T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MOBİL SOHBET UYGULAMALARININ İNCELENMESİNDE ADLİ ANALİZ MODELİNİN OLUŞTURULMASI

Sabri ERDEMİR

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği

AĞUSTOS 2021

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

MOBİL SOHBET UYGULAMALARININ İNCELENMESİNDE ADLİ ANALİZ MODELİNİN OLUŞTURULMASI

Tez Yazarı
Sabri ERDEMİR

Danışman
Dr. Öğr. Üyesi Aytuğ BOYACI

AĞUSTOS 2021
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Mobil Sohbet Uygulamalarının İncelenmesinde Adli Analiz Modelinin Oluşturulması
Yazarı:	Sabri ERDEMİR
İlk Teslim Tarihi:	13.07.2021
Savunma Tarihi:	10.08.2021

TEZ ONAYI

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

		İmza	
Danışman:	Dr. Öğr. Üyesi Aytuğ BOYACI MSÜ Hava Harp Okulu Dekanlığı Bilgisayar Mühendisliği Bölümü		Onayladım
Başkan:	Doç. Dr. Türker TUNCER Fırat Üniversitesi Teknoloji Fakültesi		Onayladım
Üye:	Dr. Öğr. Üyesi Oğuz ATA Altınbaş Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi		Onayladım

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

İmza

Doç. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Mobil Sohbet Uygulamalarının İncelenmesinde Adli Analiz Modelinin Oluşturulması" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

10.08.2021

Sabri ERDEMİR

ÖNSÖZ

Günümüzde internet kullanımı ile paralel olarak mobil cihazların kullanımının yaygınlaşması neticesinde bu cihazlar üzerinde çalışan birçok uygulama geliştirilmiştir. Bu uygulamalara bakıldığında kullanım olarak sohbet uygulamalarının daha sık uygulama marketlerinden indirildiği ve kullanıldığı görülmektedir.

Mobil sohbet uygulamalarının yaygın kullanımı, ülkelerin mevcut sistemler ile iletişim tespiti ve suçun aydınlatması konularında yetersiz kalması mobil cihazların incelenmesi gerekliliğini doğurmaktadır. Bu incelemelerde ise ortaya birtakım zorluklar çıkmaktadır. Kullanılan inceleme yazılımları bu zorlukları kısmen aşmakta fakat aşamadığı ve tanımlayamadığı durumlarda herhangi bir veri getirememektedir. Böyle bir inceleme sonucunda var olan veriler inceleme yazılımları tarafından tanımlanmadığından yapılan incelemelerin eksik kaldığı ve soruşturma konusuna herhangi bir faydasının olmadığı anlaşılmaktadır.

Bu tez çalışmasında sohbet uygulamalarına ait veri tabanı dosyalarından elde edilen bilgiler doğrultusunda bir karşılaştırma tablosu oluşturularak manuel yöntemler ile mobil sohbet uygulamalarının adli analizi modeli ortaya konulmuştur.

Akademik çalışmalarım boyunca benden hiçbir yardımını ve desteğini esirgemeyen değerli büyüğüm ve danışmanım Sayın Dr. Öğr. Üyesi Aytuğ BOYACI'ya şükranlarımı sunarım.

Ayrıca hayatımın tüm safhalarında desteklerini benden esirgemeyen aileme ve eşime minnet ve şükranlarımı sunarım.

Sabri ERDEMİR
ELAZIĞ, 2021

İÇİNDEKİLER

Sayfa

ÖZET

Mobil Sohbet Uygulamalarının İncelenmesinde Adli Analiz Modelinin Oluşturulması

Sabri ERDEMİR

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Ağustos 2021, Sayfa: xii + 70

Mobil sohbet uygulamalarının yaygın kullanımı, ülkelerin mevcut sistemler ile iletişim tespiti ve suçun aydınlatması konularında yetersiz kalması mobil cihazların incelenmesi gerekliliğini doğurmaktadır. Bu incelemelerde ise ortaya birtakım zorluklar çıkmaktadır. Kullanılan inceleme yazılımları bu zorlukları kısmen aşmakta fakat aşamadığı ve tanımlayamadığı durumlarda herhangi bir veri getirememektedir. Böyle bir inceleme sonucunda var olan veriler inceleme yazılımları tarafından tanımlanmadığından yapılan incelemeler eksik kalmakta ve soruşturma konusuna herhangi bir fayda sağlamamaktadır.

Yapılan bu tez çalışmasında imajı alınabilen mobil cihazların imajları üzerinden, imajı alınamayan mobil cihazların işletim sistemlerine uygun olarak sanal makinelerde oluşturulan işletim sistemleri üzerinden istenilen incelemeler gerçekleştirilmiştir. Her bir sohbet uygulaması için oluşturulan senaryolar üzerinden birinci aşamada mevcut inceleme yazılımları ile mobil sohbet uygulamalarının analizleri yapılmış olup ikinci aşamada ise mobil sohbet uygulamalarına ait veri tabanı dosyaları manuel olarak incelenmiş, sohbet uygulamasına ait kullanıcı verilerini tutan veri tabanı dosyalarına bakılarak hangi bilgilerin elde edilebileceği tespit edilmiştir.

Sonuç olarak incelenen sohbet uygulamalarından elde edilen bu bilgiler doğrultusunda bir karşılaştırma tablosu oluşturularak manuel yöntemler ile mobil sohbet uygulamalarının adli analizi modeli ortaya konulmuştur.

Anahtar Kelimeler: Adli Bilişim, Mobil Sohbet Uygulaması, Veri Tabanı

ABSTRACT

Establishment Of Forensic Analysis Model In The Investigation Of Mobile Chat Applications

Sabri ERDEMİR

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

August 2021, Pages: xii + 70

The widespread use of mobile chat applications, the inadequacy of countries in detecting communication with existing systems and illuminating crimes necessitate the examination of mobile devices. Some difficulties arise in these studies. The inspection software used partially overcomes these difficulties but cannot bring any data in cases where it cannot overcome and identify. Since the data available as a result of such an examination is not defined by the examination software, the examinations are incomplete and do not provide any benefit to the subject of the investigation.

In this thesis study, the desired examinations were carried out on the images of the mobile devices that can be imaged and the operating systems created in virtual machines in accordance with the operating systems of the mobile devices that cannot be imaged. In the first stage, the existing review software and mobile chat applications were analyzed through the scenarios created for each chat application.

As a result, a comparison table was created in line with this information obtained from the chat applications examined, and a forensic analysis model of mobile chat applications was put forward with manual methods.

Keywords: Digital Forensic, Mobile Chat Application, Database

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

CMK	: Ceza Muhakemesi Kanunu
PDA	: Personal Digital Assistant
OS	: Operating System
SDK	: Software Development Kit
HTML	: Hyper Text Markup Language
SMS	: Short Message Service
DEFT	: Digitan Evidence & Forensics Toolkit
BT	: Bilgi Teknolojileri
CDMA	: Code Division Multiple Access
VMDK	: Virtual Machine Disk
DB	: Database
BLOB	: Binary Large Object
UID	: User Identifier
ENC	: Encryption

1. GİRİŞ

Suç ve suçlu ile mücadelede ülkelerin oldukça zorlandığı bir dönemdeyiz. Teknolojinin baş döndürücü bir şekilde gelişmesi sonucu olarak kişiselleşen teknolojik araçların yaygınlaşması suç ile ilgili maddi delillerin tespitinde adli makamları oldukça zorlamaktadır. Özellikle mobil cihazlar ve bu cihazlara ait mobil uygulamalar gerek geliştirilme metodları (güvenlik tedbirleri, şifreleme algoritmaları ve uçtan uca şifreleme) gerek sunucularının başka ülkelerde bulunması açısından mobil cihaza erişim yapmadan bilgi elde etmeyi neredeyse imkânsız hale getirmektedir. Maddi delil elde edebilmek amacıyla mobil cihaz ile ilgili adli makamlar tarafından verilen inceleme kararına istinaden analizler yapılmaktadır. Yapılacak olan bu analizler için öncelikle mobil cihazın adli kopyasının alınması gerekmektedir. Adli kopya alınması aşamasında mobil cihazlarda birtakım sorunlar yaşanmaktadır. Mobil cihazın marka/modeli ve yüklü işletim sisteminin adli kopya alacak yazılım veya donanım tarafından tanımlanamaması en sık karşılaşılan sorunlardandır. Adli kopya alma ile ilgili ücretli ve ücretsiz araçlara bu çalışmada geniş bir şekilde yer verilmiştir. Adli kopya alınması sonrasında kopyası alınan mobil cihazın içerisindeki mobil uygulamalar ayrı ayrı analiz edilmesi gerekmektedir. Her mobil uygulamanın uygulama güvenlik tedbirleri farklılık göstermektedir. Mobil uygulamanın açılması esnasında şifreleme uygulanıp uygulanmadığı değerlendirilmeli eğer şifreleme uygulanmışsa bunu aşabilmek için çeşitli şifre kırma teknikleri uygulanmalıdır. Yine uygulama içerisinde yer alan diğer verilerin anlamlandırılabilmesi için farklı yaklaşımlar ve yöntemler geliştirilmesi ya da bu işlemleri otomatizme edecek karar destek sistemlerine gerek duyulmaktadır. Bu çalışmada mobil cihaz işletim sistemleri ile bu sistemler üzerinde adli kopya alma ve inceleme işlemlerinin yürütülebilmesi için mevcut ücretli ve ücretsiz yazılımlardan bahsedilmiş, sıklıkla kullanılan bazı sohbet uygulamalarının analizlerinin örneklerine detaylı bir şekilde yer verilmeye çalışılmıştır.

Bu tez çalışmasında imajı alınabilen mobil cihazların imajları üzerinden, imajı alınamayan mobil cihazların işletim sistemlerine uygun olarak sanal makinelerde oluşturulacak işletim sistemleri üzerinden istenilen incelemeler gerçekleştirilmiştir. Her bir sohbet uygulaması için oluşturulacak olan senaryolar üzerinden birinci aşamada mevcut inceleme yazılımları ile mobil sohbet uygulamalarının analizleri yapılmış olup ikinci aşamada ise mobil sohbet uygulamalarına ait ver tabanı analizleri incelenerek manuel olarak incelenen veri tabanındaki tutulan veriler arasındaki farklar değerlendirilmiştir. Sonuç olarak mevcut inceleme yazılımları tarafından getirilemeyen verilerin manuel olarak gerçekleştirilen veri tabanı analizi sayesinde ortaya koyulabildiği gösterilerek bu yöntemler ile mobil sohbet uygulamalarının adli analizi modeli ortaya konulmuştur.

2. ADLİ BİLİŞİM VE DELİL KAVRAMI

Gelişen teknoloji suç ve delil kavramlarına da yeni bir bakış açısı getirmiştir. Teknolojik cihazların ve kullanımının yaygınlaşması, bu cihazların hukuki süreçlere dâhil olması konusuna hız kazandırmıştır. Hukuki süreçlerde yer alan bu konu adli bilişim olarak tanımlanmıştır. Adli bilişim kavramı, belirli bir elektronik cihaz üzerinden kanıt toplamak ve saklamak için soruşturma ve analiz tekniklerinin bir mahkemede sunulmaya uygun bir şekilde uygulanmasıdır. İletişimin tespiti mümkün olmadığı durumlarda çözüm olarak yapılabilecek en etkili yöntem iletişim kurulan cihazın adli incelemesinin yapılmasıdır [1]. Adli bilişimin amacı, bir dijital delilde tam olarak ne olduğunu ve elde edilen şüpheli durumlardan kimin sorumlu olduğunu bulmak için belirlenmiş kanıt zincirinin ışığında bir soruşturma yürütmektir.

Adli bilişim süreçleri çoğunlukla standart prosedürlerden oluşmaktadır. İlk etapta yanlışlıkla değiştirilmediğinden emin olmak için söz konusu cihazı fiziksel olarak izole ettikten sonra, araştırmacılar cihazın depolama ortamının bir adli kopyasını oluşturmaktadırlar. Orijinal ortam kopyalandıktan sonra, bozulmama durumunu korumak için güvenli bir ortamda saklanır ve benzersiz bir özet değeri ile eşleştirilmektedir. Tüm araştırmalar dijital kopya üzerinde yapılmaktadır.

Araştırmacılar kopyayı incelemek, gizli klasörleri aramak ve silinmiş, şifrelenmiş veya zarar görmüş dosyaların kopyaları için ayrılmamış disk alanını araştırmak için çeşitli teknikler ve özel adli bilişim yazılımları kullanmaktadır. Adli kopyada bulunan kanıtlar dikkatlice bir "bulgu raporunda" belgelenip ve yasal işlemlere hazırlık aşamasında orijinalleri ile doğrulanmaktadır.

2.1. Elektronik (Dijital) Deliller

Teknolojinin suç işlemek için kullanılması ve gelişen adli bilişim teknolojileri sayesinde, sanal ortamlarda gerçekleştirilen suçlarla ilgili olarak kolluk kuvvetleri ve adli makamlarca elektronik deliller de kabul görmektedir.

Elektronik delil, mahkemede kabul gören, ikili biçimde sayısal ortamda saklanan veya iletilen bilgilerin bütünüdür. Herhangi bir dijital kamerada, bir bilgisayarın sabit diskinde, cep telefonunda, kişisel dijital yardımcılarda (PDA), CD'de veya flash diskte bulunabilir. Dijital deliller yaygın olarak çocuk pornografisi veya kredi kartı sahtekârlığı gibi siber suçlarla ilişkilendirilir. Bununla birlikte, dijital deliller artık sadece sanal suçları değil, her türlü suçu kovuşturmak için kullanılmaktadır. Örneğin, şüphelilerin e-postaları veya cep telefonu dosyaları, suç esnasındaki konumları ve diğer şüphelilerle ilişkileri hakkındaki kritik kanıtları içerebilir. Örneğin, 2005'te bir disket, araştırmacıları 1974'ten bu yana polisin yakalanmasından kaçan ve en az 10 mağdurun ölümüne sebep olan bir seri katile yönlendirmiştir [2].

2.2. Dijital Delil Türleri

Adli bilişimde dijital delillerin önemini küçümsemek oldukça zordur. Yalnızca bilgisayarın sabit diskinde depolanan dijital dosyalar biçiminde bulunan birçok tür kanıt bulunduğundan, günümüzde adli bilişim uzmanları için bu bilgilere erişmek çok önemlidir. Dijital delil olarak ele alınabilecek türler aşağıda sunulan başlıklar gibi sınıflandırılmıştır.

2.2.1. Anlık Mesajlaşma Uygulamaları

Anlık Mesajlaşma, zamanla önemli bir iletişim aracı haline gelmiştir. Milyonlarca insan yaşları, uyrukları, cinsiyetleri ve bilgisayar becerileri fark etmeksizin günün herhangi bir zamanında bu tür uygulamaları kullanarak çok fazla zaman harcamaktadırlar. Dolayısıyla anlık mesajlaşma uygulamalarının sohbet geçmişinden giderek daha fazla kanıt elde edilebilmektedir. Özellikle Whatsapp, Telegram, Live Messenger, ICQ, Yahoo! Messenger, Skype ve Hangouts en çok kullanılanlar arasındadır.

2.2.2. Sosyal Ağlar

Sosyal ağlar günümüzde anlık mesajlaşma uygulamalarını da içerisinde barındırdıklarından, insanların en fazla zaman harcadığı ve birbirleriyle iletişim kurduğu platformlar haline gelmişlerdir. Bu nedenle sosyal medya uygulamalarından çıkarılan iletişim ve paylaşım verileri, adli bilişim uzmanları için son derece değerli olabilmektedir.

2.2.3. Web Tarayıcıları

Web tarama da teknolojinin gelişimiyle birlikte popüler bir etkinlik halini almıştır. İnternette gezinme geçmişini, yer imlerini, önbelleğe alınmış web sayfalarını ve resimlerini, saklanan form değerlerini ve şifreleri analiz etmek, çoğunlukla farklı alanlardan elde edilemeyen önemli kanıtları elde edebilmeye imkân sağlamaktadır. Microsoft Internet Explorer, Mozilla Firefox ve Chrome'un popüler seçeneklerinin yanı sıra 4 düzine farklı Web tarayıcısı da bulunmaktadır.

2.2.4. E-posta

Anlık sohbetlerin ve sosyal ağların artmasına rağmen, e-posta hala özellikle kurumsal ortamlar için geçerli olan önemli bilgilerin önemli bir taşıyıcısıdır. Birçok çevrimiçi ve çevrimdışı e-posta istemcisi ile temelde doğru bir şekilde yaklaşmadan temel kanıtları gözden kaçırmak oldukça kolaydır. Microsoft Outlook, Outlook Express, Windows Mail, Canlı Posta, Thunderbird, TheBat! ve diğer birçok e-posta uygulaması piyasada bulunmaktadır.

2.2.5. P2P ve Dosya Değişimi Yazılımı

P2P ve popüler Torrent değişim yazılımı gibi dosya değişimi istemcileri, yasadışı görüntüler veya videolar ve çalınan, telif hakkı alınmış ve fikri mülkiyet dâhil olmak üzere temel kanıtlar içerebilmektedir. İndirilen, paylaşılan ve yüklenen dosyalar hakkındaki bilgilerin toplanan kanıt tabanına önemli bir katkısı olabilmektedir.

2.2.6. Çok Oyunculu Çevrimiçi Oyunlar

World of Warcraft gibi birçok popüler çok oyunculu oyunda, oyun oturumları arasında ve sırasında konuşmalar yapılır. Bu oyunlardan çıkarılan sohbet kayıtlarını analiz edilerek kanıt veritabanları genişletilebilmektedir. Kanada'da 2010 yılında 16 yaşındaki bir genç WoW sohbetinde bir cinayet hakkında itirafta bulunmuş ve bu oyunun sohbet kayıtlarının incelenmesi sonucu kanıtlanmıştır [3].

2.2.7. Multimedya İçeriği

Hareketsiz görüntüler ve video dosyaları içerikleri için analiz edilmesi gereken önemli kanıt kaynaklarıdır. Adli araçlar, araştırmacıların pornografi, insan yüzü veya resim dosyası olarak kaydedilmiş metin belgelerinin taranmış görüntüleri gibi şüphe arz eden konuları tespit ederek analizi otomatikleştirmesine yardımcı olabilmektedir.

2.2.8. Dijital Kanıt Türleri

Teknolojik cihazların ve kullanımının yaygınlaşması, bu cihazların hukuki süreçlere dâhil olması konusuna hız kazandırmıştır. Hakaret suçundan cinayete, terör eylemlerinden ülkelerin gizli birim görüşmelerine kadar birçok veri ve suç konusu teknolojik cihazlardan elde edilebilmektedir. Elde edilen bu veriler ise hukuk alanında dijital kanıt olarak değerlendirilmektedir [4]. Dijital kanıt türleri aşağıdakilerin tümünü ve daha fazlasını içerebilmektedir [5].

- Adres defterleri ve rehber kayıtları
- Ses dosyaları ve ses kayıtları
- Mobil cihazlara yedekleme de dâhil olmak üzere çeşitli programlara yedekleme
- Yer imleri ve sık kullanılanlar
- Tarayıcı geçmişi
- Takvimler
- Şifreli arşivler dâhil sıkıştırılmış arşivler (ZIP, RAR, vb.)
- Yapılandırma ve. ini dosyaları (hesap bilgileri, son erişim tarihleri vb. İçerebilir)
- Çerez verileri

- Veritabanları
- Belgeler
- E-posta mesajları, ekleri ve e-posta veritabanları
- Gizli ve sistem dosyaları
- Log dosyaları
- Kullanıcı öğeleri
- Sayfa dosyaları, hazırda bekleme dosyaları ve yazıcı biriktirme dosyaları
- Resimler, görüntüler, dijital fotoğraflar
- Videolar
- Sanal makineler
- Sistem dosyaları
- Geçici dosyalar

2.3. Mobil Cihazların Delil Yönünden Değerlendirilmesi

Cep telefonlarının incelenmesi hukuki açıdan CMK 134/1 maddesine dayandırılmıştır. Maddede "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir" ifadesi yer almaktadır. Mobil cihazlar bu maddeye istinaden "bilgisayar kütüğü" kapsamında tanımlanıp incelenmektedir [6].

Cep telefonları ile ilgili teknolojik gelişmeler her defasında ek özellikler ve yeniliklerle karşımıza çıkmaktadır. Uygulama çeşitlerinin artışı, özellik sayısındaki fazlalaşma ve iletişimin kolaylığı sayesinde mobil cihazlar önemli bir kanıt kaynağı haline gelmiştir.

Mobil cihaz adli incelemesi kapsamında GPS, tablet, PDA ve diğer mobil cihazları, SIM kartlar ve harici/dâhili hafıza kartları da incelenmektedir. Mobil cihazlar üzerinde gerekli veri kazıma ve veri kurtarma işlemleri yapılarak silinen dosyaları geri getirme aşamasından sonra yapılan mobil adli inceleme sonucu;

- Gelen, giden, cevapsız arama geçmişi
- Telefon rehberi veya irtibat listeleri
- SMS metni, uygulamaya dayalı (WhatsApp, Telegram gibi) ve multimedya mesajlaşma içeriği
- Resimler, videolar ve ses dosyaları ve bazen sesli e-posta mesajları
- İnternet arama geçmişi, içerik, çerezler, arama geçmişi, analitik bilgileri
- Yapılacaklar listeleri, notlar, ajanda kayıtları, zil sesleri

- Belgeler, elektronik tablolar, sunum dosyaları ve diğer kullanıcı tarafından oluşturulan veriler
- Parolalar ve kullanıcı hesabı kimlik bilgileri
- Konum bilgileri ve Bluetooth/Wi-Fi bağlantı bilgileri
- Çeşitli yüklü uygulamalardan gelen veriler
- Silinen veya şifrelenen dosya türleri
- Sistem dosyaları, kullanım günlükleri, hata mesajları elde dilebilir.

2.4. CMK Açısından Dijital Deliller

Türk Ceza Muhakemesi Kanunu dijital delillere yönelik arama, kopyalama ve el koyma tedbirlerini CMK 134'te düzenlemiştir. CMK 134. Maddenin 1. Fıkrasına göre bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (…) (2) karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

CMK 134. Maddenin 2. Fıkrası gereğince bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilmektedir.

CMK 134. Maddenin 3. Fıkrasında bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Olası veri kayıplarının önlenmesi için bu madde ciddi önem taşımaktadır.

CMK 134. Maddenin 4. Fıkrası gereğince üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınmaktadır.

CMK 134. Maddenin 5. ve son Fıkrası kapsamında bilgisayar veya bilgisayar kütüklerine el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınmaktadır.

3. MOBİL CİHAZLAR VE ADLİ BİLİŞİM

Günümüzde neredeyse her yaş grubu tarafından kullanılmakta olan kişisel mobil cihazlarda sağlık ve günlük aktivite verileri alışveriş alışkanlıkları, kullanım istatistikleri gibi her türlü verinin barındırılması mümkün olabilmektedir [7] Bu bölümde günümüzde yaygın olarak kullanılan mobil cihaz kavramı ve türleri detaylı olarak ele alınmıştır.

3.1. Mobil Cihazlar

Günümüzün mobil cihazları hem işletme hem de tüketici kullanımı için geniş bir uygulama yelpazesine ev sahipliği yapabilen çok işlevli cihazlardır. Akıllı telefonlar ve tabletler insanların mobil cihazlarını e-posta, anında mesajlaşma, yazılı mesajlaşma ve Web'de gezinmenin yanı sıra iş belgeleri, irtibat listeleri ve daha fazlası için Internet'e erişmek için kullanmalarını sağlar.

Mobil cihazlar genellikle kendi PC veya dizüstü bilgisayarınızın bir uzantısı olarak görülür ve bazı durumlarda daha yeni, daha güçlü mobil cihazlar PC'lerin yerini bile alabilir. Cihazlar birlikte kullanıldığında, bir mobil cihazda uzaktan yapılan çalışmalar, bilgisayardan uzaktayken değişiklikleri ve yeni bilgileri yansıtmak için PC'lerle senkronize edilebilir.

3.2. Mobil Cihaz Türleri

Mobil cihaz terimi, çok çeşitli tüketici elektroniği anlamına gelir. Mobil cihaz genellikle internete bağlanabilen taşınabilir cihazları tanımlamak için kullanılır. Bununla birlikte, bazıları ayrıca bağlı dijital kameraları ve standart MP3 çalarları da mobil cihazlar olarak sınıflandırır. Mobil cihazlar kategorisi, diğerlerinin yanı sıra, aşağıdaki cihazları içerir.

3.2.1. Kişisel Dijital Asistan (PDA)

Bazen cep bilgisayarları adı verilen PDA'lar, bilgisayar, telefon / faks, İnternet ve ağ öğelerini tek bir cihazda birleştiren el tipi cihazlardır. Tipik bir PDA cep telefonu, faks gönderen, Web tarayıcı ve kişisel düzenleyici olarak işlev görebilir.

Taşınabilir bilgisayarların aksine, çoğu PDA, giriş için bir klavyeden ziyade bir kalem kullanarak, kalem tabanlı olarak başladı. Bu, aynı zamanda el yazısı tanıma özellikleri de içerdikleri anlamına gelir. Bazı PDA'lar ses tanıma teknolojilerini kullanarak ses girişine de tepki verebilir. Günümüzün PDA'ları ekran kalemi veya klavye versiyonunda mevcuttur.

PDA'lar, akıllı telefonların ve tabletlerin popülaritesinin artmasıyla büyük ölçüde eski hale getirildi, ancak yine de niş pazarlarda varlığını koruyorlar. Yıllar boyunca PDA cihazlarının örnekleri

arasında Palm Pilot, Revo, Sony Clie, Hewlett-Packard Jornado, Casio var Cassiopedia, Compaq iPaq ve Toshiba Cep Bilgisayarı.

3.2.2. Tablet PC'ler

Bir tablet veya tablet PC, birincil giriş aygıtı olarak dokunmatik ekran kullanan taşınabilir bir bilgisayar olarak tanımlanmaktadır. Çoğu tablet biraz daha küçüktür ve ortalama bir dizüstü bilgisayardan daha azdır. Bazı tabletlerde katlanabilir klavye bulunurken, Apple iPad ve Motorola Xoom gibi türler yalnızca dokunmatik ekran girişi sunmaktadır.

Çapraz olarak ölçüldüğünde, çoğu tablet PC yedi ila 10 inç arasındadır. Bazı modeller x86 merkezi işlem birimlerinde (CPU) çalışır, ancak çoğu daha az güç tüketen ve daha uzun pil ömrü sağlayan Gelişmiş RISC Makine (ARM) işlemcilerine güvenir.

1990'ların başında mevcut olan kişisel dokunuşa duyarlı cihazlar - ya da PDA'lar - pazarda sınırlı başarı elde etti. Tablet PC ve PDA benzer bir form faktörünü paylaşmasına rağmen, bir PDA sınırlı yeteneklere sahip çok daha küçüktür. PDA'lar ayrıca kullanıcı girişi için bir kalem gerektirir.

Tüm kullanıcı girişi, bir klavye veya fare değil, doğrudan LCD ekrandan yapılır. Bir tablet bilgisayarda, el yazısı dijitalleştirilir ve el yazısı tanıma yoluyla standart metne dönüştürülebilir veya el yazısı metin olarak kalabilir. Özel kalem, ayrıca, harf tuşlarının QWERTY klavyeden farklı şekilde düzenlenmiş olduğu kalem tabanlı bir tuş yerleşimi yazmak için de kullanılabilir. Tablet PC'ler, giriş için bir klavye ve/veya fare ile donatılabilir.

