanımlamış olduğu KEY numarasının elde edilmesi gerekmektedir. KEY'ler AES 256 bit şifreleme biçiminde telefonun *data/data/com.whatsapp/files/key* dizininde tutulmaktadır ancak KEY bilgisine ulaşabilmek için mutlaka telefonda root yetkisi olmalıdır aksi durumda KEY'in elde edilmesi mümkün değildir.

Rootlu telefonlarda, WhatsApp verilerini elde etmek daha basit olduğundan daha fazla bilgi elde edebilmek için rootlama işlemine ihtiyaç duyulmaktadır. Rootlama işlemi telefonun bilgisayara bağlanılarak yapılacağı gibi direk telefonun içerisine uygulama yüklenerek de gerçekleştirilebilmektedir.

Bilgisayar ortamında rootlama işlem yapmak için yaygın olarak kullanılan Kingo Root adlı 3. Parti program kullanılmaktadır. Bilgisayara takılmış olan Android işletim sistemli telefonun öncelikle USB hata ayıklama modu aktif edilmektedir. Bu işlem sonrasında Kingo Root programı cihaz tarafından algılanmakta ve rootlama işlemi gerçekleştirilmektedir. Bilgisayar ortamına gerek kalmaksızın telefonda rootlama işlemi yapabilmek için 3. parti uygulamalardan olan ve yaygın olarak kullanılan King Root uygulaması kullanılabilir. Telefona yüklenen uygulama çalıştırıldığında, rootlama işlemi otomatik olarak yapılmaktadır.

Telefonda root yetkisine erişildikten sonra kök dizine erişmek için 3. parti mobil uygulamalar kullanılmaktadır. Yaygın olarak kullanılan mobil uygulamalardan bir tanesi olan ES File Explorer Manager uygulaması dosya ve uygulama yöneticisi özelliklerine sahip olup hem bilgisayarda hem de telefonlarda resim, video, müzik, metin dosyaları vb. dosyalara erişim sağlamaktadır. Bu özellikleri sebebiyle rootlanmış telefonda, kök dizine ulaşmak için bu veya buna benzer uygulamalar kullanılır.

Çalışmada ES File Explorer Manager aracılığıyla ulaşılan kök dizinden *data/data/com.whatsapp* dizinine girilerek WhatsApp ile ilgili veritabanları, log kayıtları ve key bilgilerine erişim sağlanmıştır. Rootlu telefonun inceleme uygulama adımları aşağıda verilmiştir.

- Cep telefonunun rootlama işlemi gerçekleştirilir ve ardından root dizinine ulaşmak için File Manager uygulaması telefona yüklenerek kök dizine ulaşılır.
- Kök dizinde *data/data/com.whatsapp/database* girilerek *wa.db*, *msgstore.db* ve *web_sessions.db* veritabanı dosyaları elde edilir.

- Bilgisayar ortamına aktarılan veritabanı dosyaları SQLite programı ile içeri aktarılır.

3.1. Veritabanı Dosyalarının İncelenmesi (Investigation of Database Files)

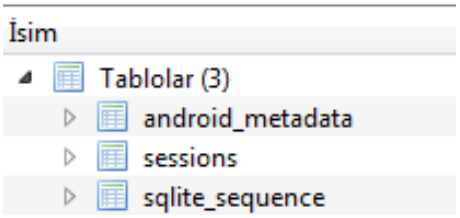
Adli bilişim uzmanları database içerisindeki *wa.db*, *msgstore.db* ve *web_sessions.db* veritabanı dosyalarına erişerek kullanıcı bilgilerine ulaşabilmektedir. Adli açıdan bu veritabanlarının içerikleri aşağıda sunulmuştur.

3.1.1. Web_sessions.db Veritabanı Analizi (Web_sessions.db Database Analysis)

İçerisine bilgisayar tarayıcısı üzerinden girilen *web.whatsapp.com* adresinde aşağıdaki bilgilere ulaşılabilmektedir.

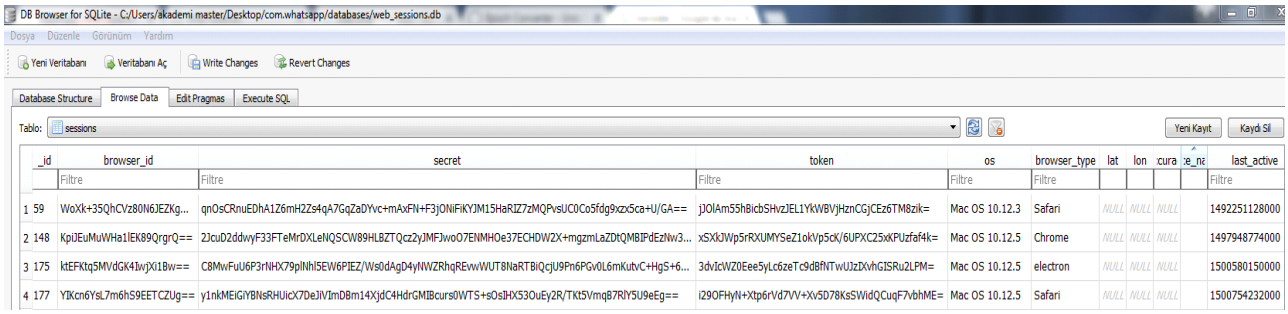
- En son ne zaman oturum açıldığı
- Hangi işletim sistemi (sürümü dâhil) üzerinde girildiği
- Tarayıcı adı (Safari, Chrome vb.) bilgisi
- Base64 şifrelemesi ile tutulan tarayıcıya özel ID bilgisi
- Oturum bilgisine ait base64 ile şifrelenmiş secret ve token bilgisi

Web_sessions.db dosyasında Şekil 4'de gösterildiği gibi 3 tablo bulunmaktadır.



Şekil 4. SQLite DB Browser programından elde edilen web_sessions.db veritabanının içeriğindeki tablolar
(The tables in the contents of the web_sessions.db database obtained from the SQLite DB browser program)

Şekil 5'de içeriği verilen *sessions* tablosu kullanıcının oturum açtığı platformla ilgili bilgileri barındırmaktadır.



Şekil 5. SQLite DB Browser programının sessions tablosunun içeriği
(Contents of the session table of SQLite DB Browser program)

3.1.2. Wa.db Veritabanı Analizi (Wa.db Database Analysis)

Wa.db içerisinde adli inceleme açısından verinin elde edilebileceği ve aşağıda verilen 5 temel tablo bulunmaktadır.

- *android_metadata,*
- *sqlite_sequence,*
- *system_contacts_version_table,*
- *wa_contact_capabilities,*
- *wa_contacts*

SQLite programında Browse Data alanına girilerek elde edilen tabloların içerikleri Tablo 2'de verilmiştir.

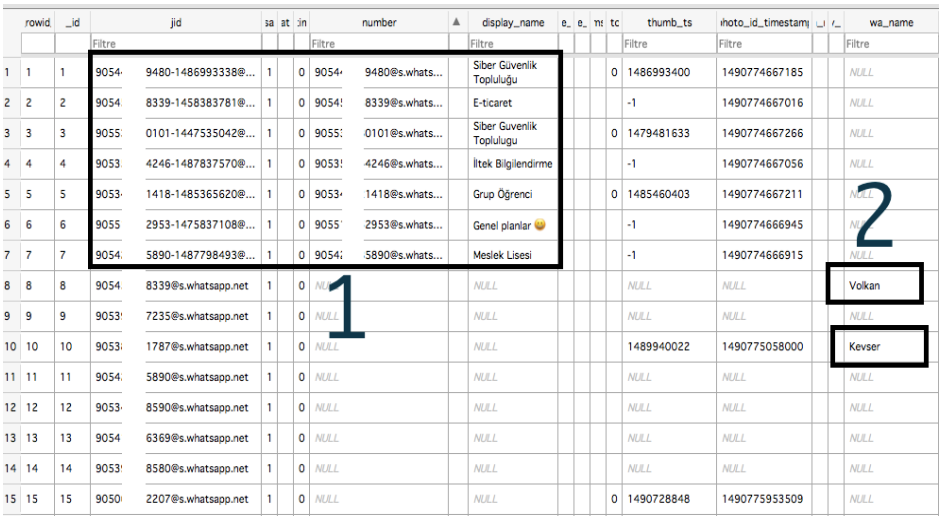
Tablo 2. File Manager programından elde edilen wa.db veritabanı içerisinde bulunan tablolar
(The tables in the wa.db database obtained from the File Manager program)