Tablet PC, özel amaçlı kalemin hareketini yakalayabilen ve hareketi LCD ekranda kaydedebilen bir elektromanyetik alan oluşturmak için bir sayısallaştırıcının bir LCD ekranın altına veya üstüne yerleştirildiği dijital mürekkep teknolojisine dayanır. Etkisi kâğıda sıvı mürekkeple yazmak gibidir. Tablet PC örnekleri arasında Apple iPad, Microsoft Surface ve Surface Pro, Samsung Galaxy Tab, Samsung Nexus, Amazon Kindle Fire HD ve Lenovo Yoga bulunmaktadır.

3.2.3. Akıllı Telefon & Cep Telefonu

Bir akıllı telefon, bütünleşmiş bir bilgisayara ve işletim sistemi, tarayıcı ve yazılım uygulamalarını çalıştırma becerisi olan ve klasik telefonlarla ilişkilendirilmeyen diğer özelliklere sahip hücresel bir telefon olarak tanımlanmaktadır [8].

İlk akıllı telefon, 1992 yılında COMDEX bilgisayar fuarında, tüketici cihazı yerine konsept cihazı olarak sunulan IBM'in Simon'ıydı [9]. Yalnızca arama yapma ve mesaj gönderme yerine, kullanıcı için e-posta ve faks gönderme ve aynı zamanda kullanıcı için etkinlik takvimi tutma yeteneğine sahiptir [10].

Nokia ve Hewlett Packard dâhil olmak üzere birçok üretici 1996 yılında, PDA'ların ve erken işletim sistemlerini (OS'ler) ve web tarama yeteneklerini içeren tipik cep telefonlarının

kombinasyonları olan cihazları piyasaya sürdü. BlackBerry, ilk akıllı telefonlarını 2000'lerin ortalarında piyasaya sürdü. Tüketiciler ve şirketler arasında çok popüler oldu. LG, 2007 yılında Prada'yı piyasaya sundu ve Apple iPhone'u dokunmatik ekrana sahip ilk akıllı telefon olarak sundu. HTC, bir yıl sonra Dream akıllı telefonunu piyasaya sürdü ve bu da Google'ın Android işletim sistemini kullanan ilk kişi oldu.

Akıllı telefonların tarihindeki diğer büyük gelişmeler arasında, Sony'nin 2015 yılında 4K çözünürlüklü bir ekrana sahip Xperia Z5 Premium telefonunun piyasaya sürülmesi yer alıyor. Wi-Fi ve LTE'deki ağ iletişimi ilerlemeleri, akıllı telefonların daha hızlı kullanım için bağlantısını artırdı.

Bir akıllı telefon; web tarayıcı, yazılım uygulamaları ve mobil işletim sistemi dâhil olmak üzere daha gelişmiş özelliklere sahiptir. Bir akıllı telefonda biyometri desteği, görüntülü sohbet, dijital asistanlar ve daha fazlası gibi yetenekler kullanıcıya sunulmaktadırBir akıllı telefonun en önemli özelliklerinden biri, bir uygulama mağazasına bağlantı sağlayabilmesidir. Uygulama mağazası, kullanıcıların telefonlarında çalıştırmak için yazılım uygulamaları arayabilecekleri ve indirebilecekleri merkezi bir portaldır. Tipik bir uygulama mağazası, verimlilik, oyun, kelime işlem, not alma, organizasyon, sosyal medya ve daha fazlası için binlerce mobil uygulama sunmaktadır.

Bir akıllı telefonun diğer önemli özelliklerinden bazıları şunlardır:

- İnternete Bağlanabilirlik
- Bir Mobil Tarayıcı
- Bir Aygıta Birden Fazla E-Posta Hesabını Senkronize Etme Yeteneği
- Gömülü Hafıza
- Donanım Veya Yazılım Tabanlı Bir Qwerty Klavye
- Dizüstü Veya Masaüstü Bilgisayarlar Gibi Diğer Cihazlarla Kablosuz Senkronizasyon
- Uygulamaları İndirme Ve Bunları Bağımsız Olarak Çalıştırma Becerisi
- Üçüncü Taraf Uygulamaları İçin Destek
- Aynı Anda Birden Fazla Uygulamayı Çalıştırma Yeteneği
- Dokunmatik Ekran
- Wi-Fi
- Tipik Olarak Video Özelliğine Sahip Bir Dijital Kamera
- Oyun;
- Birleşik Mesajlaşma
- Gps – Evrensel Konumlandırma Sistemi.

Bir işletim sistemi ve uygulamaları çalıştırdıklarından, akıllı telefonlar tutarlı yazılım güncellemeleri alır. Satıcılar mobil işletim sistemlerini yılda birkaç kez günceller ve bir uygulama mağazasındaki mobil uygulamalar, kullanıcıların yüklemeyi veya yok saymayı seçebilecekleri sabit yazılım güncellemelerini görür.

3.2.4. Giyilebilir Teknolojiler

Giyilebilir teknolojilerin kullanımı, giysilerin, saatlerin, gözlüklerin, ayakkabıların ve benzeri eşyaların da dâhil olduğu, kullanıcı tarafından giyilebilen bilgisayar destekli cihazları veya donanımları ifade eden bir terimdir. Giyilebilir bilgisayar cihazları, kalp atış hızı izleme ve adım sayarlık yetenekleri gibi çok sınırlı özelliklerin geliştirilmesinden gelişmiş "akıllı" işlevlere ve akıllı telefon veya akıllı saatlerin sunduğu özelliklere benzer yeniliklere kadar değişiklik gösterebilir.

Daha gelişmiş giyilebilir bilgi işlem cihazları, tipik olarak kullanıcının resim veya video çekmesine ve görüntülemesine, kısa mesajları ve e-postaları okumasına, sesli komutlara yanıt vermesine, internette dolaşmasına ve daha pek çok şeye olanak sağlayabilir.

Giyilebilir cihazların örnekleri arasında Apple iWatch, fitness izleme cihazları ve bir tür cam içine gömülen ilk cihaz olan devrim niteliğindeki Google Glass gibi bilgisayarlı kol saatleri sayılabilir. Giyilebilir cihazların etrafındaki bazı konular arasında gizlilik, sosyal etkileşimleri ne ölçüde değiştirdikleri, kullanıcıların bunları kullanırken nasıl göründüğü ve kullanıcı dostu tasarımla ilgili çeşitli konular yer almaktadır.

3.2.5. Akıllı Saatler

Akıllı saat, zaman işleyişinin yanı sıra diğer birçok özelliği sağlayan dijital bir saattir. Örnekler arasında kalp atış hızınızı izlemek, etkinliğinizi izlemek ve gün boyunca hatırlatıcılar sağlamak bulunmaktadır. Bir akıllı telefon gibi, bir akıllı saatin ekranına dokunarak veya kaydırarak işlem yapmanızı sağlayan dokunmatik bir ekrana sahiptir.

Modern akıllı saatler, akıllı telefonlar ve tabletler için kullanılan uygulamalara benzer çeşitli uygulamalar içerir. Bu uygulamalar, hava durumu bilgisinin görüntülenmesi, hisse senedi fiyatlarının listelenmesi ve haritaların ve yol tariflerinin görüntülenmesi gibi ek işlevler sağlar. Çoğu akıllı saat, telefon görüşmesi yapmak ve kısa mesaj göndermek ve almak için de kullanılabilir.

3.2.6. Drone

Teknolojik anlamda drone, insansız hava aracı olarak tanımlanmaktadır. Dronelar daha resmi olarak insansız hava araçları (UAV) veya insansız hava aracı sistemleri (UAS) olarak bilinir. Temel olarak bir drone, yerleşik sensörler ve GPS ile birlikte çalışan gömülü sistemlerindeki yazılım kontrollü uçuş planları aracılığıyla uzaktan kontrol edilebilecek veya otonom olarak uçabilecek bir robotik uçak sistemidir.

Geçmişte, dronelar çoğunlukla askeri sistemlerle ilişkiliydi, başlangıçta uçaksavarlık hedef uygulamaları, istihbarat toplamaları ve daha sonra tartışmalı olarak silah platformları olarak kullanılıyorlardı. Dronelar artık arama kurtarma, gözetleme trafik izleme, hava durumu izleme ve

yangınla mücadele, kişisel dronelar ve iş dronu temelli fotoğrafçılık ile videografi, tarım ve hatta teslimat hizmetlerine kadar geniş bir yelpazede sivil rollerde kullanılabilmektedir.

Dronelar, eğlence, fotoğrafçılık, ticari ve askeri gibi çeşitli amaçlara hizmet ederken, iki temel işlevi uçuş ve navigasyondur.

Uçmak için uçağı pil veya yakıt, rotor, pervane ve bir çerçeve gibi bir güç kaynağından oluşur. Bir dronun çerçevesi, ağırlığı azaltmak ve uçuş sırasındaki manevra kabiliyetini arttırmak için tipik olarak hafif, kompozit malzemelerden yapılır.

Dronelar, bir operatör tarafından uzaktan başlatılması, yönlendirilmesi ve indirilmesi için uzaktan kullanılan bir denetleyici gerektirir. Kontrolörler, Wi-Fi dâhil olmak üzere radyo dalgalarını kullanarak drone ile iletişim kurar.

Droneların her alanda yaygın kullanılmaya başlanması, diğer yaygın kullanılan cihazlarda da olduğu gibi zamanla suça sebebiyet vermesine yol açmıştır [11]. Dronelar güvenlik ve mahremiyet endişeleri doğuracak bir tehdit oluşturmaktadır. Geçmişte İHA'ların komşuları gözetlemek, insanları takip etmek ve askeri tesisler ile hassas kurumları denetlemek için kullanıldığı olaylar yaşanmıştır [12].

Ayrıca dronelar ile cezaevleri üzerinden tutuklulara kaçak telefon atıldığı, uyuşturucu kaçakçılarının uyuşturucu tedarik etmek amacıyla drone kullandıkları tespit edilmiştir [13].

3.3. Mobil Cihazlarda Yer Alan İşletim Sistemleri

Cep Telefonları, tabletler, PDA ve akıllı cihazlar için geliştirilmiş olan çeşitli işletim sistemleri bulunmaktadır. Farklı marka ve model cihaz üreticileri tercih ettikleri işletim sistemini cihazlara yüklü olarak satışa sunmaktadırlar. İşletim sistemlerine yönelik uygulama geliştiriciler tarafından da bu işletim sistemlerinin uygulama marketlerinde yayınlanan uygulamalar bulunmaktadır. İşletim sisteminin türü ve sürümü cihazın adli kopyasının alınmasından inceleme sürecine kadar birçok aşamayı olumlu veya olumsuz etkilemektedir.

3.3.1. Android İşletim Sistemi

Android işletim sistemi, Google tarafından öncelikle dokunmatik ekranlı cihazlar, cep telefonları ve tabletler için kullanılmak üzere geliştirilen bir mobil işletim sistemidir. Android işletim sistemi, ilk olarak Google tarafından 2005 yılında satın alınan Android, Inc. Tarafından oluşturulmuştur. Google, Android işletim sisteminin sürekli gelişmesinden sorumlu olan Open Handset Alliance'ı (OHA) oluşturmak için diğer şirketlerle birlikte çalışmıştır.

Tasarımı, kullanıcıların yakınlaştırma, kaydırma ve dokunma gibi genel hareketleri yansıtan parmak hareketleriyle mobil aygıtları sezgisel olarak kullanmalarını sağlar. Mobil cihazlara ek

olarak, Google, her biri benzersiz bir kullanıcı arayüzü ile donatılmış televizyonlarda, arabalarda ve kol saatlerinde Android yazılımı kullanmaktadır.

Android'in temel çekirdeği Linux'a dayanıyor olsa dahi, Google'ın talimatlarına uyacak şekilde özelleştirilerek piyasaya sürülmüştür. GNU kitaplıkları için destek yoktur ve yerel bir X Windows sistemine sahip değildir. Linux çekirdeğinde ekran, kamera, flash bellek, tuş takımı, WiFi ve ses için sürücüler bulunur. Linux çekirdeği, donanım ile telefondaki yazılımın geri kalanı arasında bir soyutlama görevi görür. Aynı zamanda güvenlik, bellek yönetimi, süreç yönetimi ve ağ yığını gibi çekirdek sistem hizmetlerini de yerine getirir.

Android işletim sisteminin ilk hedef kitlesi telefonlar olarak belirlenmiş ve telefonlara yönelik olarak tasarlanmıştır. Birçok özelliği şunlardır:

- Açık kaynak kodlu WebKit motorunu temel alan entegre tarayıcı
- Optimize edilmiş 2D ve 3D grafikler, multimedya ve GSM bağlantısı
- Bluetooth
- 3G
- Kablosuz internet
- SQLite
- Kamera
- Küresel Konumlama Sistemi
- Pusula
- İvmeölçer

Android işletim sistemi için uygulamalar oluşturmak isteyen yazılım geliştiriciler, belirli bir sürüm için Android Yazılım Geliştirme Seti'ni (SDK) indirebilir. SDK bir hata ayıklayıcı, kütüphaneler, bir emülatör, bazı belgeler, örnek kod ve öğreticiler içerir. Daha hızlı gelişme için, ilgili taraflar, Java'daki uygulamaları yazmak için Eclipse gibi grafiksel tümleşik geliştirme ortamlarını (IDE'ler) kullanabilir.

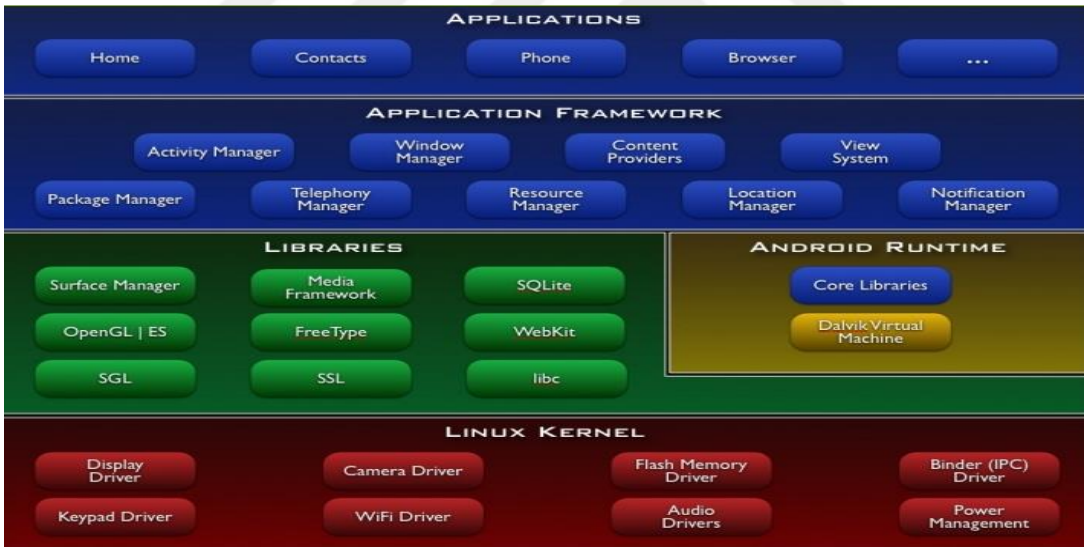
Özellikleri

- Uygulama Arayüzü: İçeriklerin yeniden kullanılabilmesini ve yer değiştirilmesini sağlar.
- Dalvik Sanal Makinesi: Mobil cihazlar için optimize edilmiştir.
- Dâhili Tarayıcı: Açık kaynak kodlu WebKit projesinden yararlanılmıştır.
- Optimize Edilmiş Grafik Yapısı: 2D ve 3D desteklemektedir.

- SQLite: Yapısal veri depolamayı sağlar. Sohbet uygulamalarında çoğunlukla kullanılan SQlite veri tabanı ile ilgili olarak analiz yöntemleri adli bilişim açısından önem arz etmektedir [14].
- Medya Desteği: Birçok değişik sistem desteklenmektedir. (MP4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- Çağrı Özelliği: GSM Telefon
- İletişim Özellikleri: Bluetooth, EDGE, 3G ve WIFI
- Diğer Özellikler: Kamera, GPS, pusula ve ivmeölçer
- Zengin Geliştirme Çevresi: Cihaz emülatörü, bellek ve performans görüntüleyicisi, debug yapmayı sağlayan tool ve ECLIPSE için plugin bulunmaktadır.

Mimari

Android İşletim Sistemi mimarisinde uygulamalar, uygulama frameworkleri, kütüphaneler ve Linux çekirdeği yer almaktadır. Bu yapılar ve alt yapıları **Şekil 3.1** de sunulmuştur.



Şekil 3.1 Android İşletim Sistemi Mimarisi

3.3.2. iOS İşletim Sistemi

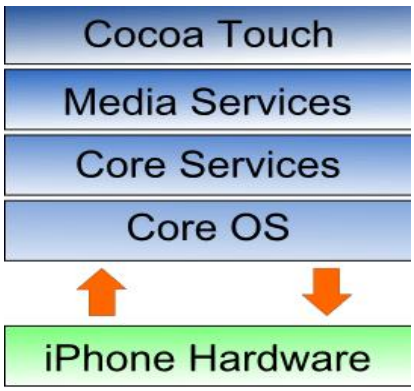
iOS (eski adıyla iPhone OS) Apple'ın başlangıçta iPhone için geliştirdiği ancak daha sonra iPod touch ve iPad'de de kullanılan mobil işletim sistemidir. Mac OS X'den türetilmiştir. iOS içinde 4 katman bulundurmaktadır: Core OS tabakası, Core Servisleri tabakası, Medya tabakası ve Cocoa Touch tabakası. Yazılım cihazın içinde 500 MB'lık bir alan kaplamaktadır. iOS işletim sistemi yapısı nedeniyle Apple App Store dışında hiçbir yerden uygulama yüklenmesine imkân vermemektedir.

İşletim sistemi ilk olarak iPhone için Macworld Conference & Expo'da 9 Ocak 2007'de duyurulmuş, aynı yılın haziran ayında yayınlanmıştır. İlk aşamada Apple pazarlama literatürü bu ismi açıkça belirtmeyerek iPhone OS X olarak açıklamıştır [15].

Başlangıçta, üçüncü tarafların geliştirdiği uygulamaların desteklenmesine imkân sağlanmamıştır. Steve Jobs daha sonra geliştiricilerin uygulamalar geliştirmesini savunmuştur. 17 Ekim 2007'de Apple SDK 'in geliştirildiğini duyurmuş ve geliştiriciler için şubat ayında yayınlamıştır. 6 Mart 2008'de iPhone OS' in beta sürümü yayınlanmıştır. Dördüncü sürüm Nisan 2010'da duyurulmuştur. Bu sürüm multitasking, iş amaçlı özellikler, e-mail ve eklentiler için şifreleme özelliklerini içeren ilk sürümdür. 7 Haziran 2010 WWDC 2010'da Apple, iPhone OS 'in adını iOS olarak değiştirdiğini açıklamıştır. Apple, Cisco System ile anlaşıp iOS markasının ticari haklarını satın almıştır. İlerleyen süreçte belli aralıklarla ve sırasıyla yeni sürümler geliştirilmiştir. Günümüzde yayınlanan son sürüm IOS 13'tür.

Mimarisi

Daha önce belirtildiği gibi, iPhone işletim sistemi, her biri işletim sisteminin üzerinde çalışan uygulamaların geliştirilmesine yönelik programlama çerçeveleri sağlayan birkaç farklı yazılım katmanından oluşur. Bu işletim sistemi katmanları [16], **Şekil 3.2.** de olduğu gibi şematik olarak gösterilebilir:



Şekil 3.2 IOS İşletim Sistemi Mimarisi

Cocoa Touch Katmanı: iPhone OS yığınının en üst katmanıdır ve iPhone uygulama geliştiricileri tarafından en sık kullanılan çerçeveleri içerir. Cocoa Touch, öncelikle Objective-C dilinde yazılmıştır ve standart Mac OS X Cocoa API' sini temel alarak çalışır.

Ortam Katmanı: Yığının üstünden ikinci katmandır. iPhone OS'ye ses, video, animasyon ve grafik yetenekleri sağlar. İPhone OS yığınının diğer katmanlarında olduğu gibi, Ortam katmanı da iPhone uygulamaları geliştirirken kullanılabilecek bir dizi çerçeve içerir.

Çekirdek Hizmetleri Katmanı: Yığın üstünden üçüncü katmandır. İPhone Çekirdek Hizmetleri katmanı, yukarıda belirtilen tüm katmanların oluşturulduğu başlangıç seviyesindeki temeli sağlar.

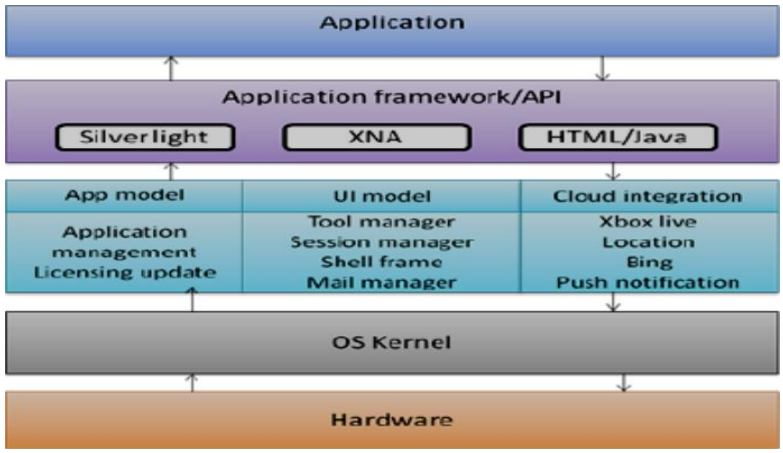
Çekirdek İşletim Sistemi Katmanı: Çekirdek İşletim Sistemi Katmanı, iPhone işletim sistemi yığınının alt katmanıdır ve doğrudan aygıt donanımının üstüne oturur. Bu katman, düşük seviyeli ağ bağlantısı, harici aksesuarlara erişim ve bellek yönetimi, dosya sistemi yönetimi ve iş parçacığı gibi genel temel işletim sistemi hizmetleri gibi çeşitli hizmetler sunar.

iPhone Donanımları: Donanım aygıtları iPhone OS tarafından yönetilir ve telefona yerel uygulamaları uygulamak için gereken teknolojileri sağlar. İşletim sistemi, kullanıcıya standart hizmetler sağlayan Posta, Safari, Telefon gibi çeşitli sistem uygulamalarıyla birlikte gelir.

3.3.3. Windows İşletim Sistemi

Windows Mobile, akıllı telefonları ve Pocket PC' leri hedef alan bir Micrososft işletim sistemidir. İlk önce Pocket PC 2000 işletim sisteminde piyasaya sürüldü ve Windows CE çekirdeğini temel aldı. Windows Mobile, Microsoft Windows API ile geliştirilen temel uygulamaları ve Microsoft tarafından kısıtlama olmaksızın özelleştirme ve yazılım geliştirme seçeneklerini içeriyordu. Yazılım uygulamaları Windows Marketplace for Mobile'dan satın alınabiliyordu.

2010 yılında, Microsoft, Windows Mobile' ın üstesinden gelmek için Windows Phone'un geliştirildiğini duyurdu. Mimarisi **Şekil 3.3**'te sunulmaktadır.



Şekil 3.3 Windows Mobile İşletim Sistemi Mimarisi

3.3.4. Blackberry İşletim Sistemi

BlackBerry OS, Research In Motion'ın (RIM) BlackBerry cihazları için özel olarak tasarlanmış tescilli bir mobil işletim sistemidir. BlackBerry OS, BlackBerry Bold, Curve, Pearl ve Storm serisi gibi Blackberry modellerinde çalışır.

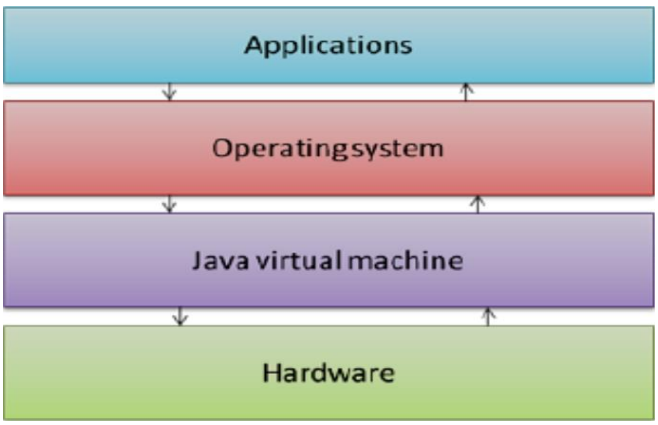
BlackBerry OS akıllı telefon ortamları için tasarlanmıştır ve push Internet e-postaları için sağlam desteği ile bilinir. Bu push e-posta işlevi, Microsoft Exchange, Lotus Domino ve Novell Groupwise için sürümleri olan özel BlackBerry Enterprise Server (BES) aracılığıyla gerçekleştirilmektedir.

Android, Microsoft Windows Mobile ve Symbian gibi diğer mobil işletim sistemleri, farklı cep telefonları markalarında çalışabilir olmasına karşın BlackBerry OS yalnızca BlackBerry telefonlarda çalışabilme imkânı sağlkamaktadır. BlackBerry OS, bu konuda Apple'ın IOS İşletim Sistemine benzetilmektedir.

Geleneksel olarak, BlackBerry uygulamaları Java, özellikle Java Micro Edition (Java ME) platformu kullanılarak yazılır. Bununla birlikte, RIM, HTML, CSS ve JavaScript kodundan oluşan küçük bağımsız Web uygulamaları oluşturmak için widget yazılım geliştirme kitini (SDK) kullanan 2010 yılında BlackBerry Web geliştirme platformunu başlatmıştır.

Java ile geliştirmeyi tercih edenler, bir editör, hata ayıklayıcı, cihaz simülatörü ve bellek görüntüleyici ile gelen bütünleşmiş bir geliştirme ortamı (IDE) olan BlackBerry Java Geliştirme Ortamı'nı (JDE) kullanabilir. JDE, BlackBerry web sitesinden indirilebilir. Bağımsız olarak veya bir grafik IDE olan Eclipse için bir eklenti olarak kullanılabilir. JDE ile birlikte kullanılan diğer araçlar RAPC derleyicisi ve Sun Java derleyicisidir.

Bir BlackBerry OS cihazına uygulama kurmanın üç yolu vardır. Bunlar, BlackBerry App World'den bir uygulama indirme yoluyla, cihazın dâhili tarayıcısı üzerinden veya BlackBerry Desktop Manager üzerinden kablosuz olarak kurulabilmektedir. Mimarisi **Şekil 3.4.** te sunulmaktadır [17].