Veritabanınında Bulunan Tablolar	Tablo İçerikleri
android_metadata	Uygulamanın yüklü olduğu ülke kodu
sqlite_sequence	Toplam mesaj sayısı
system_contacts_version_table	Versiyon bilgileri
wa_contact_capabilities	Maksimum 44 kullanıcı olmak üzere kişi listesindeki WhatsApp kullanıcılarının WhatsApp ID bilgileri
wa_contacts	İletişim halinde olunan kişi ve grupların kullanıcı adı ve ID bilgileri

Adli bilişim incelemeleri açısından *Wa.db* veritabanındaki en önemli tablo *wa_contacts* tablosudur. *Wa_contacts* tablosu incelendiğinde aşağıdaki bilgilere ulaşılabilmektedir.

- Konuşulan kişiler,
- Konuşma tarihi,
- Kayıtlı kişilerin telefon ve kullanıcı adı,
- JID bilgileri,
- Üye olunan gruplar ve bu grupları kuran kişilerin telefon numaraları
- WhatsApp JID'leri

Şekil 6'da *wa_contacts* tablosundan elde edilen grup ve yer alan 1 numaralı alanda üye olunan gruplar ve bu grupları kuran kişi bilgileri (*telefon.jid*) yer almaktadır.



rowid	_id	jid	number	display_name	thumb_ts	photo_id_timestamp	wa_name
1	1	9480-1486993338@...	9480@s.whats...	Siber Güvenlik Topluluğu	1486993400	1490774667185	NULL
2	2	8339-1458383781@...	8339@s.whats...	E-ticaret	-1	1490774667016	NULL
3	3	0101-1447535042@...	0101@s.whats...	Siber Guvenlik Toplulugu	1479481633	1490774667266	NULL
4	4	4246-1487837570@...	4246@s.whats...	İltek Bilgilendirme	-1	1490774667056	NULL
5	5	1418-1485365620@...	1418@s.whats...	Grup Öğrenci	1485460403	1490774667211	NULL
6	6	2953-1475837108@...	2953@s.whats...	Genel planlar	-1	1490774666945	NULL
7	7	5890-1487798493@...	5890@s.whats...	Meslek Lisesi	-1	1490774666915	NULL
8	8	8339@s.whatsapp.net	NULL	NULL	NULL	NULL	Volkan
9	9	7235@s.whatsapp.net	NULL	NULL	NULL	NULL	NULL
10	10	1787@s.whatsapp.net	NULL	NULL	1489940022	1490775058000	Kevser
11	11	5890@s.whatsapp.net	NULL	NULL	NULL	NULL	NULL
12	12	8590@s.whatsapp.net	NULL	NULL	NULL	NULL	NULL
13	13	6369@s.whatsapp.net	NULL	NULL	NULL	NULL	NULL
14	14	8580@s.whatsapp.net	NULL	NULL	NULL	NULL	NULL
15	15	2207@s.whatsapp.net	NULL	NULL	1490728848	1490775953509	NULL

Şekil 6. Wa_contacts tablosundan elde edilen grup ve kullanıcı bilgileri
(Group and user information from the wa_contacts table)

2 numaralı alanda ise sohbet edilen kişilerin WhatsApp uygulamasındaki kullanıcı adları görülmektedir.