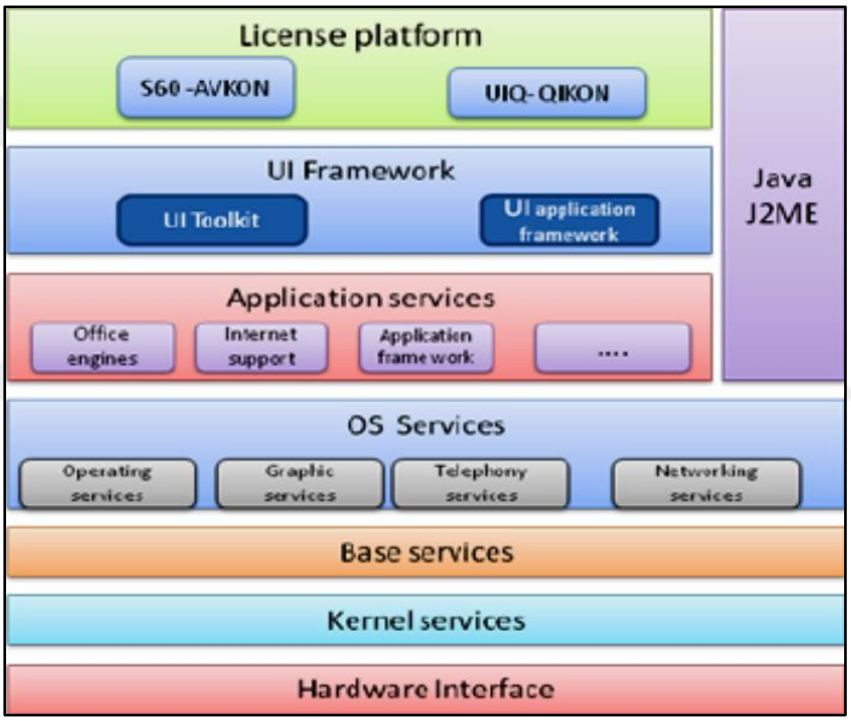
Şekil 3.4. Blackberry İşletim Sistemi Mimarisi

3.3.5. Symbian İşletim Sistemi

Symbian OS, Android tarafından üstlenildiği 2010 yılına kadar dünyada en yaygın kullanılan akıllı telefon işletim sistemidir. Symbian OS'nin geliştirilmesi Mayıs 2014' te durdurulmuştur.

Symbian OS, 1980' lerde Psion adlı bir şirket tarafından geliştirilen EPOC adlı bir işletim sistemi olarak başlamıştır. 1998' de, telefon üreticileri Nokia, Ericsson ve Motorola ile ortak girişimi olan Psion, Symbian, Ltd. ve EPOC, Symbian işletim sistemi olarak değiştirilmiştir. Nokia, 2008'de Symbian'ı satın almış ve Symbian OS' nin kaynak kodunun çoğunluğu açık kaynak lisansı altında yayımlanmıştır. O zamanlar, halka açık olan en büyük açık kaynaklı kod tabanlarından biri olarak ele alınmıştır.

2014 itibariyle, geliştiriciler artık yeni Symbian uygulamaları yayınlayamamaktadır, ancak mevcut uygulamalar hala indirilmeye hazır durumda bulundurulmakta ve indirilmeye imkân sağlanmaktadır. Mimarisi **Şekil 3.5.** te sunulmaktadır.



Şekil 3.5. Symbian İşletim Sistemi Mimarisi

3.4. Mobil Cihazlarda Adli Bilişim

Günümüzde mobil cihazların kullanımının artmasına bağlı olarak adli bilişim alanında mobil cihazların incelenmesi ve delillerin ortaya konması önem arz etmektedir. Güvenlik birimlerince yapılan aramalarda çok sayıda çeşitlilik gösteren mobil cihazlar ele geçirilmektedir. Barındırdıkları çeşitli donanımsal, yazılımsal özellikler ve güncellemeler nedeniyle diğer dijital materyallere göre imajlarının alınması ve incelenme aşamaları daha karmaşıktır.

3.4.1. Mobil Cihazlarda İmaj Alma İşlemleri

İmaj, tüm dosyalar, klasörler ve ayrılmamış, artık alanlar dâhil olmak üzere, fiziksel olarak bir depolama cihazının sektör bazında doğrudan bit kopyasıdır. Adli kopyalar, yalnızca işletim sistemi tarafından görülebilen tüm dosyaları değil, aynı zamanda boş ve boş alanda kalan dosyaları ve silinen dosyaları da içerir.

İmaj alma, adli makamlara sunmak amacıyla uygun kanıtlar toplamak için bilgisayar araştırma ve analiz tekniklerinin uygulanması olan adli bilişim dalının önemli bir unsurudur.

Tüm görüntüleme ve yedekleme yazılımları, adli imaj alma yeteneğine sahip değildir. Örneğin, Windows yedeklemesi, fiziksel aygıtın tam kopyaları olmayan görüntü yedeklemeleri oluşturur. İmajlar ise özel adli yazılımlar aracılığıyla oluşturulabilir. Adli kullanım için lisans gerektirmeyen ücretsiz bazı imaj alma yardımcı programları da tam disk görüntüleri oluşturabilir.

Bir bilişim suçunun oluşması durumunda, tespit edilmesini önlemek için silinmiş ve suç teşkil eden, işletim sisteminden elde edilecek verilerin haricinde ek kanıtlar bulunabilir. Veriler güvenli bir şekilde silinmediği ve üzerine yazılmadığı sürece, adli bilişim ya da veri kurtarma yazılımlarıyla kurtarılabilir.

İmaj alma ve yedekleme, orijinal sürücü arızalarından kaynaklanan veri kaybını önlemeye yardımcı olur. Kanıt olarak veri kaybı yasal davalara zarar verebilir. İmajlar ayrıca genel olarak kritik dosyaların kaybını da önleyebilir. Suç araştırmasının orijinal delil üzerinden yapılması hukuki olarak delil bütünlüğünü bozabileceğinden adli kopya üzerinde inceleme yapılması uygun görülmüştür. Adli kopyaların oluşturulduktan sonra, delil bütünlüğünü sağlamak amacıyla hash adı verilen benzersiz özet fonksiyonları oluşturulur ve karşılaştırılır. İmaj alma işlemi fiziksel ve mantıksal olarak iki farklı türde gerçekleştirilebilir.

Fiziksel İmaj Alma

Fiziksel imaj, veri depolama alanından yedek kopya veya arşiv olarak kopyalama işlemidir. İşlem, ana önyükleme kaydı ve tablo ayırma bilgileri gibi veriler dâhil olmak üzere kaynak sürücüde depolanan tüm verilerin kopyalanmasını gerektirir. Sabit sürücünün fiziksel görüntüsü, sürücüde bulunanları ve sıfır değerlerini ele alır. Ayrıca, sürücüdeki silinmiş alanı (yakın zamanda biçimlendirilmiş olsa bile), silinen dosyaları ve dosya parçalarını kopya olarak oluşturur. Bu nedenle, 500 GB' lik bir sürücünün fiziksel bir görüntüsü, 500 GB' lik bir sonuç dosyası verecektir. Bu imaj türü, adli bilişim incelemeleri açısından en kapsamlı türdür. Delillerin silinmiş veya tahrif edilmiş olduğundan şüphelenilen ve meta datanın önemli bir faktör olduğu durumlar için faydalıdır.

Mantıksal İmaj Alma

Mantıksal imaj, sabit sürücünün mantıksal bir bölümündeki etkin verilerin tümünün veya hedeflenmiş bir alt kümesinin belirgin bir görüntüsünü yakalar. Mantıksal bir imaj, fiziksel imajın silinmiş dosyalar, dosya parçaları ve bu bölümdeki silinmiş veya boş alanlardır.

Bu yöntem herkes tarafından bilinen dosyalarımızı kopyalamamızı sağlayan kopyala ve yapıştır komutuna benzemektedir. Ancak, standart bir kopyala ve yapıştır işlemi, adli imaj alma işlemini gerçekleştirmek için kullanılan işlemlerle aynı değildir. Bir kopyala ve yapıştır işlemi bir sabit sürücüden diğerine yapıldığında, kopyalanan yalnızca kullanıcı tarafından görülebilen dosyalardır. Sabit sürücünün gizli dosyaları bulmak ve erişmek için kullandığı diğer tüm veriler eksik olacaktır. Dosya Tahsis Tabloları (FAT) ve Ana Önyükleme Kayıtları gibi veriler kopyalanmaz. Bu nedenle, oluşturulan imajda yinelenen sürücü orijinalin yerine kullanılırsa, sistem önyükleme yapamaz ve işlevsel olmaz.

3.4.2. Lisanslı Adli Bilişim Araçları

Adli kopya üzerinde inceleme yapmaya yarayan yazılımların mobil cihaz işletim sistemi ve yüklü mobil uygulamaların çalışma prensiplerini tanıyor ve incelemeye çözümler sunuyor olması gerekmektedir [18]. Bu makalede günümüzde kullanılan popüler mobil cihaz imajı inceleme yazılımları ele alınmıştır [19]. Mobil cihazların adli bilişim açısından incelenmesinde genel olarak kullanılan lisanslı adli bilişim araçları hakkında bu başlıkta bahsedilecektir.

Cellebrite

Cellebrite adli bilişim uygulamaları için iki temel yazılım üretmiştir. Bunlar imaj alma işlemlerini sağlayan Physical Analyzer (PA) ve adli kopyaları açarak inceleme yapılmasını sağlayan UFED4PC' dir. UFED4PC cep telefonları, tabletler ve drone gibi cihazlar üzerinden imaj (adli kopya) almayı sağlayan yazılımdır. Daha detaylı açıklamak gerekirse, ufed4pc, bütün mobil cihazlardan kritik düzeyde adli kanıtlar elde etmek için, askeri, kolluk, istihbari, şirket bilgi güvenliği gibi adli bilişim alanında faaliyet gösteren çalışanlara/kullanıcılara yönelik geliştirilmiş bir yazılımdır.

UFED4PC yazılımının öne çıkan özellikleri şunlardır;

- Mobil cihaz üzerinden fiziksel, dosya sistemi ve mantıksal imaj alma gerçekleştirerek verileri ve şifreleri elde edebilir.
- Mobil cihaz üzerinden çağrı kayıtları, telefon defteri girdileri (rehber), kısa mesajlar (sms), sohbetler (whatsapp, telegram vb.), resimler, videolar, ses dosyaları, IMEI, ICCID ve IMSI gibi ayırt edici bilgileri elde edebilir.

- Apple IOS, Blackberry, Android, Symbian, Microsoft Mobile ve Palm OS gibi işletim sistemlerinden veri elde edebilir.
- Mobil cihazın şebekeye bağlanmadan işlem yapabilmek için SIM kartını kopyalayıp kopyalanmış SIM kart üzerinden çalıştırılabilir.
- Mobil cihazlar üzerinde veri tutulmasını sağlayan bütün veritabanı dosyaları ayıklanarak üzerinde inceleme yapılabilir.
- Beraberinde gelen UFED Reader özelliği ile adli kopya analizini lisans donanımı olmadan taşımak suretiyle farklı bilgisayarlarda da incelenebilir [20].

XRY

XRY, İsveçli Micro Systemation firmasının cep telefonları, akıllı telefonlar, GPS navigasyon araçları ve tablet bilgisayarlar gibi mobil cihazlardan gelen bilgileri analiz etmek ve kurtarmak için kullanılan bir adli bilişim ve mobil adli bilişim ürünüdür. Telefonları bir kişisel bilgisayara bağlayan bir donanım cihazından ve verileri çıkarmak için bir yazılımdan oluşur.

XRY, bir cihazın içeriğini adli bilişime uygun bir şekilde kurtarmak için tasarlanmıştır, böylece verilerin içeriği kullanıcı tarafından güvenilebilir. Genellikle hukuk/ ceza soruşturmaları, istihbarat operasyonları, veri uyumluluğu ve elektronik keşif davalarında kullanılır. Yazılım kolluk kuvvetleri, askeri ve istihbarat teşkilatlarına açıktır. Dijital adli toplumda bu tür çalışmalar için ortak araçlarından biri olarak iyi tanınmıştır.

Cep telefonlarını incelerken normal bilgisayarların adli incelemesine kıyasla çok daha karmaşık zorluklar vardır. Birçok cep telefonunun kendine ait işletim sistemleri vardır, bu da bu tür cihazların tersine mühendislik yapmasını çok karmaşık bir işlem yapar. Mobil cihaz pazarının hızı ayrıca düzenli olarak üretilen daha birçok yeni cihazın olduğu anlamına gelir, bu nedenle bir mobil adli bilişim aracı, amaca uygunluk konusunda kullanıcıyı bazı problemlerle karşı karşıya bırakmaktadır.

XRY sistemi hem mantıksal incelemelere (cihaz işletim sistemi ile doğrudan iletişim) hem de fiziksel incelemelere (işletim sistemini atlayarak ve mevcut belleği boşa alarak) izin verir. Verilerin mantıksal olarak kurtarılması, daha fazla cihaz için genellikle daha iyi desteklenirken, fiziksel muayene, SMS metin mesajları, görüntüler ve çağrı kayıtları gibi daha fazla silinen bilgileri kurtarma olanağı sunar.

En son sürümler, Android, iPhone ve Blackberry cihazları gibi akıllı telefon uygulamalarından veri kurtarma desteğini içerir. XRY tarafından elde edilen veriler dünyadaki çeşitli mahkeme sistemlerinde başarıyla kullanılmıştır [21, 22].

XRY, gereksinimlerine uygun birçok farklı devlet kuruluşu tarafından test edilmiştir ve şu anda dünya çapında kullanılmaktadır.

Tarantula

İlk olarak 2011'in Ekim ayında tanıtılan Tarantula, dünya çapında hızla genişleyen bir cep telefonu ailesi olan Çin yapımı yonga setlerine dayalı sorunlu mobil cihazları hedef almaktadır. Bu cihazlar tarihsel olarak marka dışı telefonlar olarak da bilinirler. Gittikçe daha fazla sayıda Çin yongası, akıllı telefonlar da dâhil olmak üzere büyük marka telefonları tarafından benimsenmiştir.

Tarantula 2.0 sistemi, bu cihazların analizini büyük ölçüde basitleştirir ve hızlandırır. Tarantula, Çin'in tüm büyük yonga setlerinden (Mediatek, Spreadtrum ve Infineon) fiziksel olarak çıkartma ve kod çözmeyi destekleyen, telefonun PIN kilitli olup olmadığına bakmayan tek mobil adli bilişim sistemidir. Tüm fiziksel analizleri kullanan Tarantula 2.0, silinen veriler de dâhil olmak üzere düşük düzeyli verileri ayıklar ve kodlarını çözer, telefon dosya sisteminin kodunu çözer ve çağrı kayıtları, SMS, telefon rehberi, medya dosyaları, şifreler ve IMEI'ler gibi verileri sunar.

Akıllı telefonlarda Çince çiplerin kullanımına yönelik bir endüstri eğiliminin ardından Şekil 3.6 da gösterilen Tarantula 2.0, günümüzde hem Akıllı Telefon yonga setlerini hem de Android Smartphone'u desteklemektedir.

Şekil 3.6 Tarantula Cihazı ve Destek Ekipman Çantası

Mobiledit

Mobiledit cep telefonu ile kişisel bilgisayar arasında arayüz sağlayan bir uygulamadır. Bilgisayarı kullanarak telefona girdi girişi yapılarak üretkenliği ve iletişimi arttırmaya yardımcı olmak için tasarlanmıştır. Cep telefonuna fotoğraf, SMS mesajı, belge ve diğer önemli verileri göndermek için de kullanılır.

MOBILedit Lite, gündelik kullanıcılar için tasarlanmıştır. Adli bilişim alanında, yasal soruşturmalara yardımcı olmak için tasarlanmıştır. Kendi türündeki diğer programlardan daha fazla marka ve modeli destekler.

Bu uygulama telefonun modeline bağlı olarak BlueTooth, Infrared veya kablo ile telefonlarla iletişim kurulmasını sağlar. Her telefon için temel sürücüler programla birlikte yüklenir. Ancak, başka bir sürücüye ihtiyaç duyulursa, telefonun desteklendiği varsayılarak web sitesinden indirilebilir.

Bir mobil adli bilişim yazılımı olarak, Mobiledit şu özelliklere sahiptir:

- Doğrudan cep telefonuna bağlı bir bilgisayardan SMS mesajları ve telefon aramaları gönderme
- Cep telefonunun pil ömrünü, sinyal kalitesini ve mevcut şebeke operatörünü izleme
- Telefondaki her şeyi bilgisayarın ekranına getirerek, telefonun daha kolay kullanılmasını sağlama
- Kullanıcının bir telefonu kişisel bir bilgisayardan kontrol etmesine izin verme
- Microsoft Outlook ile e-postayı cep telefonuna senkronize etme
- MOBILedit 'e bağlanmak için birden fazla cihaz yapılandırma
- Herhangi bir dilde güvenli raporlar oluşturma
- Belirli işlevler için belirli şablonlar oluşturma ve toplanan verileri şablona ekleme

Programın tüm fonksiyonları ana ekranda bulunur. Ayrıca, kullanıcının e-postasını telefonuyla Outlook ile senkronize etmesini sağlayan Microsoft Outlook ile de tam olarak uyumludur. Mobiledite bağlanmak için birden fazla cihaz konfigüre edilebilir.

Mobiledit tüm verileri cep telefonundan toplar ve kaydedilebilecek veya yazdırılabilecek bir kişisel bilgisayar hakkında kapsamlı bir rapor oluşturur.

Mobiledit salt okunurdur, böylece cihazdaki değişiklikleri önler ve potansiyel olarak zarar verebilecek kanıt kayıplarını önler. Tüm ürünler ayrıca dijital imzalarda kullanılan hash fonksiyonları ile daha sonra yapılacak değişikliklere karşı korunmaktadır. Telefon defteri gibi tüm veri blokları MD5 hash algoritması ile korunmaktadır. Her bir öğenin olası değişiklik yerini hızlıca bulmak için kendi MD5 kodları vardır.

Oxygen

Oxygen Software tarafından üretilen yazılım mobil cihazlardan veri ayıklama ve adli analiz/raporlama işlerinde yaygın olarak kullanılmaktadır. Yazılımın öne çıkan yönleri gelişmiş ve detaylı raporlama özellikleri ve birçok farklı donanıma ve mobil işletim sistemine destek verebiliyor olmasıdır.

Yazılım temel olarak, çalışan cihaz üzerinde ve cihazın daha önceden alınmış adli kopyası üzerinde analiz ve raporlamalar gerçekleştirmektedir. Oxygen Forensic yazılımı 8000'den fazla mobil cihazdan veri ayıklayabilmekte ve analizini yapabilme yeteneğine sahiptir. Analizini yapabildiği mobil işletim sistemleri iOS, Android, Windows Phone 8, Windows Mobile 5/6, Blackberry, Symbian ve Bada olarak sıralanabilir.

Faraday

Faraday çantaları, telsiz delillerinin toplanması, korunması, taşınması ve analizinde kolluk kuvvetlerine, askeri ve araştırmacılara yardımcı olmak için tasarlanmıştır. Cep telefonları, GPS, netbook' lar, bluetooth cihazları, dizüstü bilgisayarlar vb. gibi kablosuz cihazlar, faraday çantalarının içinde bulundukları koruyucu sistem aracılığıyla hücresel, WiFi, bluetooth ve radyo sinyallerine karşı korumalıdır. Koruma sistemi, sahada ve laboratuarda kullanım için hafif ve dayanıklı olarak tasarlanmıştır.

Faraday çantaları, radyo frekans sinyallerinin maksimum koruması için tasarlanmıştır. Faraday Çantalarının içine yerleştirildiğinde, cep telefonları ve diğer mobil cihazlar artık ağa bağlanmayacak, açık kalırken cihazın uzaktan silinmemesini, uzaktan yerleştirilmesini veya kilitlenmesini sağlamayacaktır.

Faraday torbaları olmadan, incelemeciler değerli uçucu verileri kaybedebilir veya cihaz tekrar açıldığında bir telefon/ SIM kilidi ile karşılaşabilir. Faraday çantasının gösterir görüntü **Şekil 3.7.** de sunulmaktadır.

Şekil 3.7 Faraday Çantası

EnCase

Encase Forensic, Guidance Software Inc şirketine aittir ve Guidance tarafından üretilmiştir. Adli bilişim alanında en yaygın kullanılan inceleme yazılımlarından biridir. Adli kopyaları görüntüleme ve korumadan, anahtar kelime arama ve temel veri kurtarma işlemlerine, bayt düzeyinde bir sabit sürücünün analizine kadar çeşitli adli bilişim fonksiyonlarını gerçekleştirebilme yeteneğine sahiptir.

Binlerce incelemeci lisans satın alarak kullanmaktadır. Gelişmiş donanım özelliklerine sahip olan Encase ile Motorola, Nokia, Siemens, Samsung, LG, Palm, BlackBerry, HTC, Sony Ericsson, UTStarcom markaların hatta daha fazlasını içeren en yaygın mobil cihaz üreticilerinin donanımların adli bilişim analizleri yapılabilmektedir. Mobil cihazların adli bilişim işlemleri yapmak maksadıyla tasarlayan Encase, zamanla endüstri lideri haline gelmiştir.

Paraben’s Device Seizure

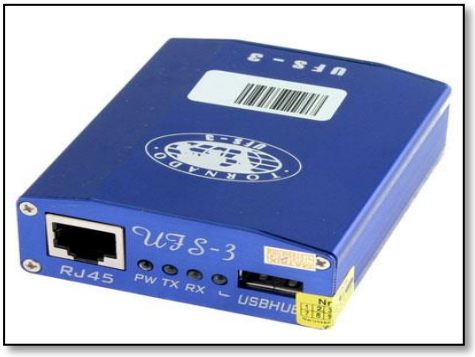
Paraben’s Device Seizure cep telefonları ve PDA' lardaki verileri incelemek için kullanılan bir yazılımdır. Fiziksel bir toplama yöntemi kullanır. İPhone eklentisinden elde edilen veri miktarı işletim sisteminin sürümüne bağlı olarak değişebilmesine rağmen, LG, Motorola, Nokia, Siemens, Samsung, Sony Ericsson ve iPhone tarafından üretilen telefonları destekler. Ayrıca telefonun Root/Jailbreaking yazılımı kullanılarak açılıp açılmadığını tespit edebilmektedir. Araç aynı zamanda bir SIM kart okuyucu kullanan GSM SIM kartlarını da destekler.

Bu yazılımda tüm işletim sistemlerinin tüm sürümleri desteklenmese de Palm OS, Windows CE, Cep Bilgisayarı ve Windows Mobile, Blackberry, Symbian ve EPOC çalıştıran PDA'ları da desteklemektedir.

Üretici firma, ürünün Garmin GPS cihazlarından veri kurtarabildiğini iddia etmektedir, ancak bu durum henüz doğrulanmamıştır.

Flasher Box

Mobil cihazlarda PIN ve güvenlik kilitlerini kırmak amacıyla kullanılan cihaza verilen isimdir. Birçok marka ve model mobil cihazı destelemekte olup adli bilişim incelemelerinde kullanılabilmektedir. Kullanımı ciddi derecede hassasiyet gerektirdiğinden yanlış veya hatalı kulanılması durumunda mobil cihaza kalıcı zararlar verebilmesi mümkündür. Flasher Box aletini gösterir ekran görüntüsü **Şekil 3.8** de sunulmaktadır.



Şekil 3.8 Flasher Box

3.4.3. GPL Lisanslı Adli Bilişim Araçları

Mobil cihazların adli bilişim açısından incelenmesinde genel olarak kullanılan GPL lisanslı adli bilişim araçları hakkında bu başlıkta bahsedilecektir.

Deft

DEFT (Digital Evidence & Forensics Toolkit'in kısaltması), aygıtlara zarar vermeden veya bozmadan sistemlerde (hard diskler vb.) önyükleme işleminin gerçekleştiği PC / Mac'e bağlı olarak çalışan ücretsiz bir adli bilişim aracıdır. DEFT sistemi GNU Linux'a dayanmaktadır, canlı (DVDROM veya USB aracılığıyla) çalışabilir veya VMware'de Sanal Cihaz olarak çalışabilir. Tüm bunların yanı sıra DEFT birçok yerde ve farklı meslek gruplarında kullanılmaktadır. Bunlardan birkaçı şunlardır:

- Kolluk Kuvvetleri
- Devlet Memurları
- Bilirkişiler
- Adli Bilişim Araştırmacıları
- Uzman Tanıklar
- BT Denetçileri
- Üniversiteler
- Bireyler

DEFT %100 İtalya'da üretilmiştir ve Tesla Danışmanlık şirketlerinin Ar-Ge Ofisi tarafından yönetilen ve sürdürülen bir projedir [23].

Bitpim

BitPim, telefonunuzun birçok özelliğine erişmenizi sağlayan ücretsiz, açık kaynaklı bir yazılım programıdır. Telefonunuzdaki rehber, resimler, duvar kâğıtları, arama geçmişi, kısa mesaj geçmişi, zil sesleri, müzik, videolar ve takvim gibi verilere erişebilme yeteneğine sahiptir. BitPim, cep telefonu verilerini bilgisayarınıza yedeklemenizi sağlar, bunun tersi olarak dosyaları bilgisayarınızdan telefonunuza da aktarabilme imkânı sağlar [24].

BitPim PC, Mac ve Linux işletim sistemlerinde mevcuttur, ancak yalnızca CDMA telefonlarla çalışır. ABD'de Verizon ve Sprint en büyük CDMA taşıyıcılarıdır (AT&T ve T-Mobile, GSM şebekelerini kullanır) [25].

Tulp 2G

Tulp 2G (2^{nd} Generaiton), hücresel telefon ve SIM kartlardan veri çıkarma ve okumak için kullanılan açık kaynak kodlu bir adli bilişim aracıdır. Tulp 2G, bir veri kablosu, Bluetooth veya IrDA Bağlantısı ve uyumlu bir protokol eklentisi kullanarak cep telefonundan veri alır [26].

Caine

CAINE Linux, adli bilişim inceleme işlemini gerçekleştirmek için gereken tüm araçları sağlayan açık kaynaklı bir adli bilişim platformudur. Aynı zamanda, adli bilişim uzmanları için önem arz eden ve çok çeşitli adli bilişim araçlarıyla birlikte gelir. İnceleme esnasında bir bilgisayarda meydana gelenleri araştırmak için kolluk kuvvetleri, askeri ve kurumsal adli bilişim uzmanları tarafından kullanılabilir.

CAINE, veritabanı, bellek ve ağ analizini destekleyen yazılım araçları sunar. Linux, Microsoft Windows ve bazı Unix platformlarının incelenmesi için imkân sağlar. CAINE' da ayrıca bir Windows IR/ Live Forensic aracı da vardır [27].

- Sleuth Kit
- Authopsy
- WinAudit
- PhotoRec
- RegRipper
- Tinfoleak
- Fsstat
- USB Write Blocker
- Windows File Analyzer
- MWSnap
- Wireshark
- Arsenal Image Mounter
- FTK Imager
- Hex Editor
- JpegView
- NTFS Journal Viewer
- QuickHash
- NBTempoW

Pilot-Link

Pilot-link, Linux topluluğu ve Palm OS cihazları arasındaki aktarılması gereken bilgilerin izin verilmesi için orijinal olarak geliştirilmiş açık kaynaklı bir yazılımdır.

Pilot-link, bir Linux (BSD, Solaris, Dijital UNIX / Tru64, Linux, AIX, POSIX uyumlu herhangi bir vb.) iş istasyonunu bir Palm OS'a bağlamak için en yaygın kullanılan yöntemi oluşturan komut satırı programları topluluğudur [28]. En sık kullanılan program bir Palm OS'tan PDA'ya veya PDA'dan Palm OS'a dosya transferi yapan pilot-xfer programıdır. Bu, kullanıcının USB karakter modu cihazlarını yapılandırmasına gerek kalmadan doğrudan Linux USB alt sistemine bağlanır. Pilot-Xfer cihazın mantıksal içeriklerini almayı sağlar. Bu kullanım alanları ile elde edilen herhangi bir konumdaki veriler, gerekirse bir hex editörü ile çıkarılabilir. Pilot-link, elde edilen bilgilerin hash değerlerini hesaplamaz.