3.1.3. Msgstore.db Veritabanı Analizi (Msgstore.db Database Analysis)

Adli bilişim açısından bir diğer önemli veritabanı dosyası *msgstore.db*'dir. Bu veritabanı dosyası SQLite programı ile incelendiğinde:

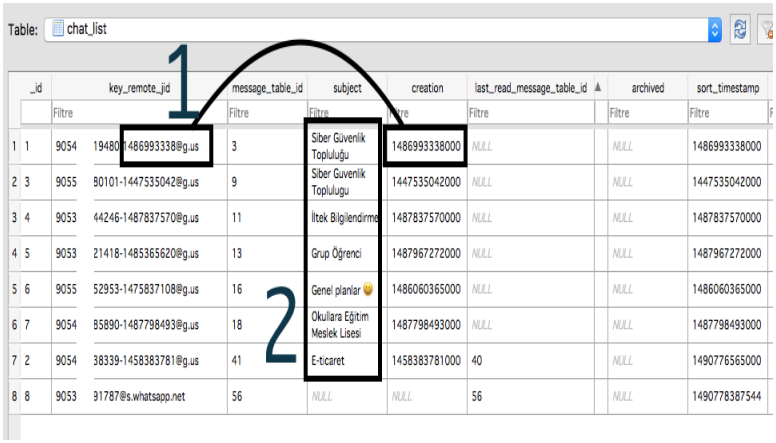
- Kişinin telefon numarası,
- Mesaj içeriği,
- Mesaj durumu,
- Zaman damgaları
- Mesajdaki eklerle ilgili ayrıntı

gibi verilere ulaşılabilmektedir. Tablo 3'de *Msgstore.db* veritabanı dosyasının tablo yapısı ve içerikleri verilmiştir.

Tablo 3. Msgstore.db veritabanı dosyasının tablo içeriği
(Table contents of the Msgstore.db database file)

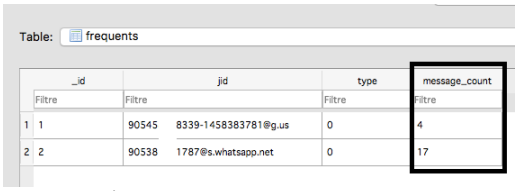
Veritabanınında Bulunan Tablolar	Tablo İçeriği
chat_list	Kayıtlı sohbet ve grupların listesi
frequents	Sıkça konuşulan kişi ve grupların bilgisi ve toplam mesaj sayısı bilgisi
group_participants	Grup üyelerinin bilgisi
group_participants_history	Grup üyelerinin geçmiş bilgileri
media_streaming_sidecar	İnternet üzerinden sıkıştırılmış biçimde gönderilen video veya ses içeriği
message_thumbnails	Mesajların içeriğinde yer alan ön izleme resimleri
messages	Gönderilen ve alınan mesaj içerikleri
messages_edits	Düzenlenmiş mesajların içerik bilgisi
messages_fts	Gönderici ve alıcı bilgisi olmadan sadece mesaj içerikleri
messages_fts_content	Gönderici ve alıcı bilgisi olmadan mesaj içeriği ve her mesaja ait ID numarası
messages_links	Mesaj içeriğinde yer alan URL listeleri
messages_vcards	Telefon rehberindeki kişi bilgileri
messages_vcards_jids	Telefon rehberindeki kişilerin WhatsApp ID bilgisi

Şekil 7'de *chat_list* tablosundaki *key_remote_jid* sütununda iletişimde olunan gruplar ve kişiler bilgisinin tutulduğu görülmektedir. Burada, 1 numaralı alanda yer alan şekilde grubu kuran kişi ve grup kurulma Şekil 7'de *chat_list* tablosundaki *key_remote_jid* sütununda iletişimde olunan gruplar ve kişiler bilgisinin tutulduğu görülmektedir. Burada, 1 numaralı alanda yer alan şekilde grubu kuran kişi ve grup kurulma zamanı ile ilişkilendirip *jid* bilgileri elde edilmektedir. 2 numaralı alanda ise grup isimleri yer almaktadır. Aktif olarak konuşulan kişi ve grupların bilgisi ve toplam mesaj sayısı bilgisi *frequents* tablosunda tutulmaktadır.