Osaf

OSAF-Toolkit, Cincinnati Üniversitesi'nden bir grup bilişim öğrencisi tarafından üst düzey bir tasarım projesi olarak Android zararlı yazılım analizinin standardizasyonuna öncülük etmek ve önünü açmak amacıyla geliştirilmiştir. OSAF-Toolkit, Ubuntu 11.10' dan üretilmiştir. Tersine mühendislik incelemesi ve zararlı yazılım analizi uygulamaları ayırmak için gereken tüm araçlar ile önceden derlenmiştir [29].

4. MOBİL SOHBET UYGULAMALARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Günümüzde internet kullanımı ile paralel mobil cihazların kullanımının yaygınlaşması neticesinde bu cihazlar üzerinde çalışan birçok uygulama geliştirilmiştir. Bu uygulamalara bakıldığında kullanım olarak sohbet uygulamalarının daha sık uygulama marketlerinden indirildiği ve kullanıldığı görülmektedir. Birbiri ile aynı özelliklerin yanında kendilerine özgü özellikleri de barındıran sohbet uygulamaları ile ilgili olarak bu başlık altında dosya yapıları, veri tabanı yapıları, şifreli ve şifresiz verilerin saklanma yöntemi, medya dosyalarının tutulma şekli gibi bilgilere bakılarak hangi verilerin elde edilebileceğine yönelik çalışmalar ortaya konacaktır.

4.1. Mobil Cihaz Sohbet Uygulamaları

Whatsapp: WhatsApp, şüphesiz dünyanın en popüler mesajlaşma platformlarından biri. İnternet üzerinden karşılıklı mesajlaşma ve dosya göndermeye yarayan programlardan olan WhatsApp, GSM operatörlerine ödediğimiz kısa mesaj ücretlerini aza indirgemeye çalışır.

Telegram: Telegram, Whatsapp' a rakip olarak kurulan anlık mesajlaşma uygulamasıdır. Her geçen gün kullanıcı sayısını hızla artırıyor. Milyonlarca kullanıcı sayısına ulaşan Telegram, büyümesini her geçen gün sürdürerek, daha çok insana ulaşmayı hedefliyor.

Skype: Skype' ın metin ve benzersiz sesli ve görüntülü çağrı özellikleri sayesinde kolayca başkalarıyla iletişime geçebilirsiniz. Bire bir konuşma ve grup konuşmaları için tasarlanmıştır.

Line: Whatsapp gibi anlık mesajlaşma uygulamasıdır. Line, 2011 Haziran ayından itibaren yayına girmiştir. Kullanıcı sayısı da hızla büyüyor. Japonya'da ve uzak doğu ülkelerinde Whatsapp'tan daha popüler bir uygulamadır. Whatsapp'a göre güvenlik ayarları çok daha gelişimiş ve kullanılması kolay ve pratik olduğundan tercih ediliyor.

Viber: Viber de kişiler 7000 karaktere kadar mesaj gönderebilmektedir bu da kullanıcılarına oldukça geniş bir yazı alanı sunmaktadır. Bunun yanı sıra Viber uygulamasına sahip kişileri görüntülü aramak, mesaj göndermek ücretsizdir. Fakat burada önemli bir detay bulunmaktadır. Kişi, Viber uygulamasını kullanıyor olsa bile aranılan kişide Viber uygulaması yoksa arama Viber üzerinden değil, telefonun kendi mevcut tarifesi üzerinden gerçekleşecektir.

Falcon: Falcon bir güvenli anlık mesajlaşma uygulaması olup Google Cloud Messaging hizmeti üzerinden çalışmaktadır. Bu uygulama üzerinden gönderilen ve alınan veriler şifrelenmektedir. Ve 256-bit uçtan uca AES şifrelemesi ile korunur. Günümüzde terör örgütü mensupları arasında şifreli olması ve verileri belirlenen bir süre sonra silmesi nedeniyle kullanılmış olduğu bilinmektedir.

4.2. Mobil Cihaz Analiz Sürecinde Karşılaşılan Zorluklar

Günümüzde işlenen suçların birçoğunda adli inceleme yapılaması için kolluk kuvvetleri tarafından delil olabileceği şüphesi ile alınan mobil cihazlarla karşılaşmaktayız. Bu cihazlar telefon, tablet veya bir simcard olarak karşımıza çıkmaktadır. Cihaz adli incelmeye başlanılmasından öce izole edilmelidir. Android ve IOS işletim sistemleri yaygın olarak incelenecek cihazların işletim sistemlerini oluşturmaktadır. Daha az ihtimalle Symbian ve Windows Mobile işletim sitemine sahip mobil cihazlarda bulunmaktadır.

Donanım Farklılıkları: Mobil cihaz pazarında insanların mobil cihazlar için sürekli artan istekleri karşısında üreticilerin talepleri karşılamasıyla performansı ve güveliği daha geliştirilmiş farklı kesimlere hitap eden cihazlar üretmektedir. Buda mobil cihazlar içinde çeşitliliğe sebep olmaktadır. Bu durum kısa bir ürün geliştirme süreci sonucunda çok farklı modellerin üretilmesi anlamına gelmektedir. Bu çeşitlik farklı boyuttaki dahili hafızalar, sahip oldukları farklı kapasitede Ram bellekler, işlemci farklılıkları ve cihazların farklı işletim sistemlerine sahip olması olarak gösterilebilir. Mobil adli inceleme sürecinde adli incelemeyi yapan kişinin bu değişime uyum sağlayabilmesi ve inceleme yaptığı yazılım ve donanımın sürekli güncel tutulması gereklidir.

İşletim Sistemi Farklılıkları: Google firmasına ait Android, Apple firmasına ait IOS veya Microsoft firmasının Windows Mobile işletim sistemleri gibi pek çok işletim sistemi bulunmaktadır. Her ne kadar Android ve İOS mobil cihaz piyasasını domine etmiş olsa da adli bir inceleme için Symbian, Blackbery OS, webOS gibi çok bilinmeyen işletim sistemlerine sahip mobil cihazların incelenmesi istenebilir.

Mobil Cihazların Güvenlik Özellikleri: Mobil uygulamaların gizlilik ve güvenlik yönüyle üst düzey tasarımlara sahip olması ülkelerin mevcut iletişimin tespiti olanaklarını da sonuçsuz bıraktığı bilinmekle birlikte insanlar için gizlilik kişisel verilerinin güvende olması adına önemli bir kavramdır [30]. Mobil cihaz üreticileri kullanıcının gizlilik ihtiyacını ve kullanıcının verilerinin maksimum şekilde güvende tutulması için farklı güvenlik mekanizmaları kullanmaktadır. Modern cihazlar donanım ve yazılım katmaları arasında tanımlı şifreleme mekanizmaları kullanır. Bu da adli inceleme sürecinde bu şifrelemelerin kırılması gerektiği anlamına gelmektedir.

Kaynak Eksikliği: Mobil cihazların çeşitliğinin artması adli inceleme yapacak kişinin cihazlara uygun USB kablolara, bataryalara veya şarj cihazı gibi ekipmanlara sahip olmasını gerektirmektedir.

İncelenecek Cihazın Durumu: Adli incelemeyi yapacak kişiye gelecek cihazın ekran kilidine sahip olabileceği, İncelenmesi istenen delilin fiziksel olarak hasarlı, veri yolunun bozuk, şarj probleminin olabileceği veya mobil cihazın bir uygulamayla şifrelenmiş olabileceği ihtimaline karşı dikkatli davranılması gerekmektedir. Ayrıca arka planda çalışan uygulamaların veri kaybına, cihazdaki verilere zarar vermesine veya veri transferine sebep olabileceği için adli incelemeyi yapan kişinin önlem almasını gerektirir.

Anti Adli Teknikler: Teknolojinin hızlı bir şekilde geliştiği bu dönemde suça karışan kişilerinde teknolojik bilgi birikimlerinin arttığı gözlenmektedir. Şüpheli şahısın yakalanması durumuna karşı veri gizleme, veri sahteciliği veya güvenli silme (wipe) gibi anti adli yöntemleri kullanabileceği için adli incelemeyi yapacak kişinin dikkatli olması gerekmektedir.

Kanıtların Yapısı: Mobil cihazlar bilerek veya bilmeyerek değiştirilebilir. Örnek olarak mobil cihazda bir uygulamayı incelemeye çalışmak uygulamanın cihazdaki verileri kalıcı olarak değiştirmesine sebep olabilir.

Uygulamalar: Mobil cihazlarda varsayılan olarak gelen veya kullanıcı tarafından cihaza kurulmuş pek çok uygulama bulunur. Bu uygulamalar kullanıcı geri bildirimleri ile uygulamayı geliştirenler tarafından sürekli güncel tutulur veya yenilenir. Adli incelemede kullanılan araçlarında bu güncelleştirme ve gelişim sürecine ayak uydurması gerekmektedir. Adli incelemeyi yapan kişinin ise araçlarını sürekli güncel tutması gerekmektedir. Adli incelemede kullanılan araç uygulamalardaki güncelleştirmeler karşısında yetersiz kalırsa adli incelemeyi yapan kişinin downgrade yaparak cihazdaki verilere erişmesi gerekmektedir.

Cihazın Sıfırlanmış Olması: Mobil cihazlarda kullanıcının isteği dahilinde kullanabileceği cihazı sıfırla veya fabrika ayarlarına geri dön şeklinde seçenekler bulunmaktadır. Adli inceleme için gönderilen mobil cihazın sıfırlanmış olması adli inceleme yapacak kişinin veri kurtarma yapmasını gerektirir. Böyle bir durumda adli inceleme yapacak kişinin elde edebileceği veriler kısıtlı olacaktır.

Şifreli Mobil Cihaz: Adli incelemede incelenecek cihaz şifreliyse adli incelemeyi yapacak kişinin cihazdaki verilere zarar vermeden cihazdaki verilere ulaşması gerekmektedir.

İzolasyon: Mobil cihazların Wifi, Bluetooth veya Kızılötesi kullanarak kablosuz veri transferi yapabildiği bilinmektedir. Ayrıca mobil cihazın GSM operatörünün baz istasyonu ile iletişiminin kesilmesi gerekmektedir.

Mobil Adli İncelemede Kullanılan Araçların Yetersizliği: Mobil cihazların çeşitliliği sebebiyle bir araç tüm cihazları desteklemeyebilir. Bu sebeple adli inceleme yapan kişinin birden fazla araç kullanmasını gerektirir.

Zararlı Yazılımlar: Adli inceleme yapılacak mobil cihaz virüs veya Trojan gibi kötü amaçlı yazılımları içerebilir. Kablolu bir ara yüzden yayılmaya alışacağı gibi kablosuz olarak da yayılmaya çalışabilir. Bu da adli inceleme yapacak kişinin dikkatli davranmasını gerektirir.

Yasal Zorunluluklar: Adli incelemeyi yapan kişi suçun niteliğinin ve yasal sınırların bilincinde olmalıdır.

4.3. Mobil Cihaz Sohbet Uygulamaları Analizi

Yaygın olarak kullanılan mobil sohbet uygulamalarından Whatsapp, Telegram ve Skype ile hali hazırda uygulama marketlerinde olmayıp ancak kurulum dosyası bulunan Falcon isimli sohbet

uygulamasının android işletim sistemi üzerine kurulumları gerçekleştirilmiştir. Sonrasında alınan mobil cihazın imajında ve sanallaştırılan android işletim sistemi üzerinde mobil uygulamalar ayrı ayrı analiz edilmiştir. Bu analizde sohbet uygulamalarının veri tabanı yapıları, şifreli ve şifresiz veriler, medya dosyalarının tutulma şekli gibi bilgilere bakılarak hangi verilerin elde edilebileceğine yönelik çalışmalar ve zorluklardan bahsedilmiştir [31]. Yapılan analizlere ait sonuçlar aşağıda başlıklar halinde sunulmuştur.

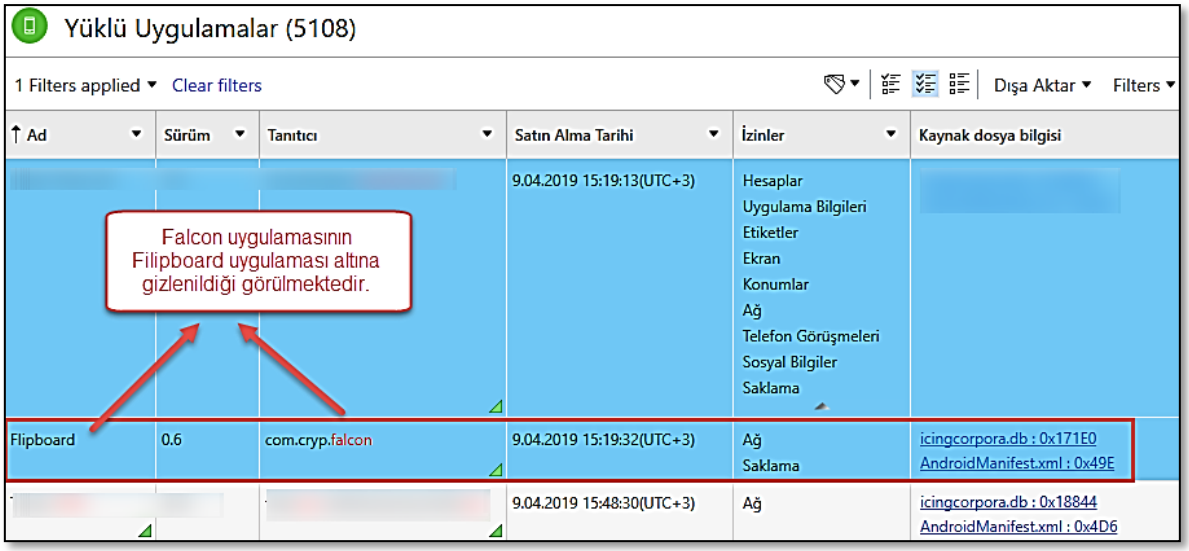
4.3.1. Falcon Sohbet Uygulaması Analizi

Falcon isimli sohbet uygulaması günümüzde kullanılan uygulama marketleri üzerinde bulunmayıp Türkiye' de FETÖ/PDY Silahlı Terör Örgütü tarafından tasarlanarak örgüt üyelerinin birbirleri ile şifreli olarak yazışmalar gerçekleştirildiği belirtilen bir şifreli sohbet uygulaması olarak bilinmektedir.

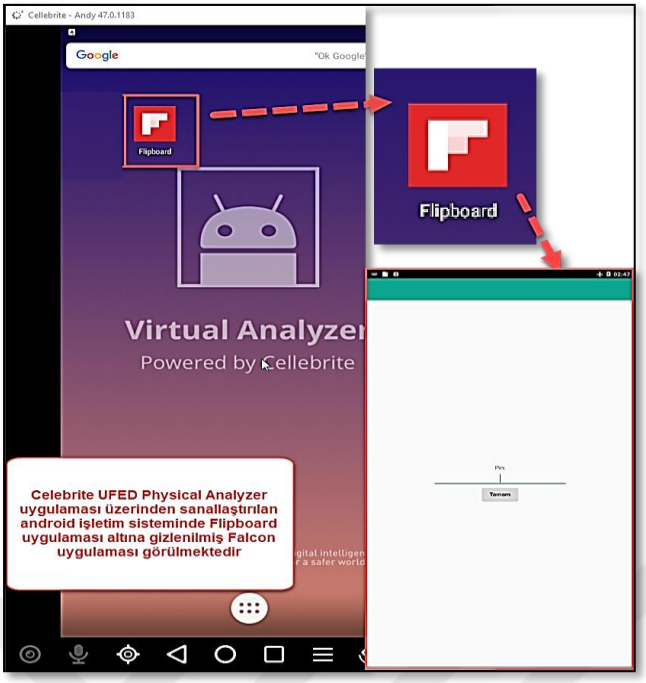
Falcon sohbet uygulaması ile ilgili olarak gerçekleştirilen analizler aşağıda sunulmuştur.

Yapılan incelemelerde Falcon sohbet uygulaması ilk olarak popüler uygulamalardan Flipboard isimli uygulamanın isim ve simgesinin altına gizletilmiştir. Sonrasında cep telefonun imajı alınmış ve UFED Physical Analyzer 7.21.1.7 uygulaması ile açılmıştır.

UFED Physical Analyzer yazılımında Yüklü Uygulamalar başlığına bakıldığında Falcon (com.cryp.falcon) uygulamasının FlipBoard uygulaması altına gizletildiği görülmekte olup **Şekil 4.1.** ve **Şekil 4.2** de sunulmaktadır.

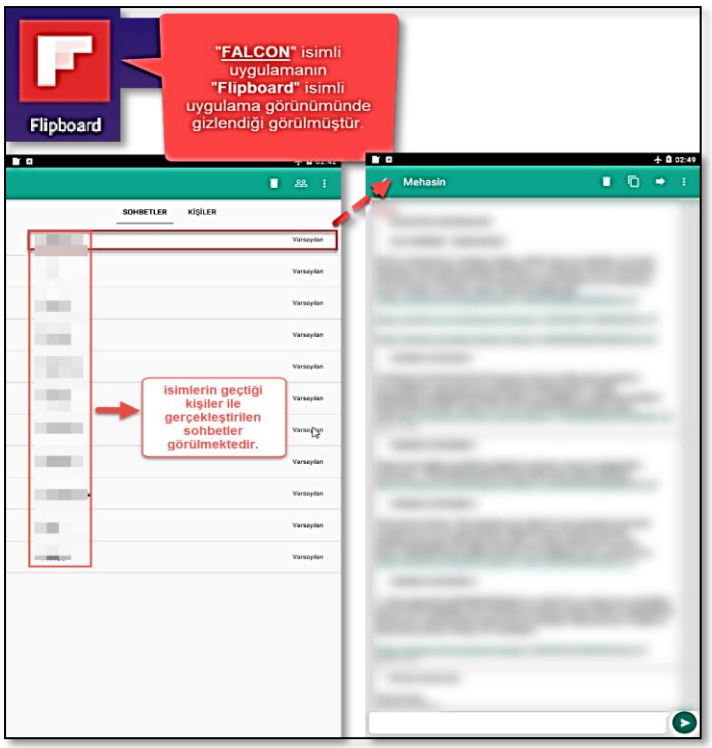


Şekil 4.1 Falcon' un FlipBoard uygulaması altına gizlenmesi



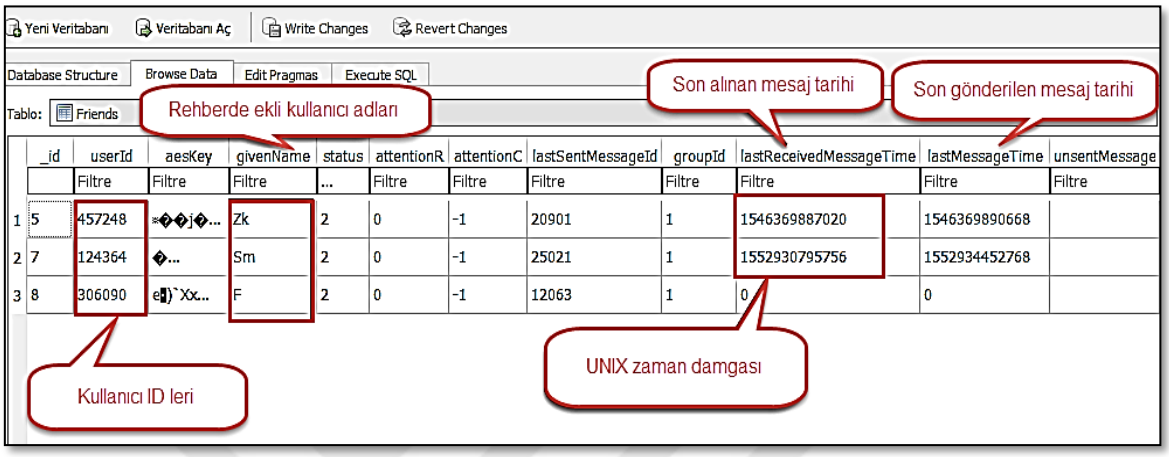
Şekil 4.2 Falcon' un FlipBoard' a ait ikon ile gösterilmesi.

Flibboard uygulamasına ait simge altına gizlenmiş olan Falcon uygulamasının arayüzü ile sohbet tabloları **Şekil 4.3**'te gösterilmektedir.



Şekil 4.3 Falcon arayüzü ve sohbet tabloları

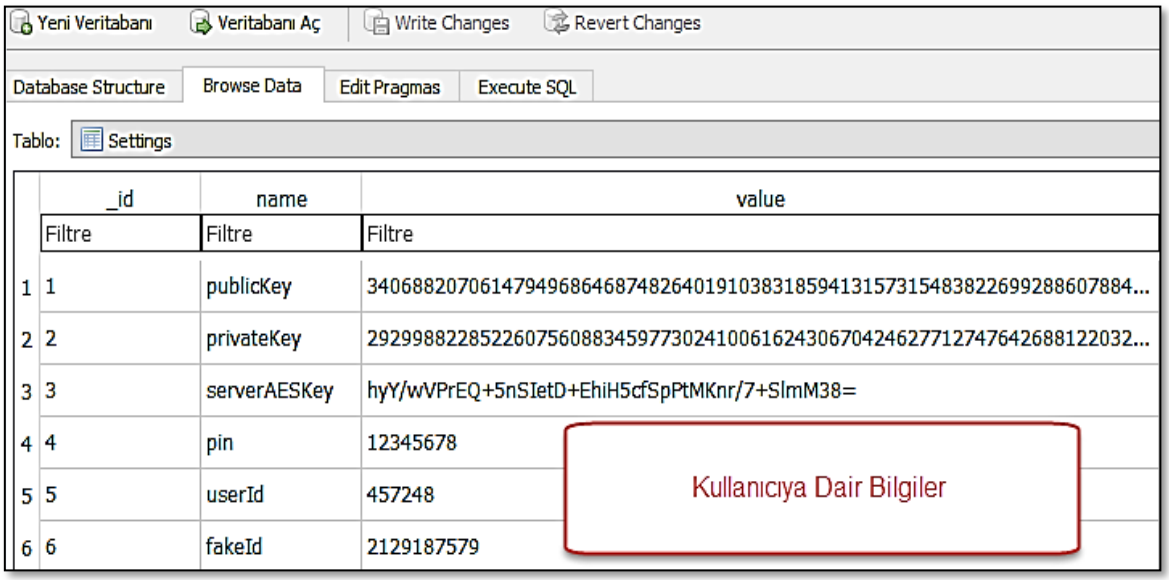
Falcon uygulamasına ait "userdata (ExtX)/Root/data/com.cryp.falcon/databases/" veri yolundaki "enc.db" isimli veri tabanı dosyasına bakıldığında "user id, kullanıcı adları, son alınan mesaj zamanı, son gönderilen mesaj tarihi" gibi bilgileri içerdiği görülmekte olup **Şekil 4.4** te sunulmaktadır.



	_id	userId	aesKey	givenName	status	attentionR	attentionC	lastSentMessageId	groupId	lastReceivedMessageTime	lastMessageTime	unsentMessage
	Filtre	Filtre	Filtre	Filtre	...	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	5	457248	×��j�...	Zk	2	0	-1	20901	1	1546369887020	1546369890668	
2	7	124364	...	Sm	2	0	-1	25021	1	1552930795756	1552934452768	
3	8	306090	e]`Xx...	F	2	0	-1	12063	1	0	0	

Şekil 4.4 Falcon veri tabanında arkadaş listesi tablosu

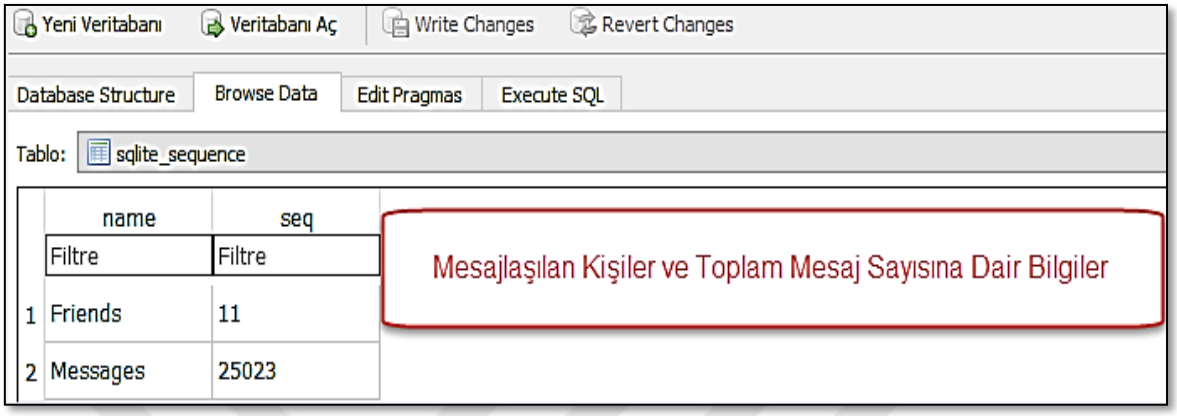
Falcon uygulamasına ait veri tabanı dosyasında "Settings" tablosuna bakıldığında Falcon kullanıcısına dair kullanıcı ID, Kullanıcı Sahte ID, PIN gibi bilgilerin yer aldığı görülmekte olup **Şekil 4.5** te sunulmaktadır.



	_id	name	value
	Filtre	Filtre	Filtre
1	1	publicKey	3406882070614794968646874826401910383185941315731548382269928860788 4...
2	2	privateKey	2929988228522607560883459773024100616243067042462771274764268812203 2...
3	3	serverAESKey	hyY/wVPrEQ+5nSIetD+EhiH5cfSpPtMKnr/7+SlmM38=
4	4	pin	12345678
5	5	userId	457248
6	6	fakeId	2129187579

Şekil 4.5 Falcon veri tabanında ayarlar tablosu.

Falcon uygulamasına ait veri tabanı dosyasında "sqlite_sequence" tablosuna bakıldığında mesajlaşılan kişiler ve tüm mesajların sayısal değerlerine dair bilgilerin yer aldığı görülmekte olup **Şekil 4.6** da sunulmaktadır.