Şekil 7. Msgstore.db içerisindeki chat_list tablosu içeriği
(Chat_list table contents in Msgstore.db)

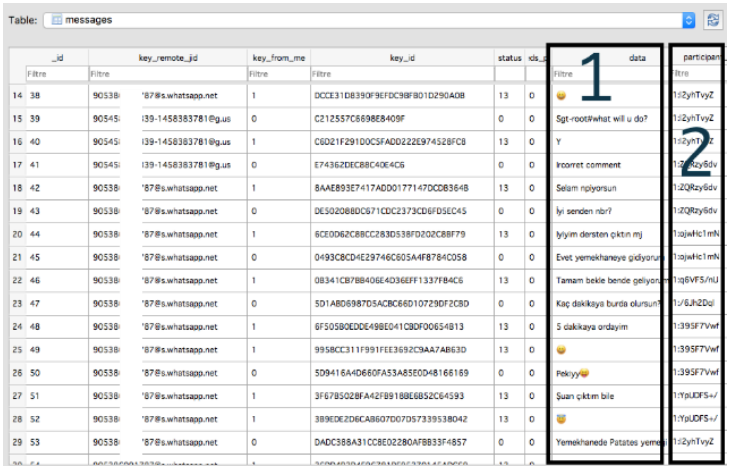
Şekil 8'de ise *frequents* tablosunun içeriği gösterilmiştir.



Şekil 8. İletişim kurulan toplam mesaj sayısı
(The number of messages contacted)

Frequents tablosu *Message_count* sütununda toplam mesaj sayısı tutulmaktadır. *Msgstore.db* veritabanında en önemli tablolardan birisi de Şekil 9'da içeriği verilen *messages* tablosudur.

Bu tabloda sohbet geçmişi, her mesajın *key* bilgisi ve *hash* değerleri tutulur. Şekil 9'da 1 numaralı alan sohbet geçmişini, 2 numaralı alan ise her mesaja özel *hash* değerini göstermektedir.



Şekil 9. Messages tablosunda bulunan sohbet geçmişi ve her mesajın hash değeri
(The chat history in the Messages table and the messages hash value)

3.2. Log Dosyalarının Analizi (Log Files Analysis)

Log dosyaları *com.whatsapp\files\Logs* klasörü altında tutulmaktadır. Uygulama kullanıcı ile ilgili yapılan işlemleri log dosyalarında saklamaktadır. Log dosyaları incelenerek adli bilişim açısından çeşitli veriler elde edilebilmektedir.

3.2.1. Şarj Durumu (Battery Status)

Şarj durumu inceleme yapacak kişiye Şekil 10'da verildiği gibi şarj yüzdesi ve batarya sağlığının durumu bilgisi vermektedir.

```
2017-07-25 08:39:17.389 LL I M [1:main] battery changed;
newEvent=BatteryChange health=good, level=39, plugged=0, scale=
100, percent=39.0] 2
                    1
```

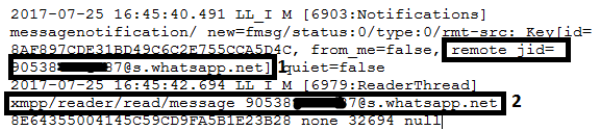
Şekil 10. Şarj durum bilgisi
(Battery status information)

Şekil 10'da gösterilen 1 numaralı alanda batarya durumu, 2 numaralı alanda ise bataryanın şarj yüzdesi elde edilebilir.

3.2.2. Mesaj Gönderen Bilgisi (Message Sending Information)

Mesaj gönderen bilgisi; mesaj şifreleri, her saniye WhatsApp ile etkileşim halinde olup olmadığının kontrolü, hangi mesajın ne zaman okunduğu ve ne zaman cevap

yazıldığı bilgisi gibi temel bilgileri içermektedir. Şekil 11'de, 1 numaralı alanda gönderen kişinin telefon numarasını, 2 numaralı alanda ise mesajın okunduğunu yani karşı taraftan geldiği bilgisini tutmaktadır.



Şekil 11. Mesaj gönderen bilgisi
(Message sending information)

Aynı zamanda *com.whatsapp\files\Avatars* dizini kişi listesinde yer alan kişilerin profil fotoğraflarına erişilebilmektedir.

3.3. Medya Verileri (Media Data)

Çalışmada, bir diğer inceleme alanı ise medya dosyalarıdır. Medya dosyaları telefonda, *sdcard/whatsapp/media* veya *dâhili depolama/whatsapp/media* klasörü altında barındırılmaktadır. Belirtilen dosya yolundaki *media* klasörü incelendiğinde içerdiği klasörler ve içerikleri Tablo 4'de verilmiştir.

Tablo 4. Msgstore.db veritabanı dosyasının tablo yapısı
(Table structure of the Msgstore.db database file)

Klasör İsmi	Klasör İçeriği
WhatsApp Images	WhatsApp üzerinden gönderilen ve alınan tüm resim bilgileri
WhatsApp Voice Notes	WhatsApp üzerinden WhatsApp ses kayıt özelliği kullanılarak gönderilen/alınan tüm ses kayıtları ([YIL][AY] klasörleri içerisinde)
WhatsApp Documents	WhatsApp tarafından gönderilen/alınan ve WhatsApp tarafından desteklenen tüm dosya formatlarına erişim
WhatsApp Animated Gifs	WhatsApp tarafından gönderilen/alınan GIF dosyaları
WhatsApp Video	WhatsApp tarafından gönderilen/alınan videolar
WallPaper	Kullanıcı tarafından, WhatsApp arka planı yapılan görsellere erişim
WhatsApp Audio	WhatsApp üzerinden gönderilen/alınan ses verileri
WhatsApp Profile Photos	Kullanıcıya ait profil fotoğrafları bilgisi

Adli inceleme yapılırken uygulamanın *medya* verilerine erişilmek isteniyor ise SD kart veya dâhili hafızada yer alan *WhatsApp/media* dizini incelenmelidir.

Ayrıca WhatsApp mesajlaşma uygulamasında 2.18.46 sürüm numarası ile mevcut veritabanlarına *emojidictionary.db, google_app_measurement_local.db, google_app_measurement.db, hsmpacks.db, location.db, media.db* olmak üzere 6 yeni veritabanı eklenmiştir Bu veritabanları incelendiğinde anlamlı bilgi barındıran *emojidictionary.db* dosyası, WhatsApp Messenger içerisinde kullanılan emojilerin ikon ve isimlerini tutmaktadır. Aynı zamanda bu versiyon ile WhatsApp uygulamasının kullanıcılara sunmuş olduğu durum paylaşma özelliği *Msgstore.db* veri tabanının *message_quotes* tablosunun *key_remote_jid* sütununda *status@broadcast* olarak kayıt edilmektedir. Kullanıcı rehberinde ekli olan ve durum paylaşan kişilerin durum içerik bilgileri bu alanda depolanmaktadır. Durum olarak paylaşılan ve veritabanına kayıt edilen medya verilerinin url adreslerine yalnızca 24 saat erişilmektedir.

3.4. Elde Edilen Verilerin Adli Bilişim Açısından Değerlendirilmesi (Evaluation of the Data Obtained in Terms of Digital Forensics)

Çalışmada WhatsApp uygulamasının kullanıldığı Android işletim sistemi tabanlı mobil cihazlardan elde edilebilecek veriler rootlu ve rootsuz incelenmesi ile elde edilen bulgular Tablo 5'de verilmiştir.