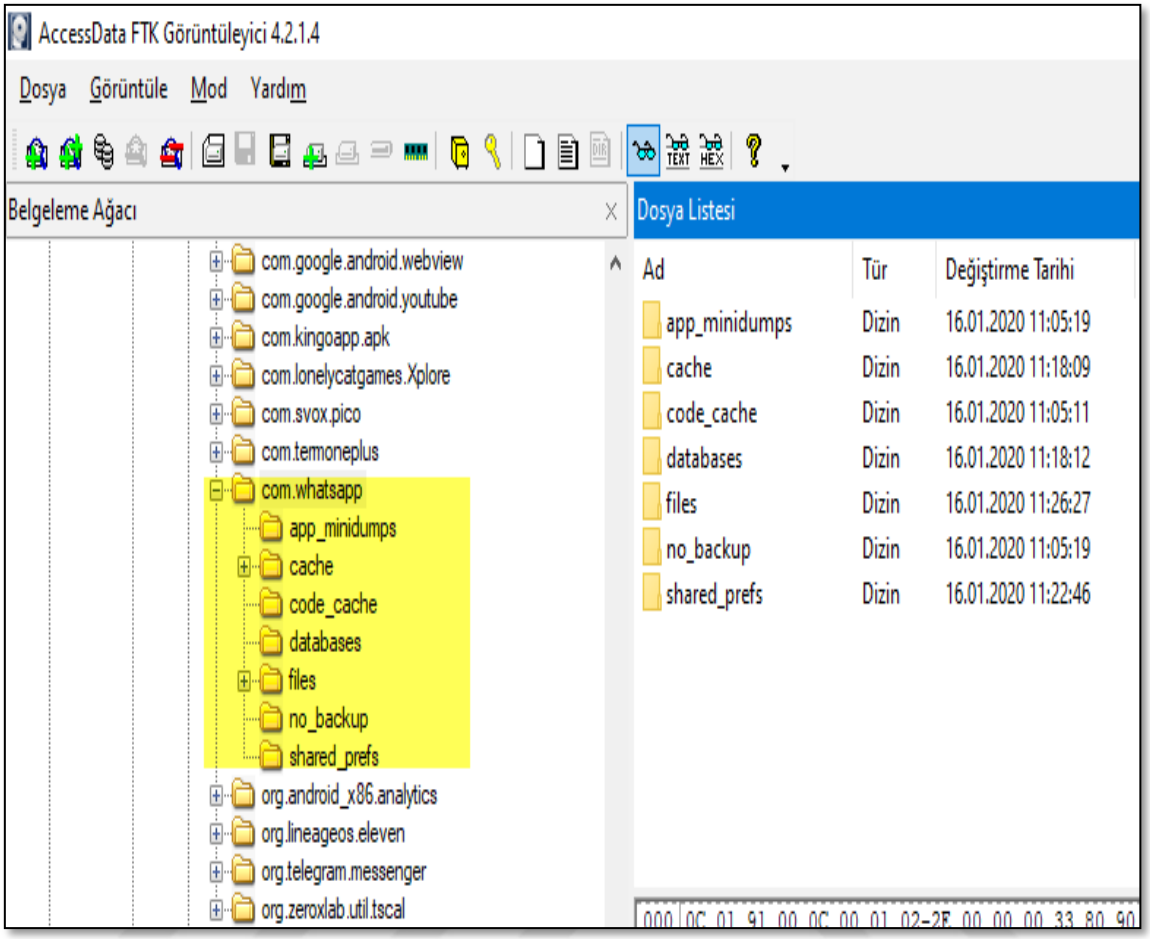
Şekil 4.6 Falcon veri tabanında kişiler ve toplam mesaj adedi bilgisi

4.3.2. Whatsapp Sohbet Uygulaması Analizi

Whatsapp uygulaması günümüzde uygulama marketleri üzerinde 1 milyardan fazla indirme sayısına sahip Dünyanın en çok kullanılan anlık mesajlaşma ve görüşme uygulamasıdır. İlk verisonlarında sadece anlık mesajlaşmaya imkân sağlarken günümüz itibari noktadan noktaya şifreleme ile korunan ile anlık mesajlaşmanın yanı sıra sesli ve görüntülü görüşme olanağı sağlamaktadır.

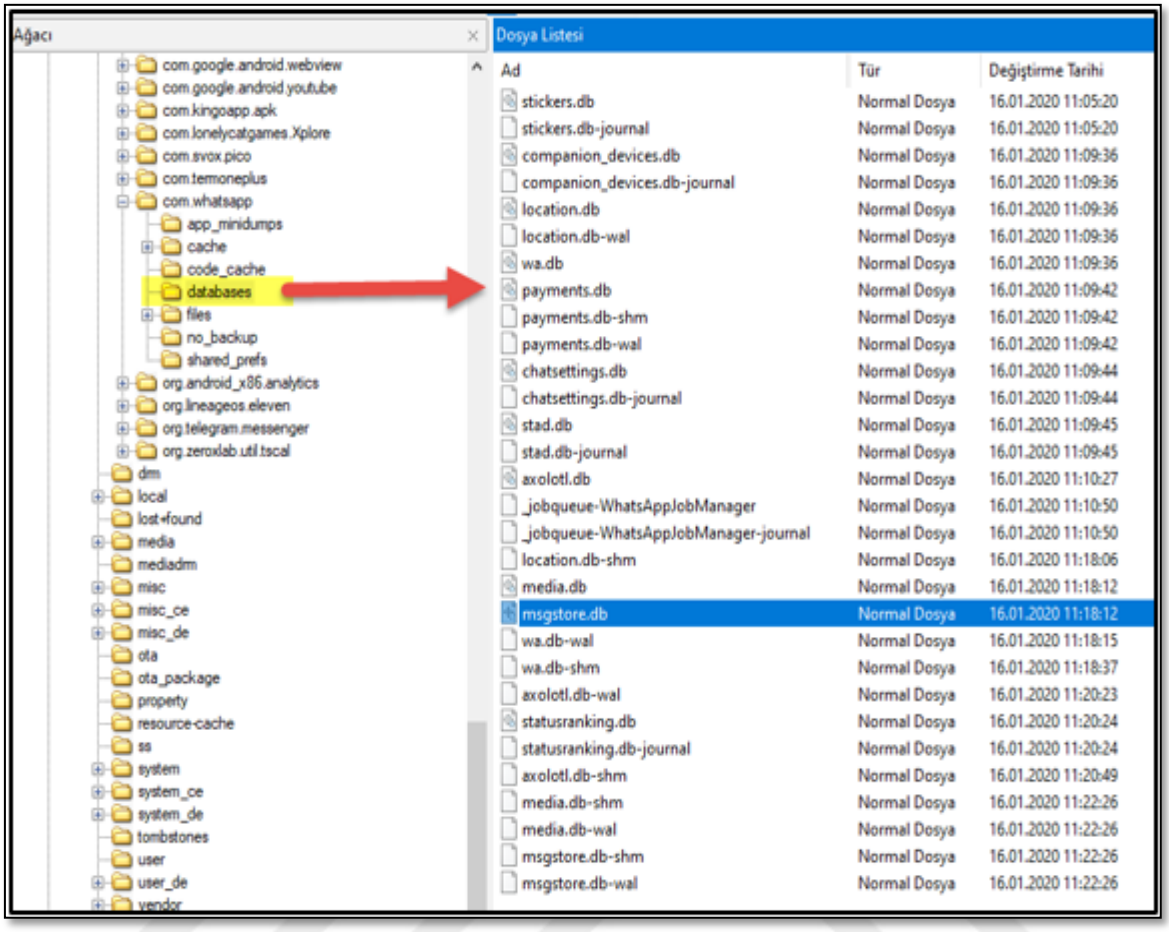
Yapılan incelemelerde öncelikle; VMware Workstation yazılımında hazırladığımız sanal android işletim sisteminde bir Google hesabı tanımlanmıştır. Play Store isimli uygulama marketi üzerinden Whatsapp isimli mesajlaşma uygulaması indirilip yüklendikten sonra Whatsapp uygulamasına telefon numarası doğrulaması yapark giriş yapılmış akabinde mesaj, sesli mesaj, resim ve video gönderme işlemleri simüle edilerek sanal makine kapatılmıştır.

Akabinde WMware Workstation kapatılarak sanal işletim sistemine ait .vmdk dosyası Access Data FTK Imager yazılımı ile açılmıştır. İnceleme aşamaları aşağıda sunulmuştur. Whatsapp uygulamasının root dizini üzerindeki yeri ve içerdiği klasör yapıları **Şekil 4.7** de görüntülenmektedir.



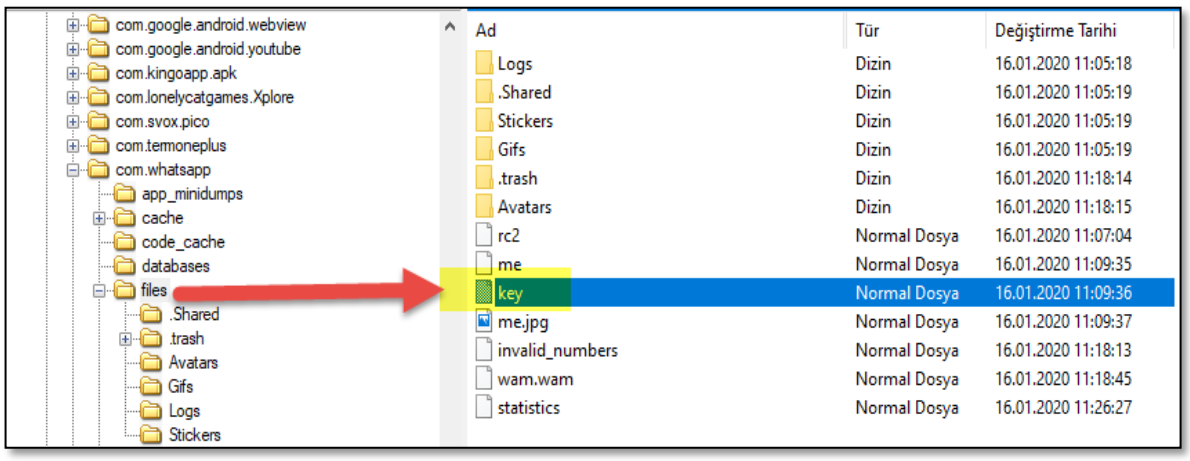
Şekil 4.7 Whatsapp' ın root dizini üzerindeki yeri ve klasör yapıları

Uygulama kurulması ile "root\data\data\com.whatsapp" dizini üzerinde "database" klasörü içerisinde mesajlaşma içeriklerini barındıran veritabanı dosyalarının bulunduğu görülmekte olup **Şekil 4.8.** de sunulmaktadır. "files" klasörü içerisinde de mesajlaşma veritabanı dosyalarına ait kripto anahtarı "key" isimli dosya bulunmaktadır.

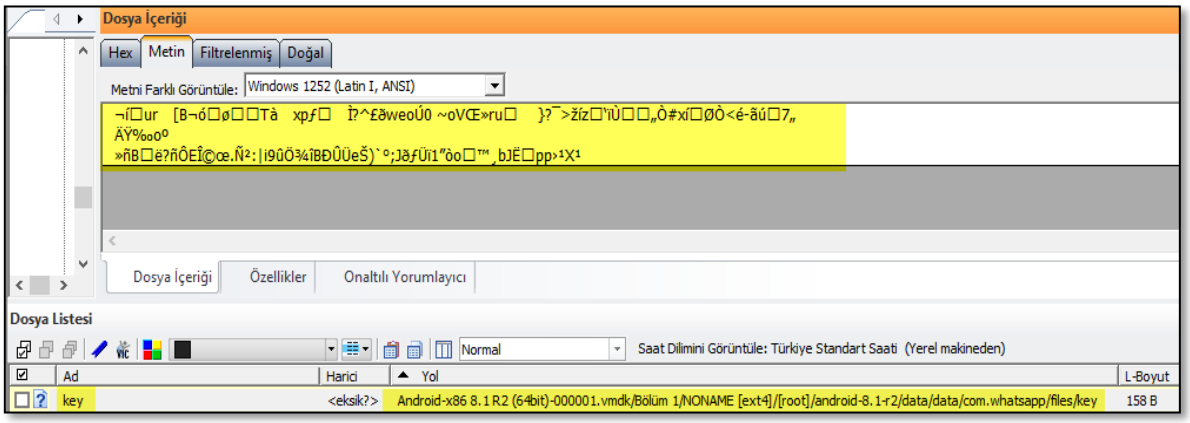


Şekil 4.8 Whatsapp' ın database klasörü içerisindeki veri tabanı dosyaları

"files" klasörü içerisinde de mesajlaşma veritabanı dosyalarına ait kripto anahtarı "key" isimli dosya bulunduğu görülmekte olup **Şekil 4.9.** da sunulmuş, "key" dosyasının yapısı ise **Şekil 4.10.** da sunulmaktadır.

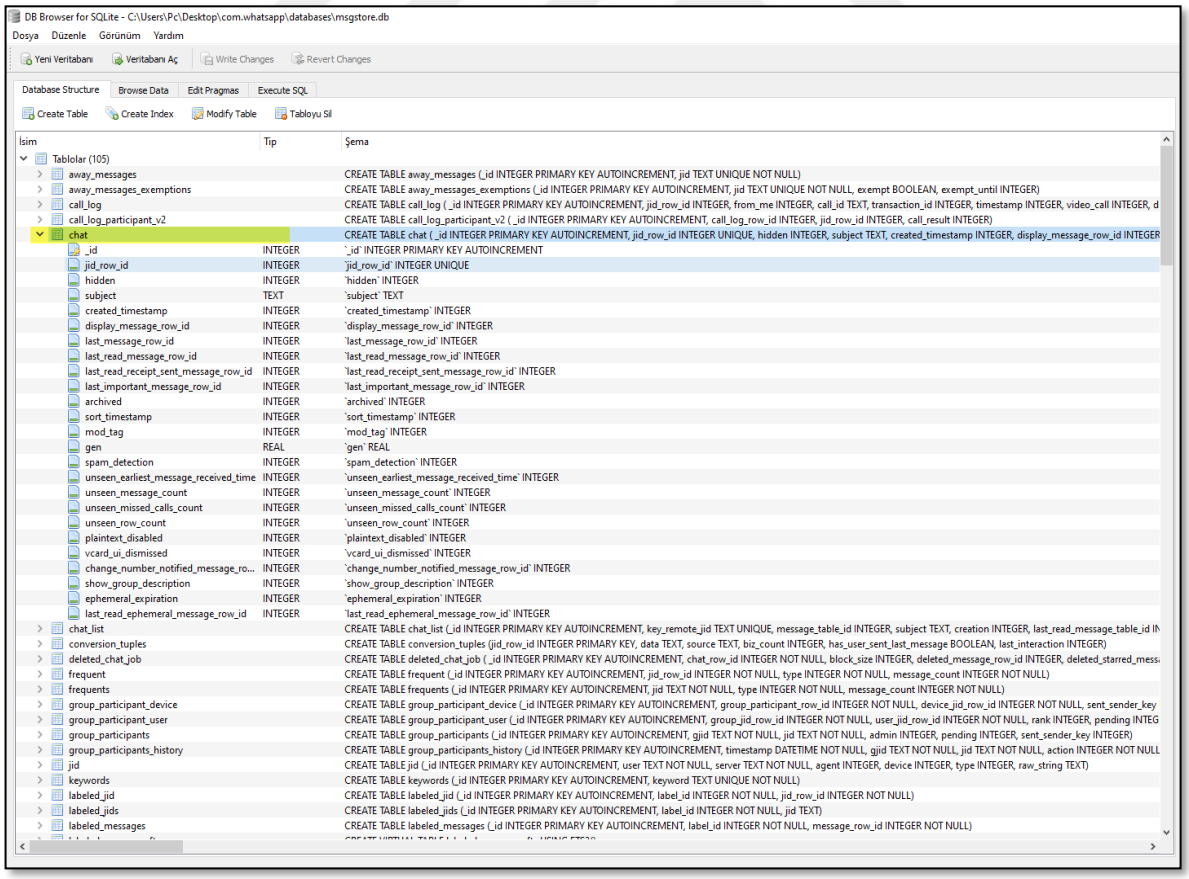


Şekil 4.9 Whatsapp' ın kripto anahtarı "key" isimli dosyası



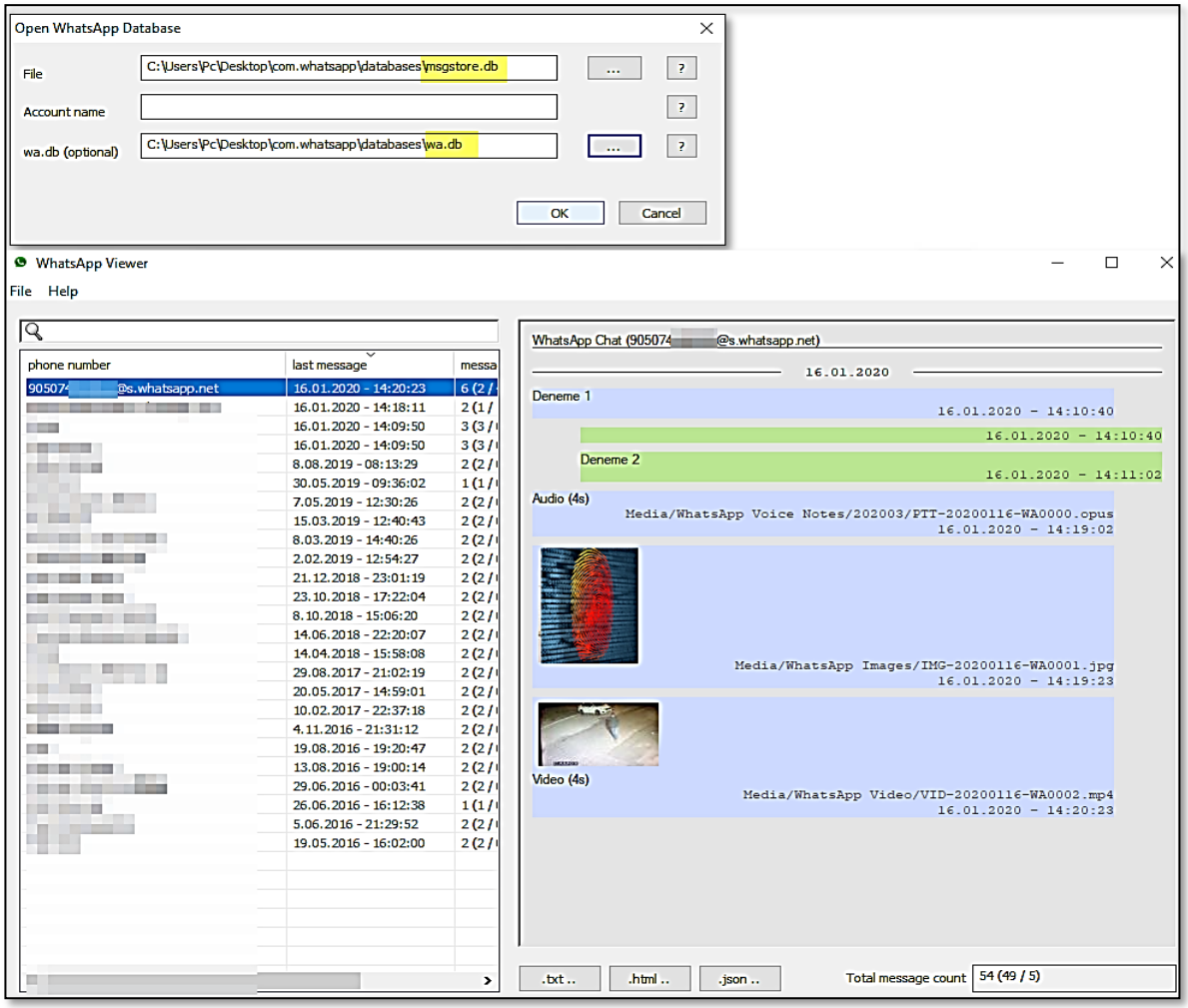
Şekil 4.10 Whatsapp' a ait "key" dosyasının yapısı

Whatsapp uygulamasına ait "msgstore.db" isimli veri tabanı dosyası DB Browser for SQlite yazılımı ile açıldığında veri tabanı dosyasının sahip olduğu yapılar görülmekte olup **Şekil 4.11.** de sunulmaktadır.



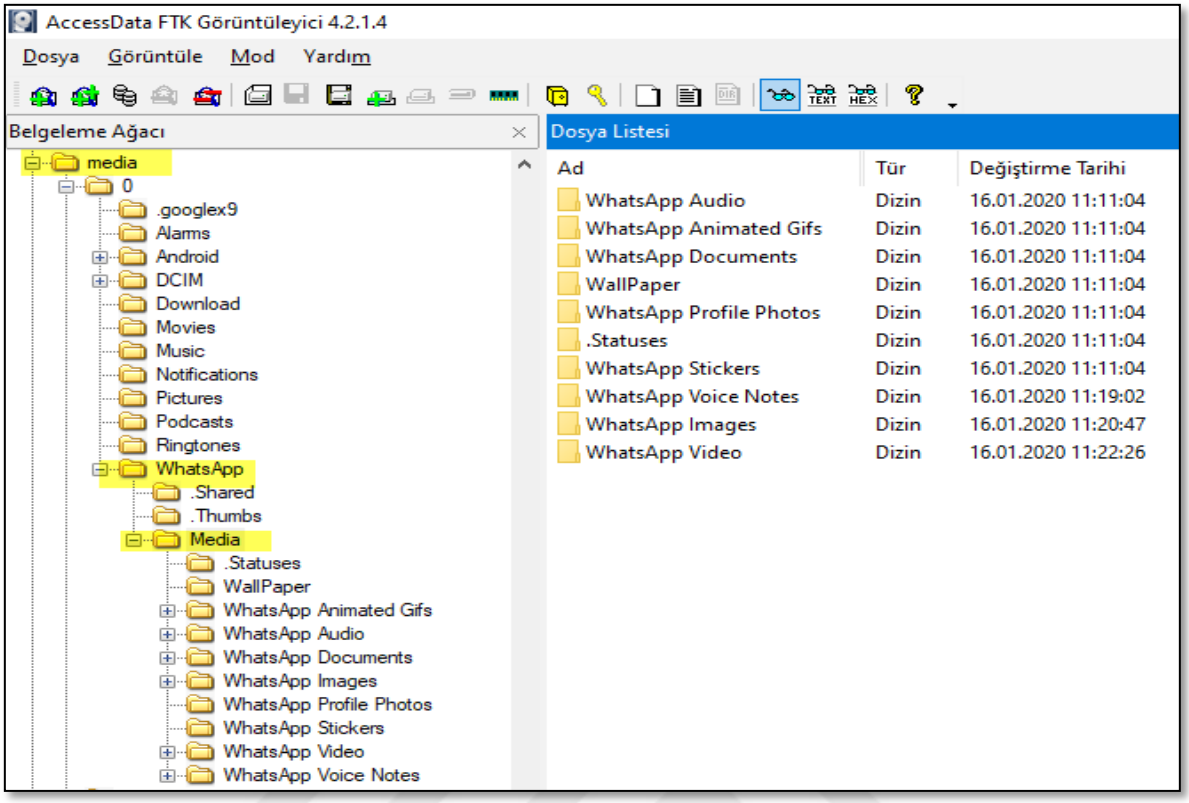
Şekil 4.11 Whatsapp'a ait "msgstore.db" veri tabanı dosyası

Elde edilen db dosyaları içerisinde yer alan chat kayıtları Github (https://github.com/andreas-mausch/whatsapp-viewer) [32] üzerinde açık kaynak kodlu olarak paylaşılan Whatsapp Viewer isimli yazılım ile açıldığında msgstore.db dosyası veritabanı dosyası içerisinde chat kayıtlarının, wa.db dosyası içerisinde bu chat kayıtlarının kontak isimlerinin tutulduğu görülmekte olup **Şekil 4.12.** de sunulmaktadır.

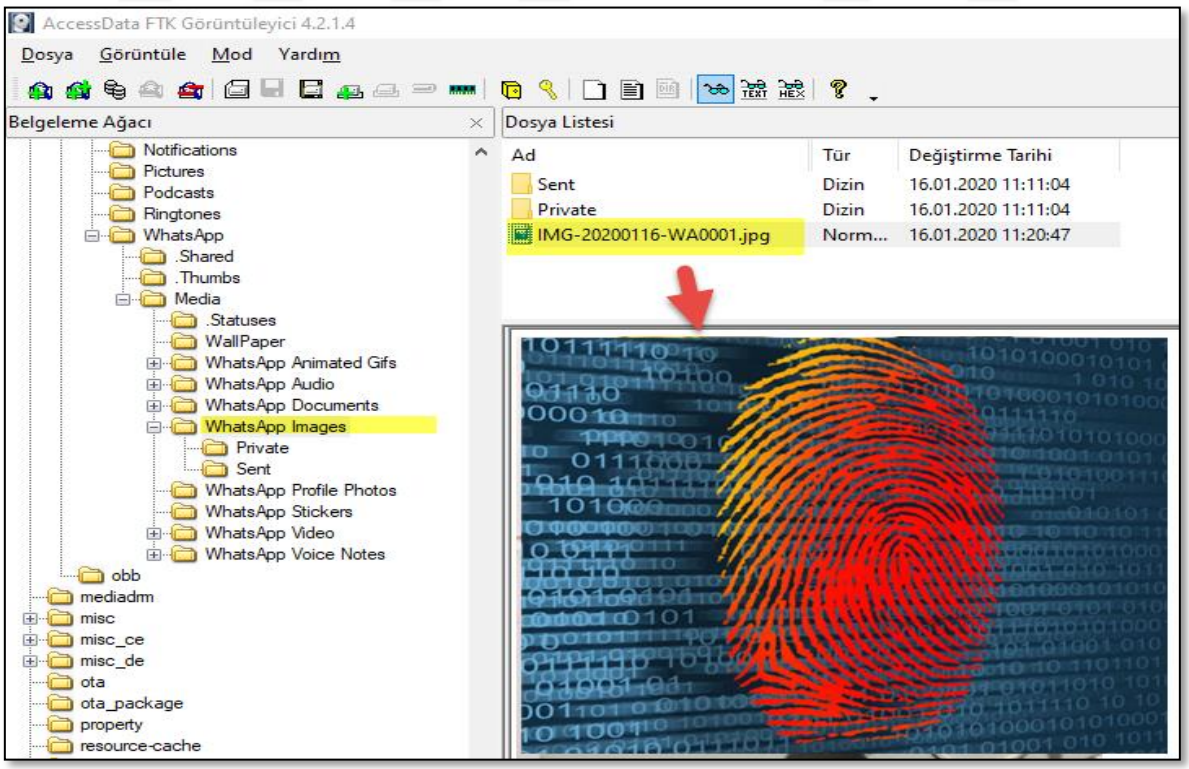


Şekil 4.12 Whatsapp Viewer ile msgstore.db dosyası ve wa.db dosyasının açılması

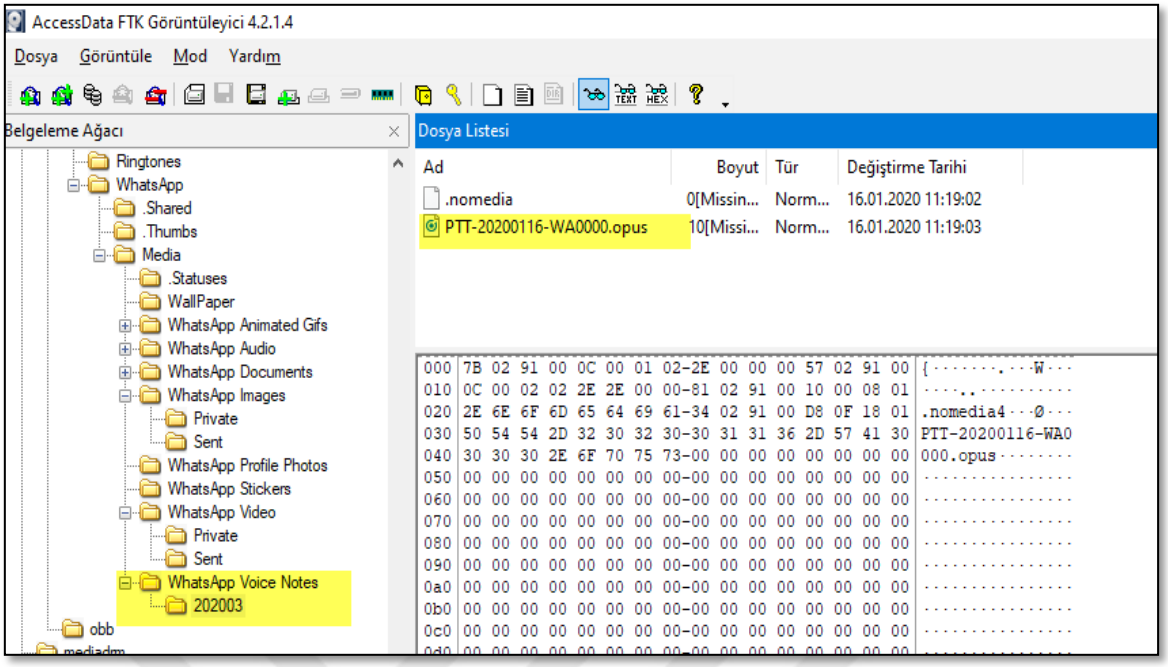
Yine uygulamanın kurulması ile Whatsapp klasöründe yer alan media dizini içerisinde sohbetlerde gönderilen medya dosyaları tutulmaktadır. Simüle edilen mesajlaşma içeriğinde gönderilen fotoğrafın WhatsApp Images klasörü içerisinde yer aldığı görülmekte olup **Şekil 4.13.** te, mobil cihaz kullanıcısı tarafından gönderilen fotoğraflar ise "sent" klasöründe yer almakta olup **Şekil 4.14** te, Gönderilen Sesli Mesajlar WhatsApp Voice Notes klasörü içerisine kaydedildiği görülmekte olup **Şekil 4.15.** te Video dosyaları ise WhatsApp Video klasörü içerisine kaydedildiği görülmekte olup Şekil **4.16.** da sunulmaktadır.



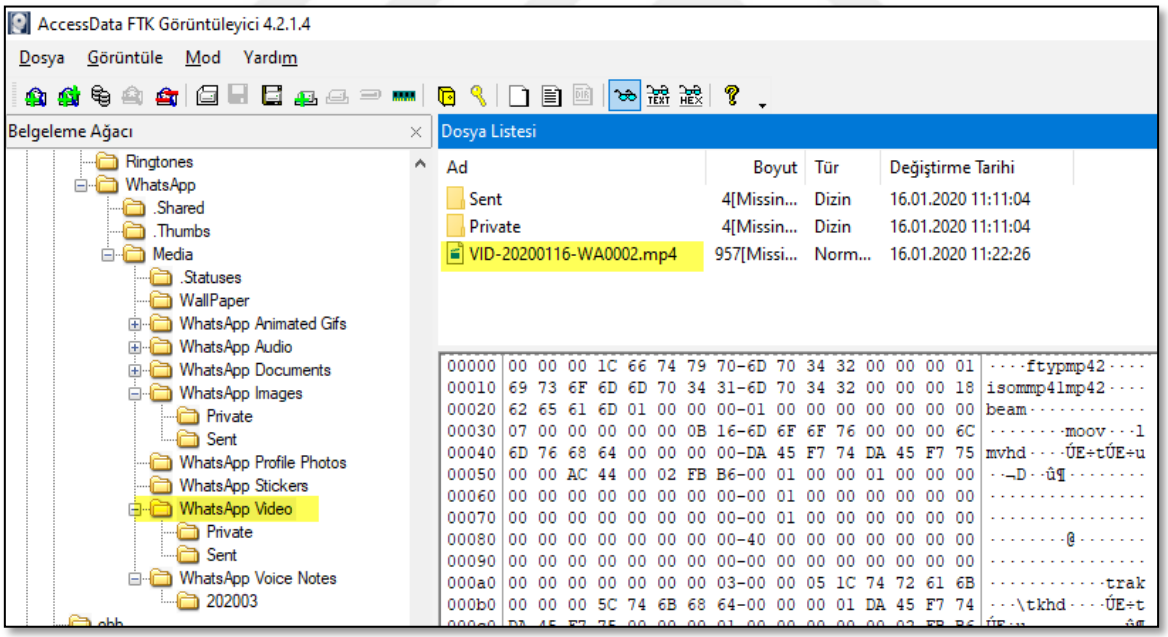
Şekil 4.13 Whatsapp klasöründe yer alan media dizini



Şekil 4.14 WhatsApp Images klasörü

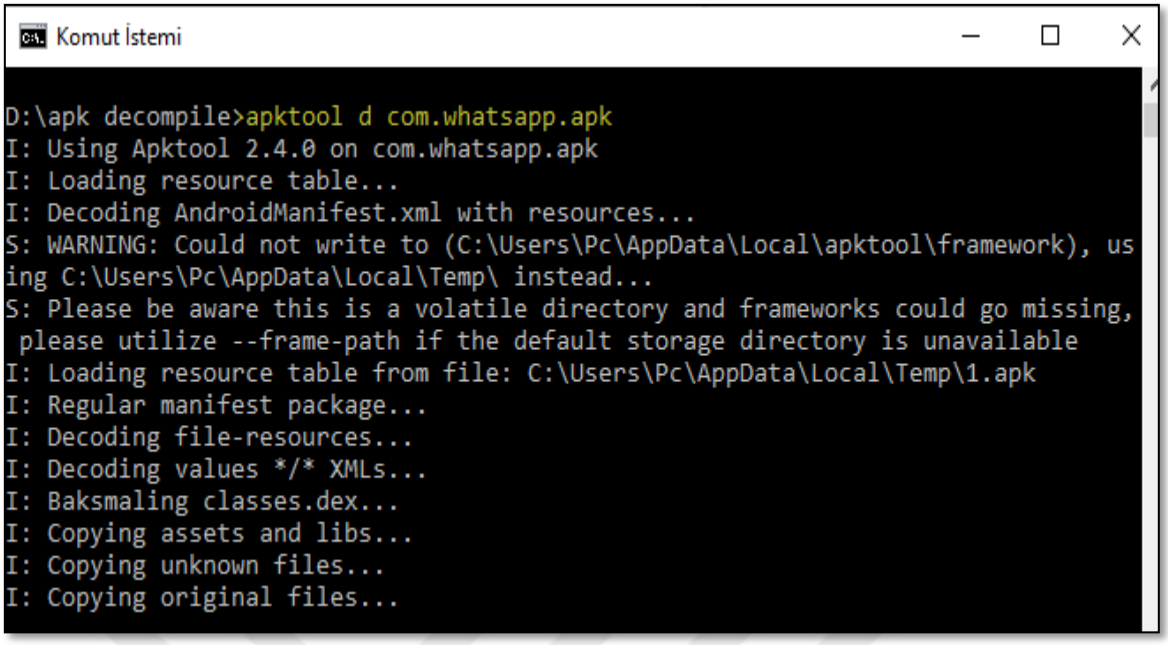


Şekil 4.15 WhatsApp Voice Notes klasörü



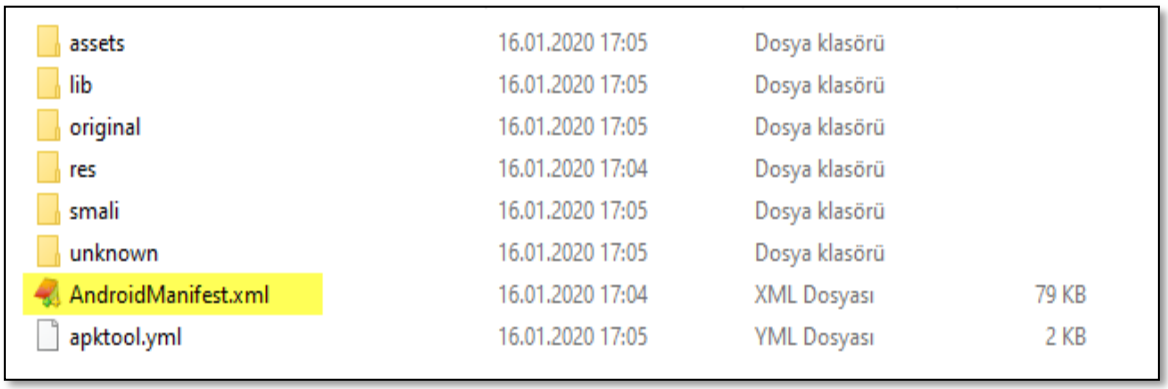
Şekil 4.16 WhatsApp Video klasörü

Whatsapp uygulaması market üzerinde yer alan son sürüm kurulum dosyası Github üzerinde (https://github.com/iBotPeaches/Apktool) [33] isimli açık kaynak kodlu yazılım ile kaynak kodları decompile edilmiş olup Şekil 4.17 de sunulmaktadır.

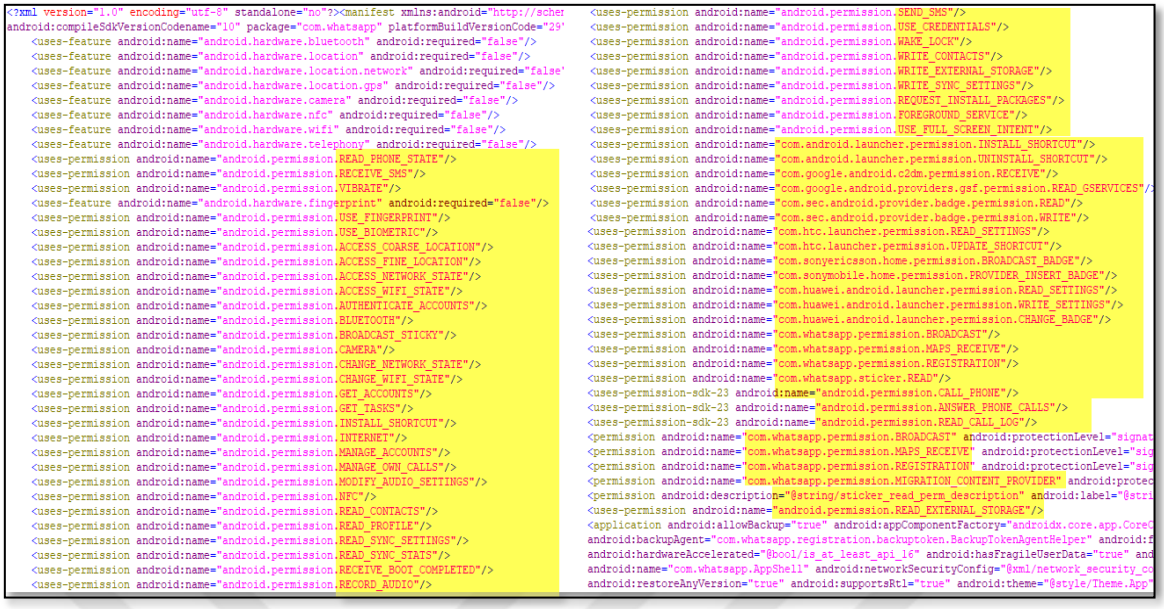


Şekil 4.17 Whatsapp'ın kaynak kodlarının decompile edilmesi.

Whatsapp uygulamasının kaynak kodları içerisinde yer alan manifest dosyası **Şekil 4.18.** de sunulmak birlikte manifest dosyası içerisinde yer alan bilgilerden whatsapp uygulamasının hangi izinleri aldığı görüntülenmiş olup **Şekil 4.19.** de sunulmuştur.



Şekil 4.18 Whatsapp'a ait AndroidManifest.xml dosyası



Şekil 4.19 Whatsapp' a ait AndroidManifest.xml dosyasının içeriği

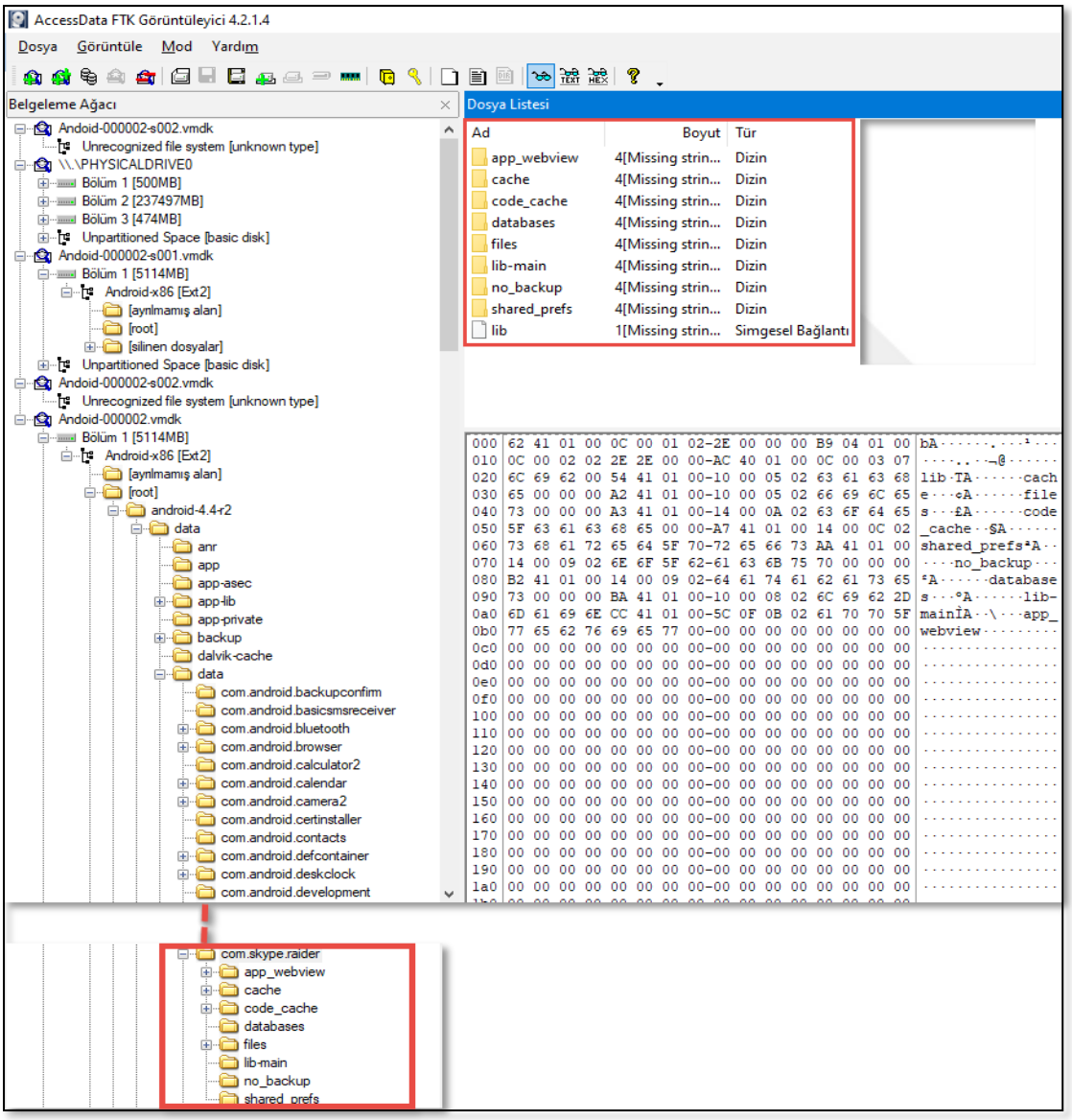
Whatsapp uygulamasına ait izinlerin ne anlama geldiklerini gösterir ekran görüntüsü **Şekil 4.20.** de sunulmaktadır.

android.permission.READ_PHONE_STATE	Telefon durumuna salt okunur erişim sağlar.
android.permission.RECEIVE_SMS	Uygulamaya SMS mesajları alma izni verir.
android.permission.VIBRATE	Vibratöre erişim sağlar.
android.permission.USE_FINGERPRINT	Uygulamaya, parmak izi donanımını kullanma izni verir.
android.permission.ACCESS_COARSE_LOCATION	Uygulamaya, yaklaşık konumlara erişme izni verir.
android.permission.ACCESS_FINE_LOCATION	Uygulamaya, kesin konuma erişme izni verir.
android.permission.ACCESS_NETWORK_STATE	Uygulamalara, ağlarla ilgili bilgilere erişme izni verir.
android.permission.ACCESS_WIFI_STATE	Uygulamalara, kablosuz ağlar hakkındaki bilgilere erişme izni verir.
android.permission.BLUETOOTH	Uygulamalara eşleştirilmiş bluetooth cihazlarına bağlanma izni verir.
android.permission.BROADCAST_STICKY	Uygulamaya, yapışkan amaçları yayınlama izni verir.
android.permission.CAMERA	Kamera cihazına erişebilmek için gereklidir.
android.permission.CHANGE_NETWORK_STATE	Uygulamalara ağ bağlantı durumunu değiştirme izni verir.
android.permission.CHANGE_WIFI_STATE	Uygulamalara, Kablosuz bağlantı durumunu değiştirme izni verir.
android.permission.GET_ACCOUNTS	Hesaplar Hizmeti'ndeki hesap listesine erişime izin verir.
android.permission.GET_TASKS	Bu sabit, API düzey 21'de kullanımdan kaldırıldı. Artık uygulanmadı.
android.permission.INTERNET	Uygulamalara ağ soketleri açma izni verir.
android.permission.MODIFY_AUDIO_SETTINGS	Uygulamaya, genel ses ayarlarını değiştirme izni verir.
android.permission.NFC	Uygulamalara, NFC üzerinden G / Ç işlemleri yapma izni verir.
android.permission.READ_CONTACTS	Uygulamaya, kullanıcının kişi verilerini okuma izni verir.
android.permission.READ_SYNC_SETTINGS	Uygulamalara, senkronizasyon ayarlarını okuma izni verir.
android.permission.READ_SYNC_STATS	Uygulamalara senkronizasyon istatistiklerini okuma izni verir.
android.permission.RECEIVE_BOOT_COMPLETED	Uygulamaya, sistem yeniden başlatmayı tamamladıktan sonra yayınlanan ACTION_BOOT_COMPLETED etkinliğini alma izni verir.
android.permission.RECORD_AUDIO	Uygulamaya ses kaydetme izni verir.
android.permission.SEND_SMS	Uygulamaya SMS mesajları gönderme izni verir.
android.permission.WAKE_LOCK	İşlemcinin uyumasını veya ekranın kararmasını önlemek için PowerManager WakeLocks kullanımına izin verir.
android.permission.WRITE_CONTACTS	Uygulamaya, kullanıcının kişi verilerini yazma izni verir.
android.permission.WRITE_EXTERNAL_STORAGE	Uygulamaya harici depolama birimine yazma izni verir.
android.permission.WRITE_SYNC_SETTINGS	Uygulamalara, senkronizasyon ayarlarını yazma izni verir.
android.permission.REQUEST_INSTALL_PACKAGES	Uygulamaya, paketlerin yüklenmesini isteme izni verir.
izinler com.android.launcher.permission.INSTALL_SHORTCUT	Uygulamaya, Başlatıcı'ya bir kısayol yükleme izni verir.
com.android.launcher.permission.UNINSTALL_SHORTCUT	Uygulamaya, Başlatıcı'daki bir kısayolu kaldırma izni verir.
android.permission.READ_EXTERNAL_STORAGE	Uygulamaya harici depolama biriminden okuma izni verir.

Şekil 4.20 Whatsapp uygulama izinlerinin anlamı

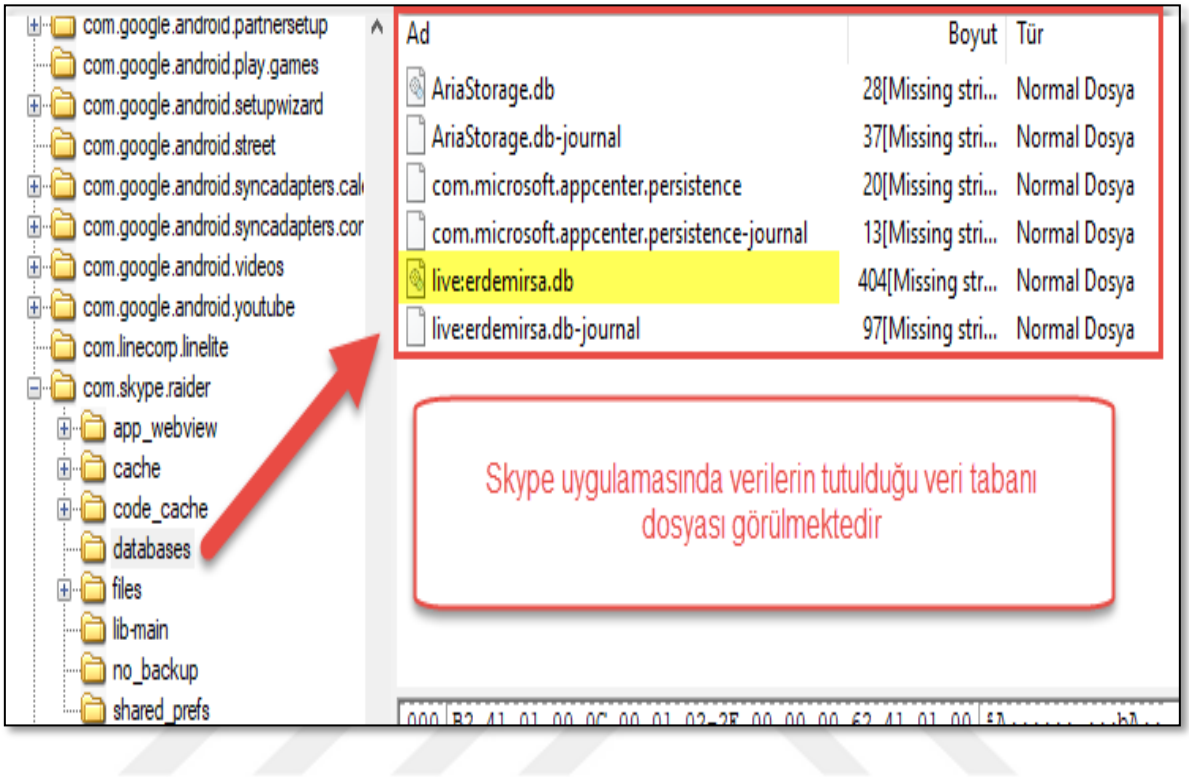
4.3.3. Skype Sohbet Uygulaması Analizi

Skype isimli sohbet uygulaması ile ilgili olarak yapılan çalışmalarda öncelikle VMware Workstation yazılımında hazırladığımız sanal android işletim sisteminde bir Google hesabı tanımlamıştır. Play Store isimli uygulama marketi üzerinden Skype isimli sohbet uygulaması indirilip yüklendikten sonra Skype uygulamasında tanımlanmış hesabın girişi yapılmıştır. Daha sonra WMware Workstation kapatılarak sanal işletim sistemine ait .vmdk dosyası Access Data FTK Imager yazılımı ile açılmıştır. Skype uygulamasının root dizini üzerindeki yeri ve içerdiği klasör yapıları **Şekil 4.21.** de görüntülenmektedir.



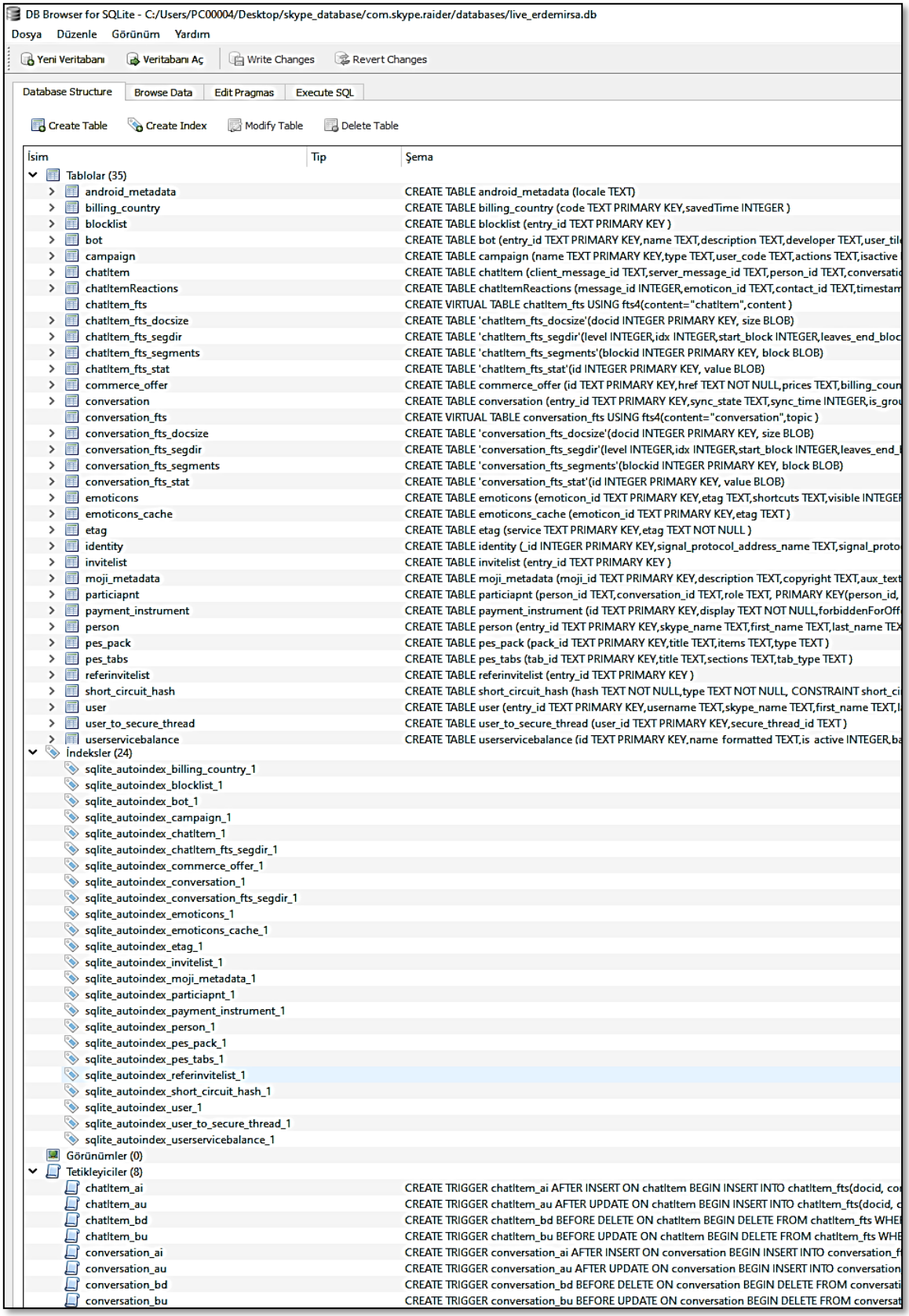
Şekil 4.21 Skype' ın root dizini üzerindeki yeri ve klasör yapıları

Skype uygulamasına ait “database” klasörü içerisinde veri tabanı dosyalarının tutulduğu görülmekte olup **Şekil 4.22.** de sunulmaktadır.