Tablo 5. Msgstore.db veritabanı dosyasının tablo yapısı
(Table structure of the Msgstore.db database file)

Veriler	Rootsuz Telefon	Rootlu Telefon
Msgstore.db	Şifreli	Şifresiz
Wa.db	Bulunamadı	Bulundu
Telefon Numarası	Şifresiz	Şifresiz
Mesajlar	Şifresiz	Şifresiz
Medya Dosyaları	Şifresiz	Şifresiz
İletişim Numaraları	Şifresiz	Şifresiz
Lokasyon	Şifresiz	Şifresiz
SQL Sorgusu	Şifresiz	Şifresiz
Profil Fotoğrafı	Erişim Sağlanamadı	Erişim Sağlandı
Loglar	Erişim Sağlanamadı	Erişim Sağlandı
Dizin Yapısı	Erişim Sağlanamadı	Erişim Sağlandı
Silinen Mesajlar	Erişim Sağlanamadı	Erişim Sağlanamadı
Silinen Medyalar	Erişim Sağlanamadı	Erişim Sağlanamadı
Android API	Erişim Sağlanamadı	Erişim Sağlanamadı

Tablo 5 incelendiğinde, root yapılmış telefonda *Msgstore.db* dosyası şifresiz olarak elde edilirken root yapılmamış telefonda bu dosya şifreli olarak elde edilmiştir. *Wa.db* dosyası ise root yapılmamış telefonda elde edilememiştir. Profil fotoğrafı, loglar ve dizin yapısı yine root yapılmış telefonda incelenebilecek formda bulunmuştur. Mesajlar, telefon numarası, medya dosyaları, iletişim numaraları, lokasyon, SQL sorgusu rootlu ve rootsuz telefonda şifresiz olarak incelenebilmiştir.

Silinen mesajlar, silinen medyalar ve ANDROID API'ler ise her iki özellikte de elde edilememiştir. Bunun nedeni

ise WhatsApp verileri yedeklemeye dayalı olarak tutmaktadır. Bu yedekleme işlemi telefon üzerinde belirli saatlerde otomatik ya da kullanıcı isteğiyle gerçekleşmektedir. Eğer kullanıcının telefonunda bu iki durumdan biri gerçekleşmemiş ise silinen verilere ulaşılması için WhatsApp dosyalarını incelemek yetersiz kalacaktır. Silinen verileri kurtarmak için veri kurtarma yeteneklerine sahip adli bilişim yazılımlarının kullanılmalıdır.

4. SONUÇ VE ÖNERİLER (RESULTS AND SUGGESTIONS)

Adli bilişim elektronik ortamda mevcut verilerin güvenliğinin sağlanması için alınması gereken önlemleri, hukuki sürece yardımcı olabilecek şekilde verilerin incelenmesi ve değerlendirilmesi olarak tanımlanabilir. Günümüzde elektronik ortamda yaygın kullanılan programlar ve uygulamaların kendilerine ait özel dosya yapısı bulunmaktadır. Bir adli bilişim uzmanı yaygın kullanılan bu uygulamaların dosya yapısını düzgün ve belirli standartlara uygun olarak analiz edebilirse hem hukuki süreci hızlandırmış olur hem de amaçlanan verinin elde edilmesi mümkün hale gelebilir. Bu çalışmada WhatsApp v.2.17.106 sürümüne sahip bir telefon rootlu ve root yapılmadan incelenerek çeşitli vakalarda adli bilişim uzmanları için elde edilebilecek veriler değerlendirilmiştir. Adli bilişim inceleme uzmanlarının uygulama dosyaları, bu dosya içeriklerinin neler olduğunu ve hangi verilerin tutulduğunun bilinmesi incelemeyi kolaylaştırmaktadır. Bu nedenle çalışmada sunulan bulgular WhatsApp uygulamasının yapısını ortaya koymaktadır.