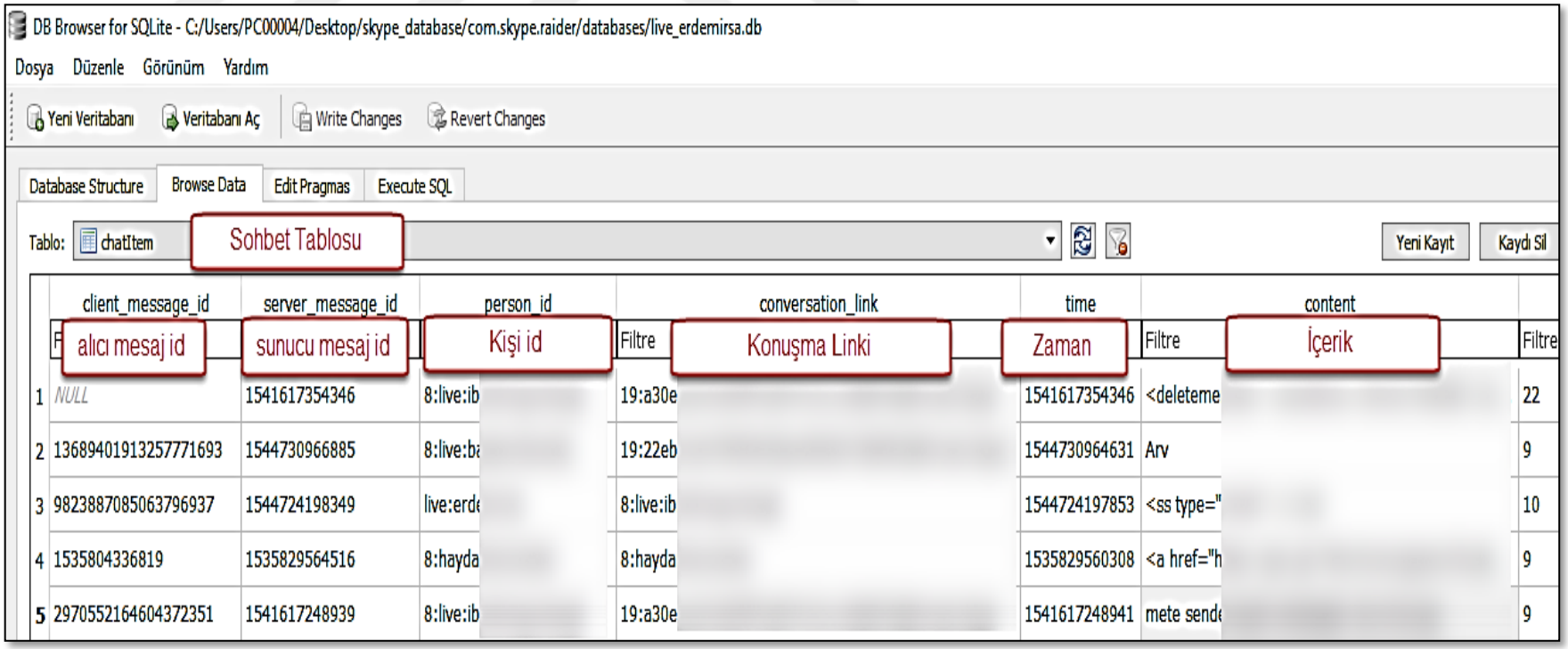
Şekil 4.22 Skype’ a ait veri tabanı dosyası

DB Browser for SQlite yazılımı üzerinde Skype uygulamasına ait “live_erdemirsa.db” isimli veri tabanı dosyasının barındırdığı yapılar görüntülenmekte olup **Şekil 4.23.** te sunulmaktadır.



Şekil 4.23 Skype'a ait veri tabanı dosyasının içerdiği yapılar

Skype uygulamasına ait “live_erdemirsa.db” isimli veri tabanı dosyasına bakıldığında “chatitem” isimli sohbet tablosunda Alıcı Mesaj ID, Sunucu Mesaj ID, Kişi ID, Konuşma Linki, Zaman ve İçerik gibi bilgilerin yer aldığı görülmekte olup **Şekil 4.24.** te sunulmaktadır.

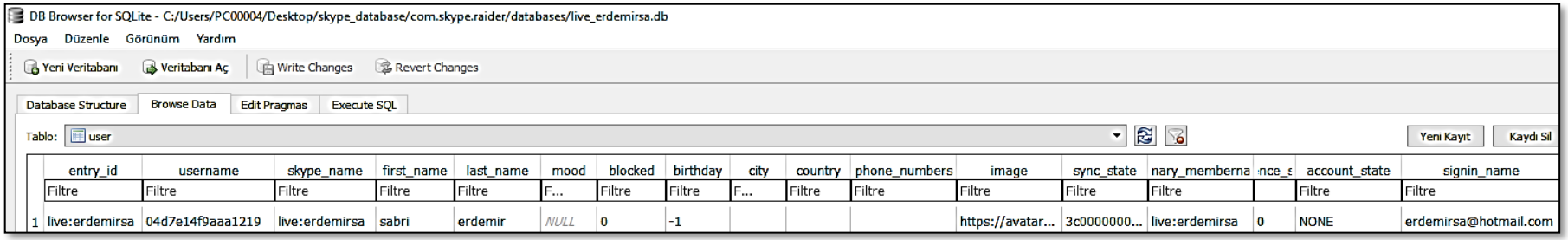


Şekil 4.24 Skype’a ait veri tabanı dosyasında sohbet tablosu

Skype uygulamasına ait “live_erdemirsa.db” isimli veri tabanı dosyasına bakıldığında “emoticons_cache” isimli tabloda kullanılan ifadelere dair bilgilerin yer aldığı görülmekte olup **Şekil 4.25.** te sunulmaktadır.

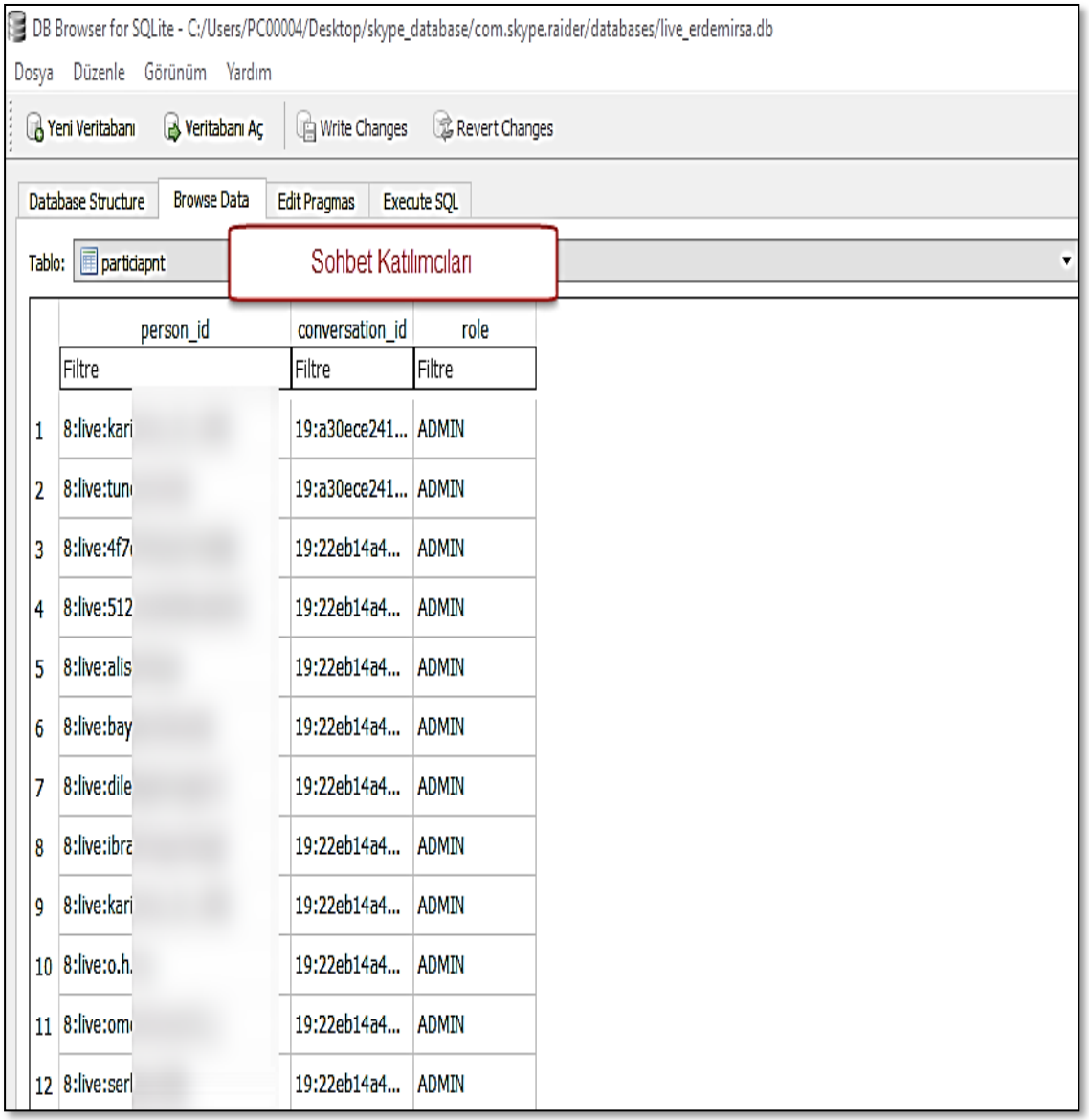
Şekil 4.25 Skype’ a ait veri tabanı dosyasında kullanılan ifadeler tablosu

Skype uygulamasına ait “live_erdemirsa.db” isimli veri tabanı dosyasına bakıldığında “user” isimli tabloda Skype adı, kullanıcı adı ve soyadı, giriş adı gibi bilgilerin yer aldığı görülmekte olup **Şekil 4.26.** te sunulmaktadır.



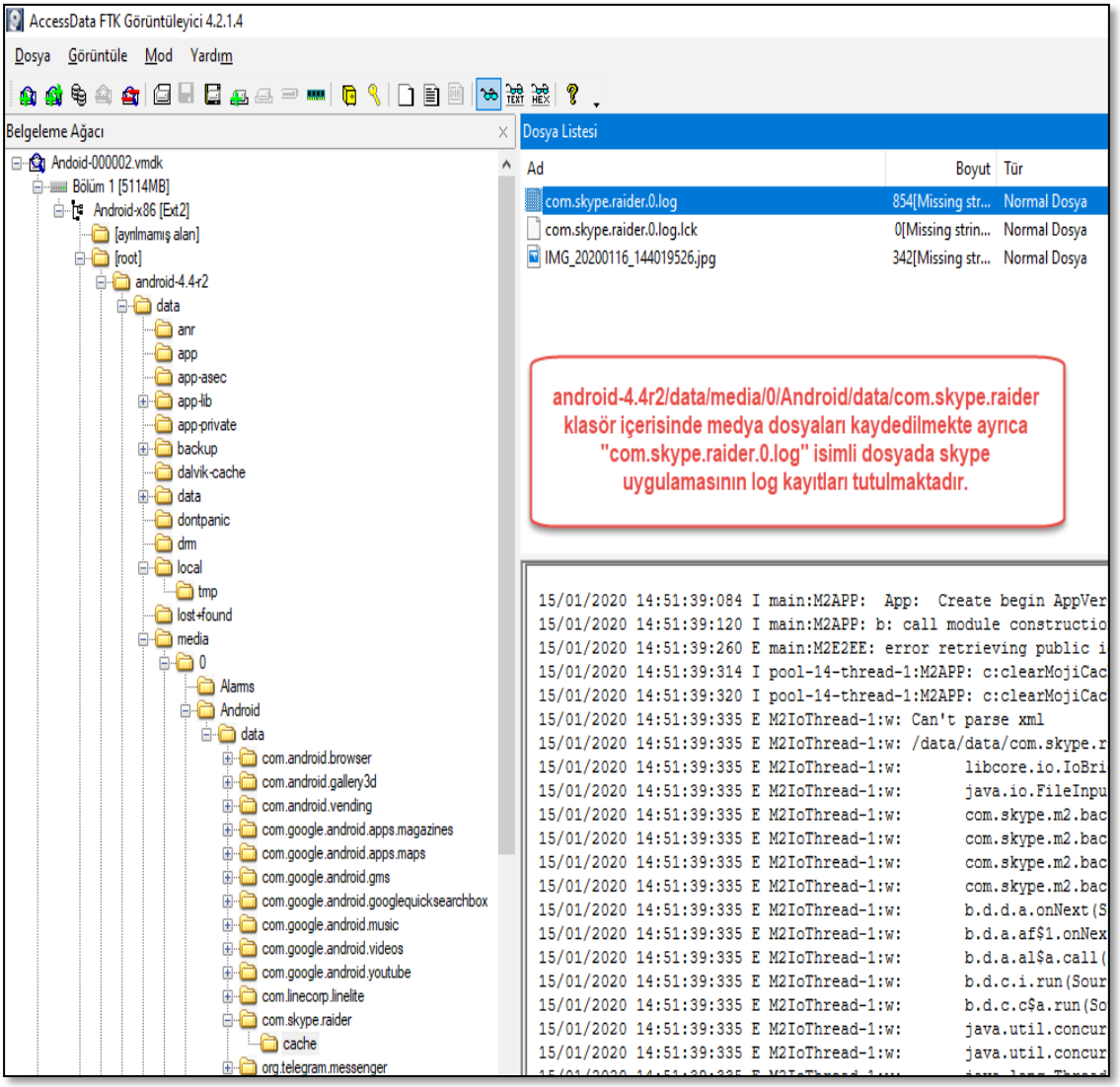
Şekil 4.26 Skype’ a ait veri tabanı dosyasında kullanıcı bilgileri tablosu

Skype uygulamasına ait “live_erdemirsa.db” isimli veri tabanı dosyasına bakıldığında “particiapnt” isimli tabloda sohbet katılımcıları bilgilerinin yer aldığı görülmekte olup **Şekil 4.27.** te sunulmaktadır.

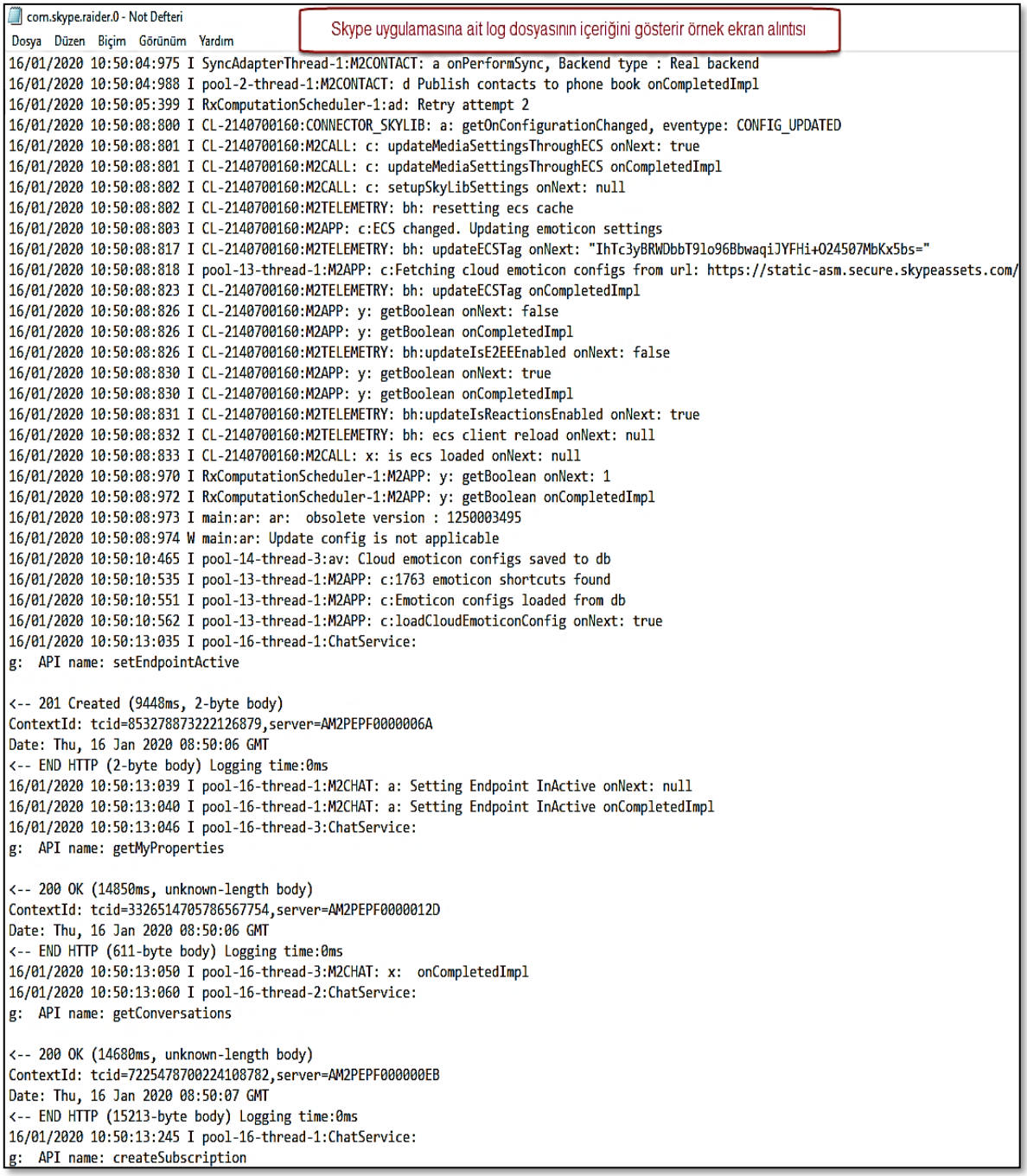


Şekil 4.27 Skype’ a ait veri tabanı dosyasında sohbet katılımcıları tablosu

Skype uygulamasına ait “com.skype.raider” klasörü içerisinde medya dosyalarının kaydedildiği ve uygulamaya ait log kayıt dosyasının da bu klasör içerisinde bulunduğu görülmekte olup **Şekil 4.28** de sunulmakla birlikte log kayıt dosyasının içeriği **Şekil 4.29.** da sunulmaktadır.



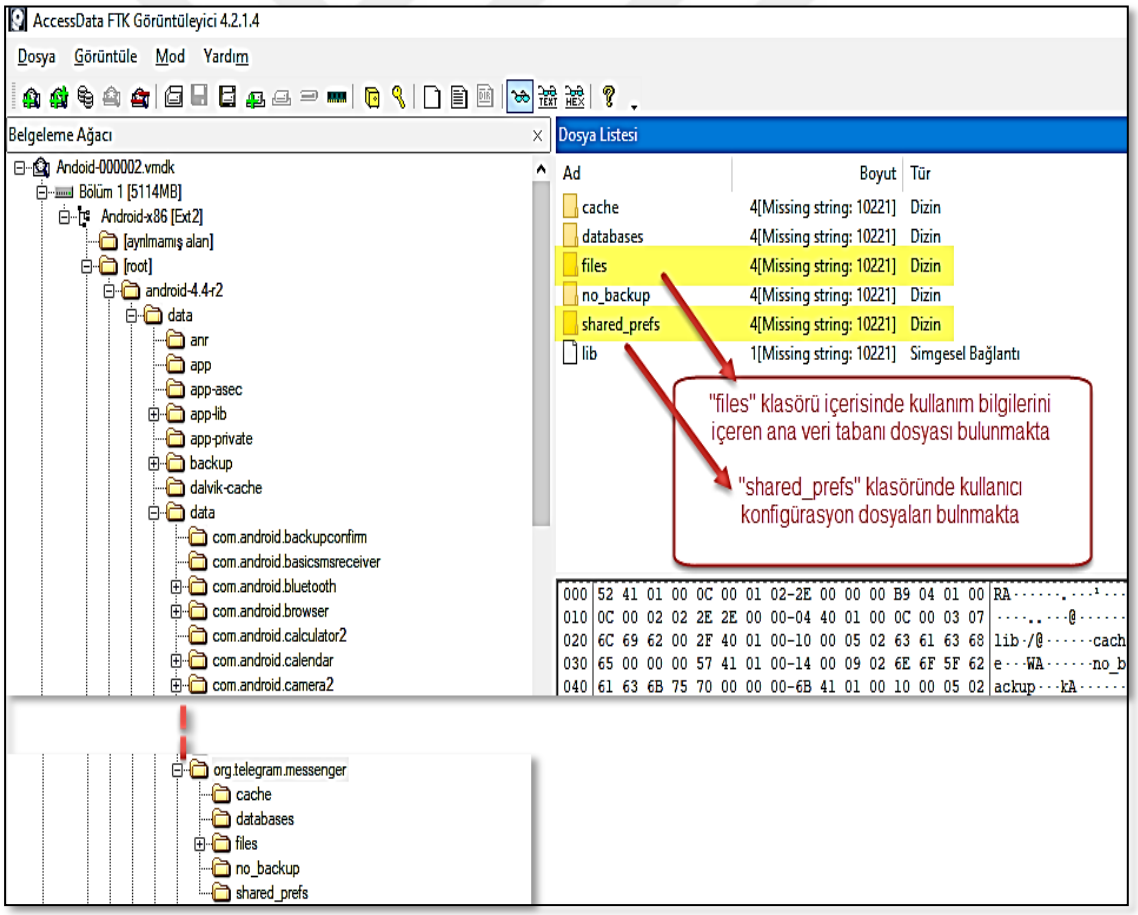
Şekil 4.28 Skype’ ta Log kayıt dosyası ile medya dosyaların kaydedildiği klasör



Şekil 4.29 Skype' ait ait log kayıt dosyasının içeriği

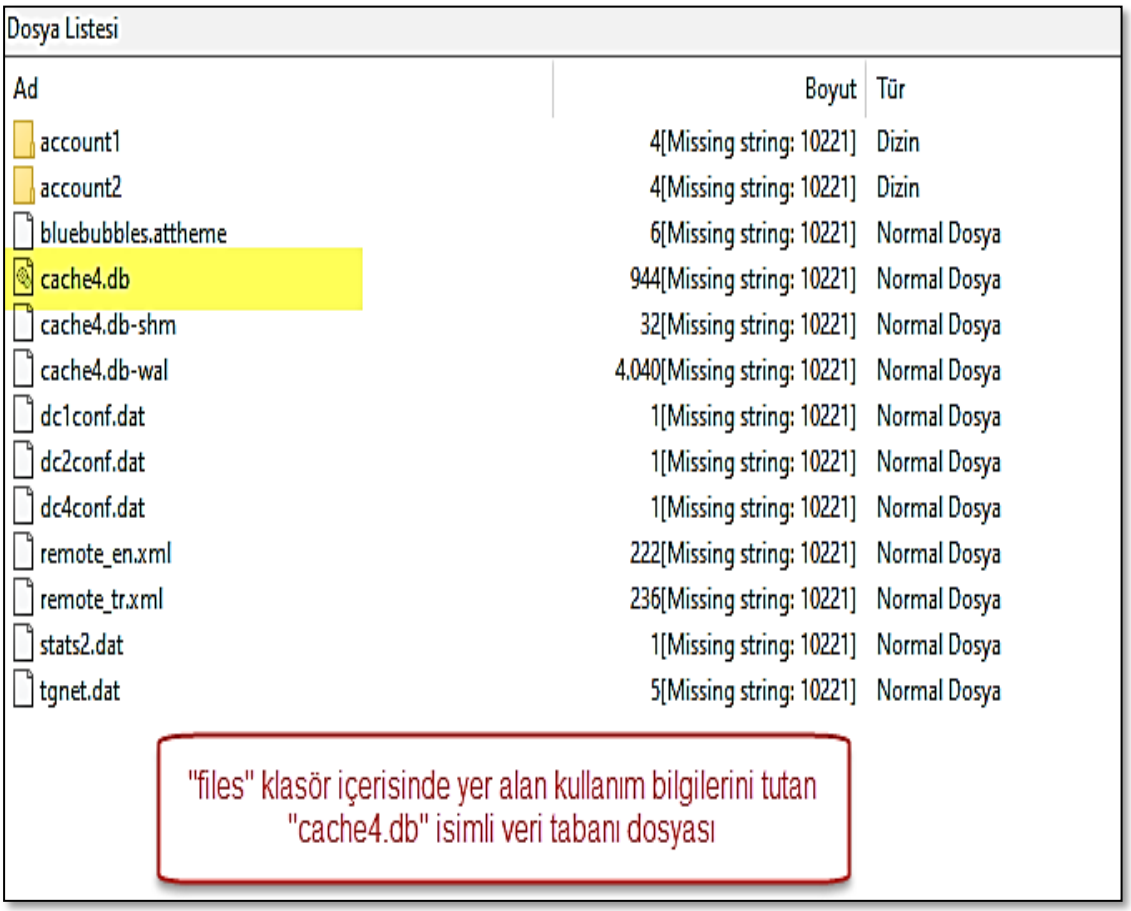
4.3.4. Telegram Sohbet Uygulaması Analizi

Telegram isimli sohbet uygulaması ile ilgili olarak yapılan çalışmalarda öncelikle VMware Workstation yazılımında hazırladığımız sanal android işletim sisteminde bir Google hesabı tanımlamıştır. Play Store isimli uygulama marketi üzerinden Telegram isimli sohbet uygulaması indirilip yüklendikten sonra Telegram uygulamasında daha önceden tanımlanmış olan cep telefonu numarasının girişi yapılmıştır. Daha sonra WMware Workstation kapatılarak sanal işletim sistemine ait .vmdk dosyası Access Data FTK Imager yazılımı ile açılmış, "Android-4.4r2/data/data/org.telegram.messenger/" veri yolunda veri tabanı dosyalarını içerir "files" klasörü ile kullanıcı konfigürasyon dosyalarını içeren "shared_prefs" klasörünün yer aldığı **Şekil 4.30**. da gösterilmektedir. Telegram uygulamasının analizinde Cosimo Anglano, Massimo Canonico, Marco Guazzone tarafından ele alınan Forensic analysis of Telegram Messenger on Android smartphones isimli makaleden faydalanılmıştır [34].



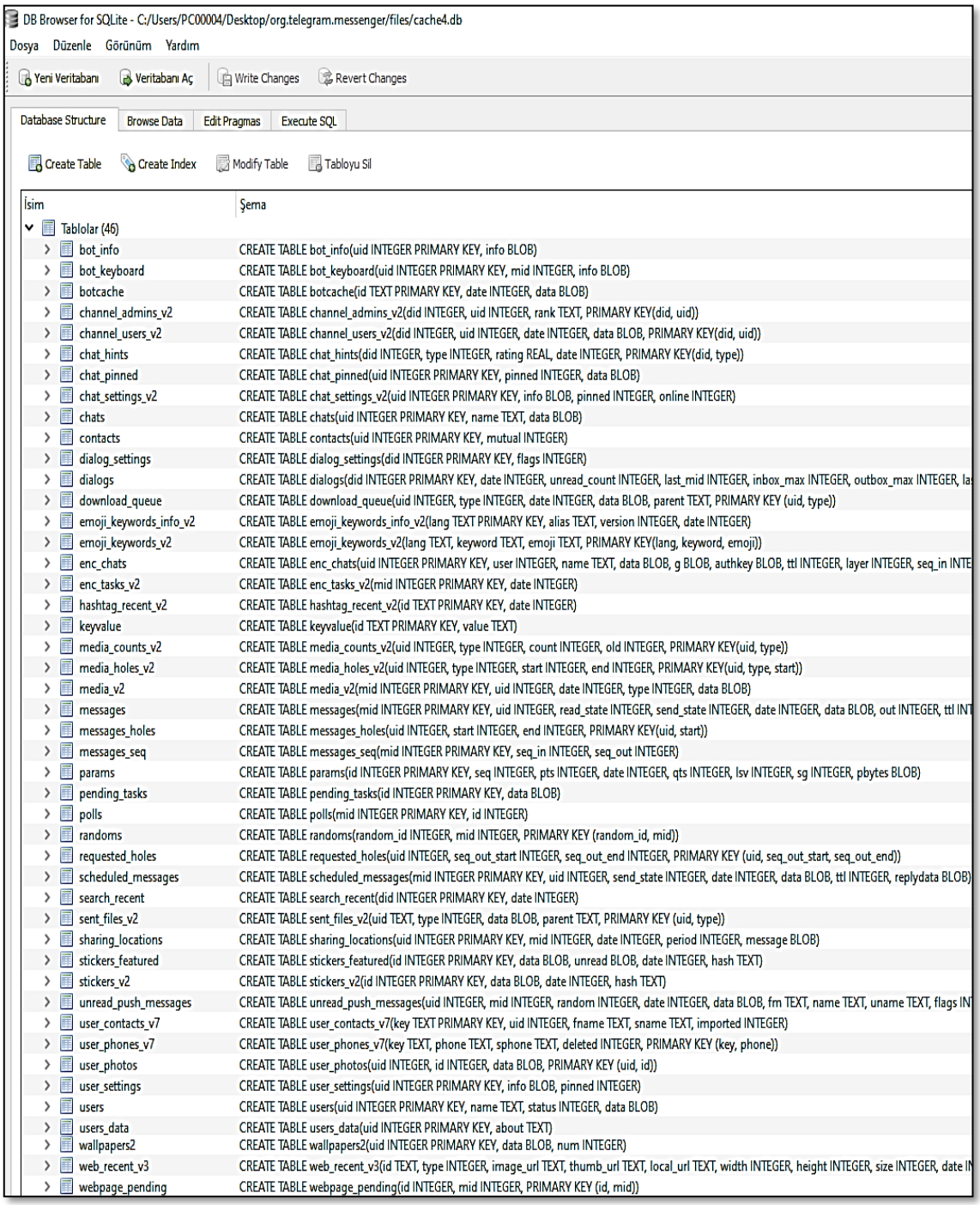
Şekil 4.30 Telegram' a ait root dizini üzerindeki klasör içerikleri

“Android-4.4r2/data/data/org.telegram.messenger/” veri yolunda yer alan “files” klasörü içerisinde kullanım bilgilerini tutan “cache4.db” isimli ana veri tabanı dosyası bulunmaktadır. “files” klasör içeriği Şekil 4.31 de gösterilmektedir.