Çalışmada Android işletim sistemine sahip bir telefonda WhatsApp uygulaması veritabanı, medya ve log dosyaları başlıkları ile ele alınarak incelenmiştir. Veritabanında web_sessions, wa ve msgstore dosyalarına erişim ve içerik bilgileri sunulurken aynı zamanda log dosya analizi ile telefonda şarj durumu ve mesaj gönderim bilgileri ayrıntılı olarak değerlendirilmiştir. Aynı zamanda WhatsApp programı vasıtası ile gönderilen ses, video, kullanıcı profil resimleri, sohbet arka planı gibi adli bilişim açısından büyük önem taşıyan verilerin konumu ve elde edilme süreci sunulmuştur.

KAYNAKLAR (REFERENCES)

[1] E. Casey, **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**, Academic Press, 2011.

[2] E. Yılmaz, H. Ulus, S. Gönen, "Bilgi Toplumuna Geçiş Ve Siber Güvenlik", *Bilişim Teknolojileri Dergisi*, 8(3), 133-146, 2015.

[3] K. P. O'Hara, M. Massimi, R. Harper, S. Rubens, J. Morris, "Everyday Dwelling with WhatsApp", **17th ACM Conference on Computer Supported Cooperative Work & Social Computing**, Baltimore, A.B.D., 1131-1143, 15-19 Şubat 2014.

[4] M. Orakcı, I. Kök, H. Çakır, "Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi", *Bilişim Teknolojileri Dergisi*, 9(2), 137-145, 2016.

[5] E. Casey, **Handbook of Digital Forensics and Investigation**, Academic Press, 2009.

[6] S. Sahu, "An Analysis of WhatsApp Forensics in Android Smartphones", *International Journal of Engineering Research*, 3(5), 349-350, 2014.

[7] A. S. Şirikçi, N. Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi", *Bilişim Teknolojileri Dergisi*, 5(3), 29-34, 2012.

[8] K. Church, R. Oliveira, "What's up with Whatsapp?: Comparing Mobile Instant Messaging Behaviors with Traditional SMS", **15th International Conference on Human-Computer Interaction with Mobile Devices and Services**, Münih, Almanya, 352-361, 27-30 Ağustos 2013.

[9] İnternet: The Statistics Portal, https://www.statista.com/, 01.07.2017.

[10] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, V. K. Katos, "A Critical Review of 7 Years of Mobile Device Forensics", *Digital Investigation*, 10(4), 323-349, 2013.

[11] R. P. Mislan, E. Casey, G. C. Kessler, "The Growing Need for on-Scene Triage of Mobile Devices", *Digital Investigation*, 6(3), 112-124, 2010.

[12] M. Turan, Ö. Külcü, "Türkiye'de bilişim suçlarının tanımlanması ve yaşanan ihlallere yönelik içerik analizi", *Türk Kütüphaneciliği*, 28(1), 18-46, 2014.

[13] H. Hekim, O. Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158, 2013.

[14] C. Anglano, Forensic "Analysis of WhatsApp Messenger on Android Smartphones", *Digital Investigation*, 11(3), 201-213, 2014.

[15] R. Malekhosseini, M. Hosseinzadeh, K. Navi, "Evaluation of users' privacy concerns by checking of their WhatsApp status", *Journal of Software: Practice and Experience*, 48(5), 1143-1164, 2018.

[16] A. Shortall, M. H. B. Azhar, "Forensic acquisitions of WhatsApp data on popular mobile platforms", **Sixth International Conference on Emerging Security Technologies (EST)**, Braunschweig, Almanya, 13-17, 3-5 Eylül 2015.

[17] F. Karpisek, I. Baggili, F. Breitinger, "WhatsApp Network Forensics: Decrypting and Understanding the WhatsApp Call Signaling Messages", *Digital Investigation*, 15, 110-118, 2015.

[18] B. Carrier, **File System Forensic Analysis**, Addison-Wesley Professional, 2005.

[19] A. Hoog, **Android Forensics: Investigation, Analysis and Mobile Security for Google Android**, Elsevier, 2011.