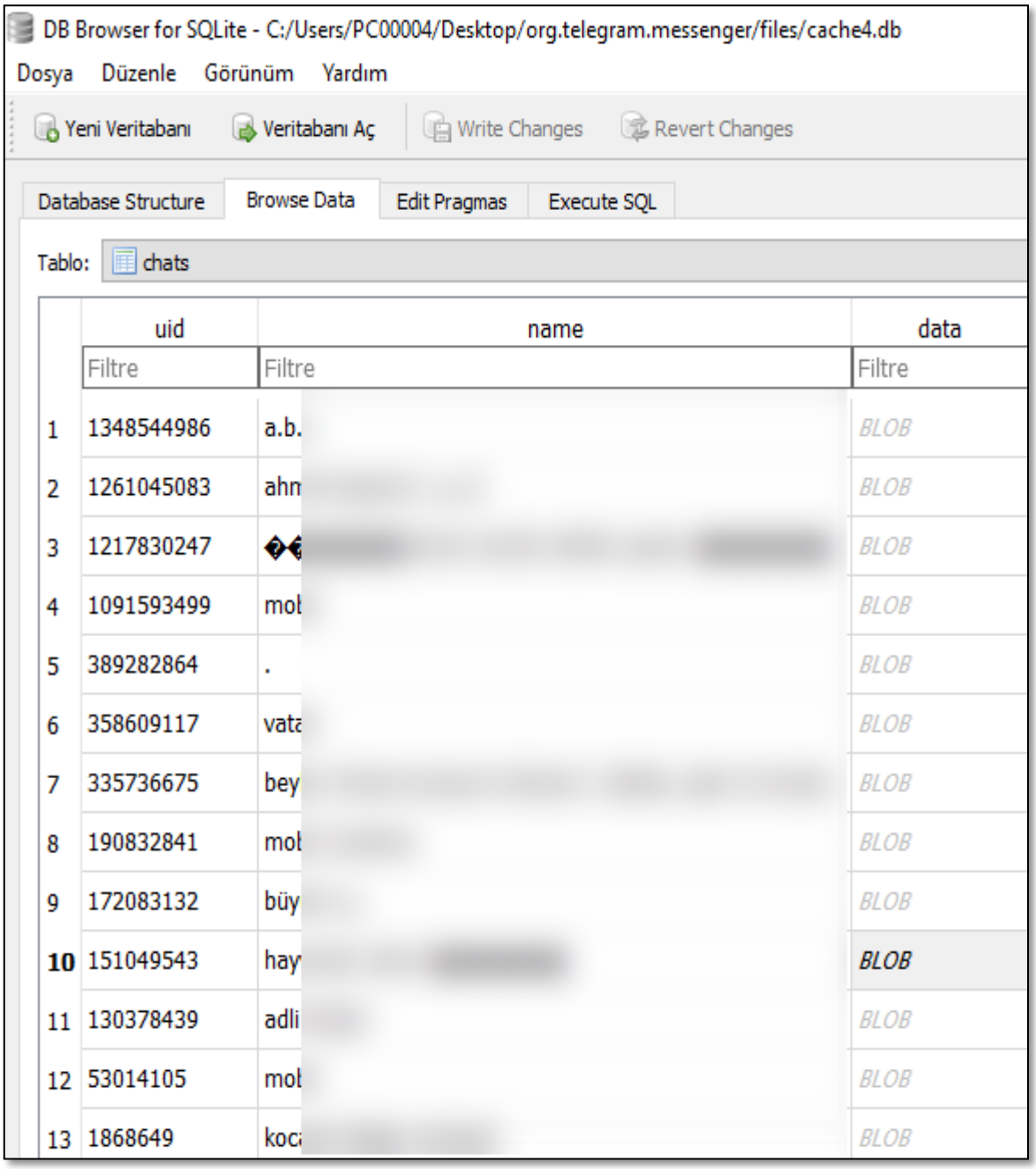
Şekil 4.31 Telegram’ a ait “files” klasör içeriği

"cache4.db" isimli veri tabanı dosyasının kullanıcı, rehberde kayıtlı kullanıcılar, sohbetler, mesajlaşma içerikleri, gizli mesajlaşma içerikleri gibi yapıları barındırdığı görülmüş olup içerik **Şekil 4.32.** de gösterilmektedir.



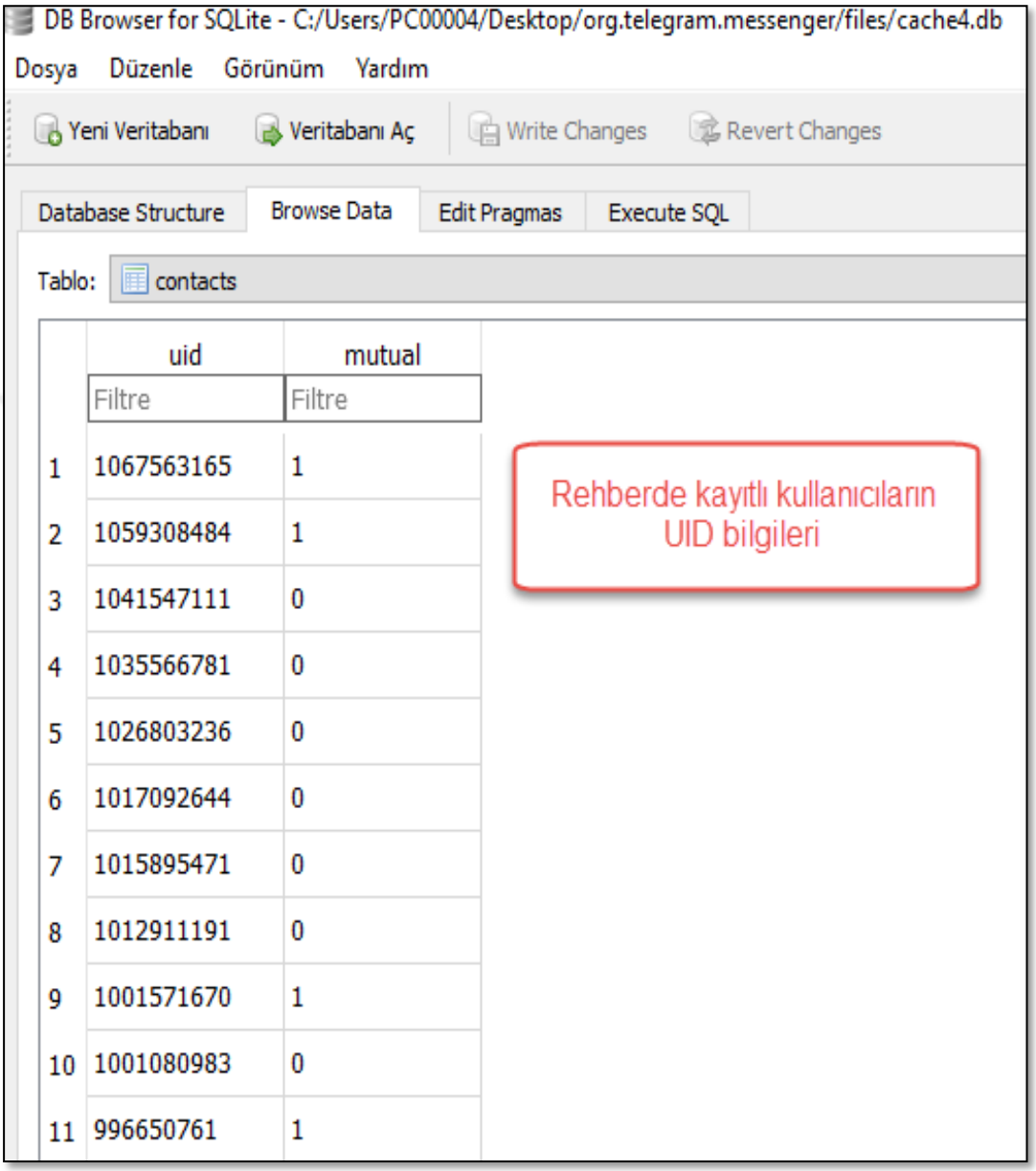
Şekil 4.32 Telegram' a ait veri tabanı dosyasının barındırdığı yapılar

"cache4.db" veri tabanında "chats" sütununda telegram üzerinden yapılan aramaların tutulduğu görülmüştür. "chats" tablosu içeriği **Şekil 4.33.** te gösterilmektedir.



Şekil 4.33 Telegram' ait veri tabanı dosyasında chats tablosu

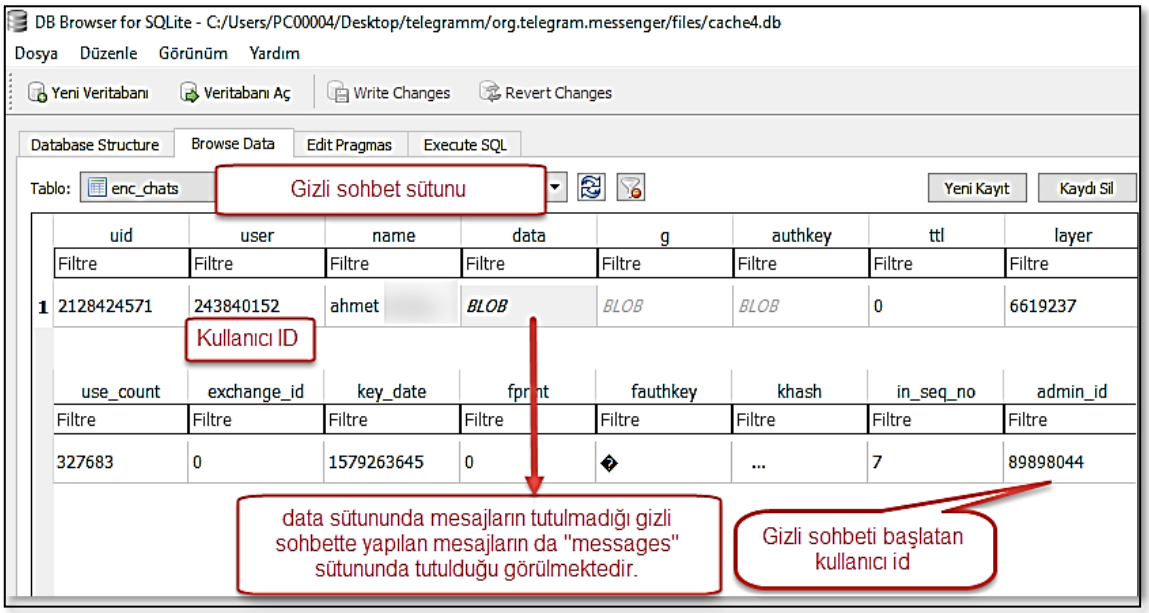
"cache4.db" veri tabanında "contacts" sütununda rehberde kayıtlı kullanıcıların UID bilgilerinin tutulduğu görülmüştür. "contacts" tablosu içeriği **Şekil 4.34.** te gösterilmektedir.



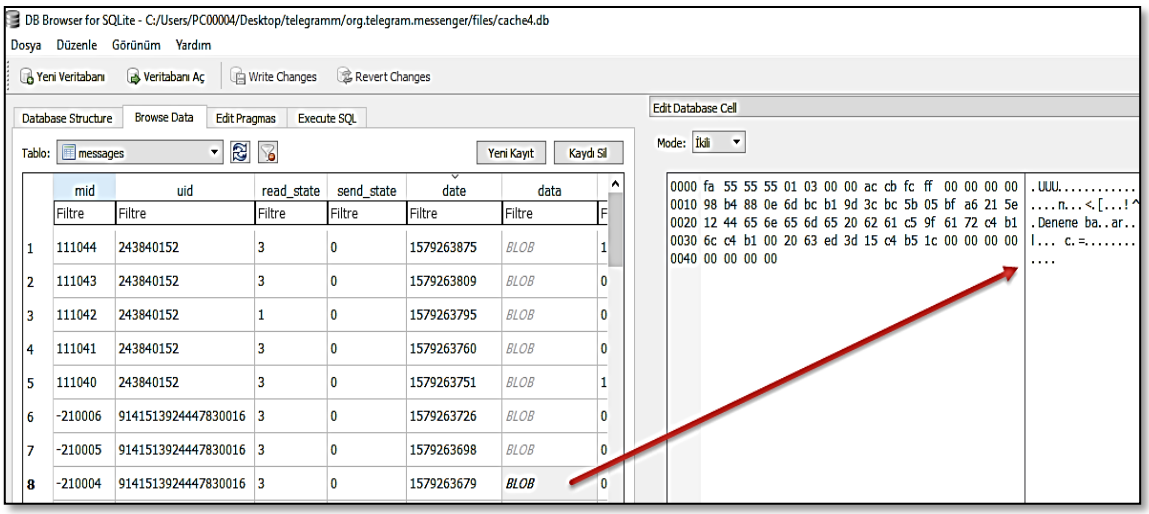
Şekil 4.34 Telegram' a ait veri tabanı dosyasında contacts tablosu

Telegram uygulamasına ait “cache4.db” isimli veri tabanı dosyasında “enc_chats” tablosunda gizli sohbet kayıtlarının tutulduğu görülmektedir. “enc_chats” tablosu içeriği **Şekil 4.35** te gösterilmektedir.

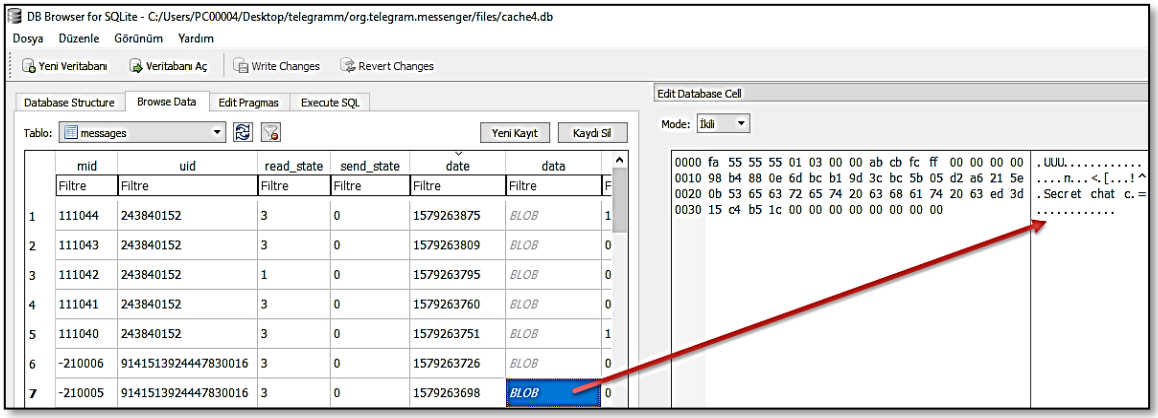
243840152 kullanıcı ID ile gerçekleştirilen Gizli Sohbet içeriğinde yapılan yazışma içerikleri “Messages” sütununda BLOB veri olarak tutulduğu görülmekte olup deneme çalışmasında gerçekleştirilen “Deneme 1” ve “Secret Chat” kelimeleri kullanılarak yapılan yazışmalar ile ilgili tespitler **Şekil 4.36.** ve **Şekil 4.37** de sunulmaktadır.



Şekil 4.35. Telegram’a ait veri tabanı dosyasında enc_chats tablosu

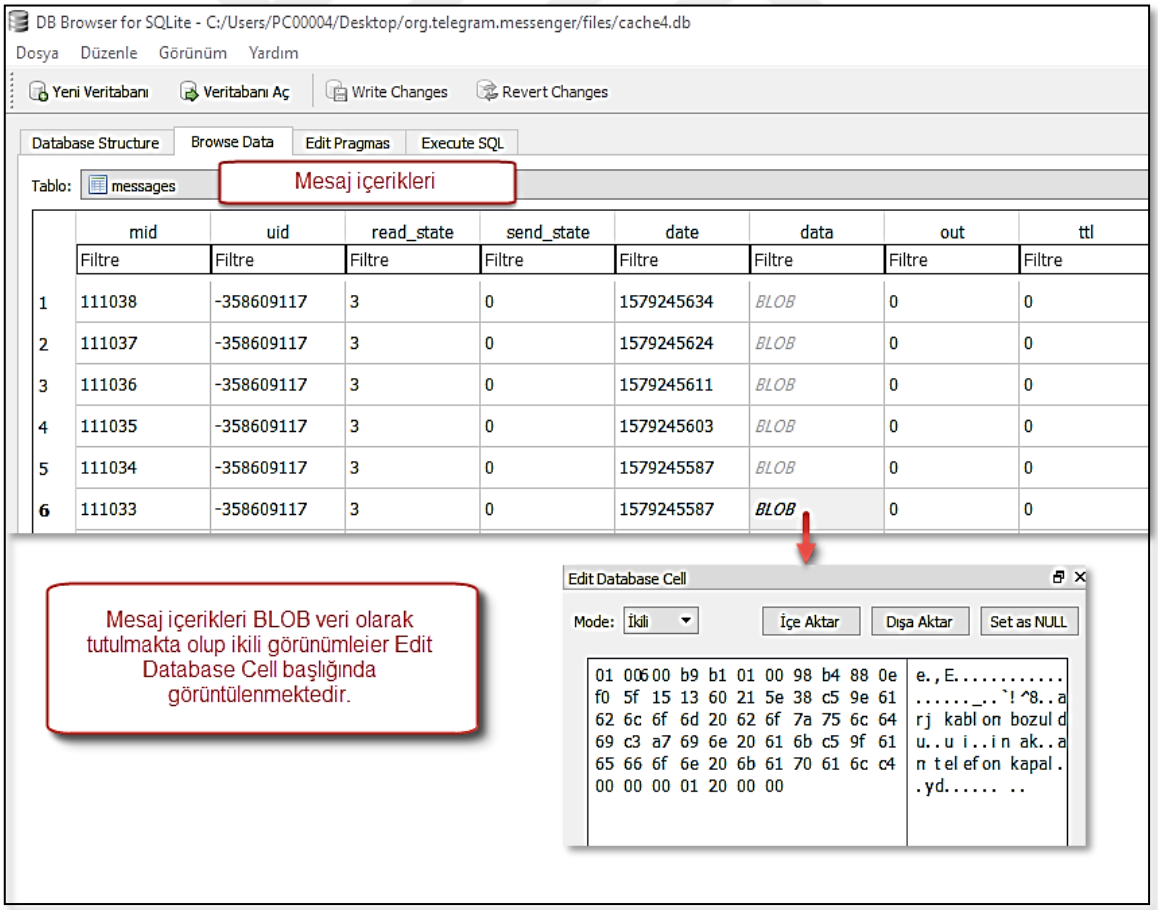


Şekil 4.36 Telegram’ da gizli sohbet içeriklerinin “Messages” tablosunda tutulması



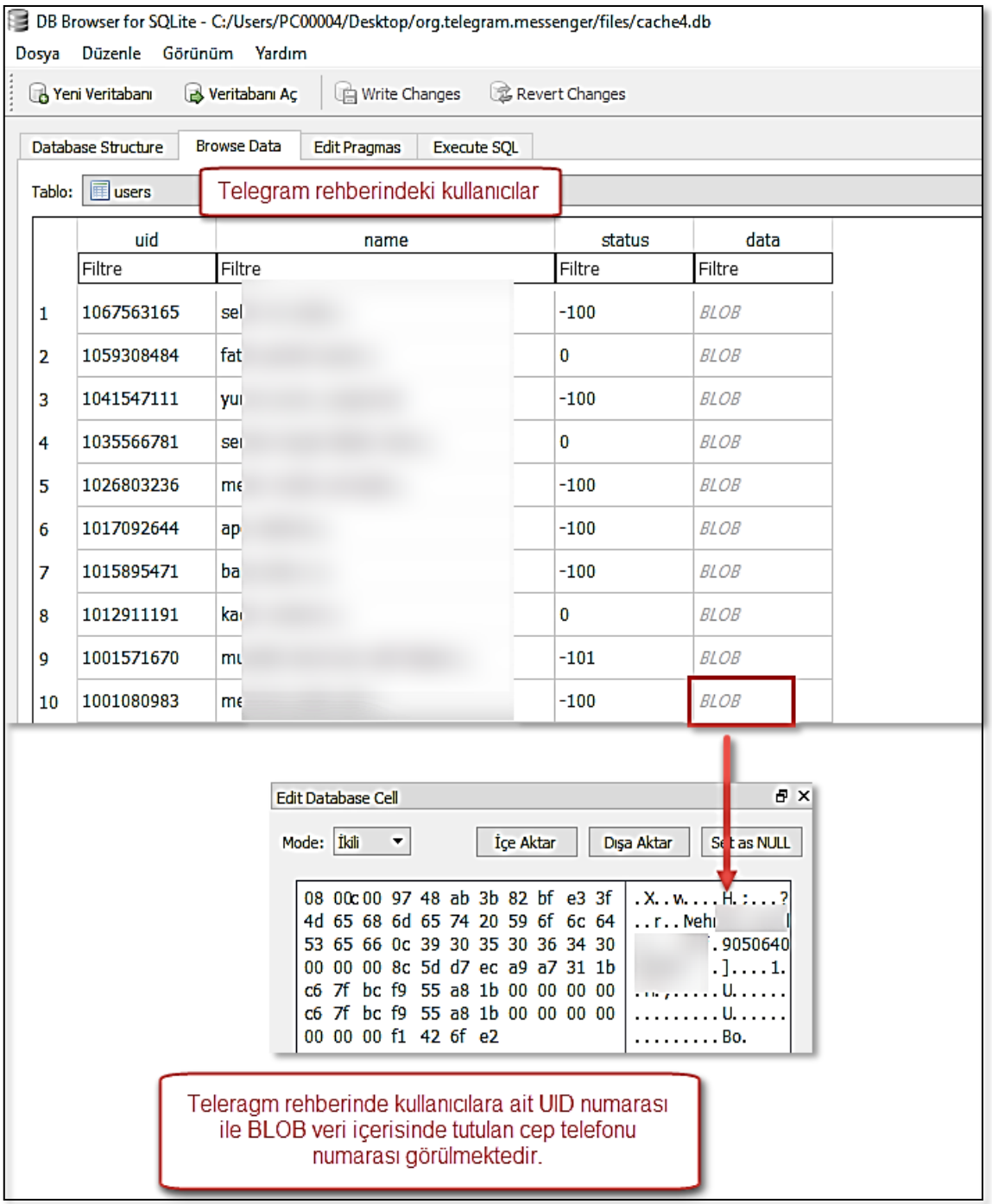
Şekil 4.37 Telegram' da gerçekleştirilen örnek gizli sohbet içeriği

Telegram uygulamasına ait "cache4.db" isimli veri tabanı dosyasında "messages" tablosunda mesaj içeriklerinin tutulduğu görülmektedir. "messages" tablosu içeriği **Şekil 4.38** te gösterilmektedir.



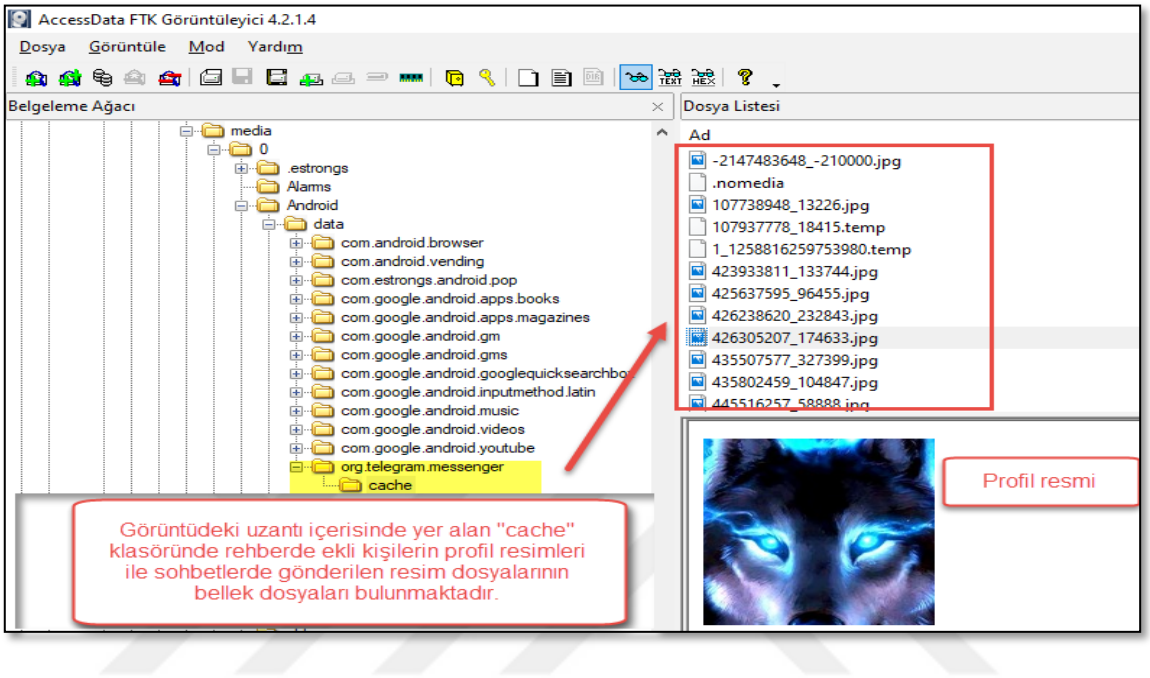
Şekil 4.38 Telegram' a ait veri tabanı dosyasında "messages" tablosu

Telegram uygulamasına ait “cache4.db” isimli veri tabanı dosyasında “users” tablosunda telegram rehberinde kayıtlı kullanıcı bilgilerinin tutulduğu görülmektedir. “users” tablosu içeriği **Şekil 4.39** da gösterilmektedir.



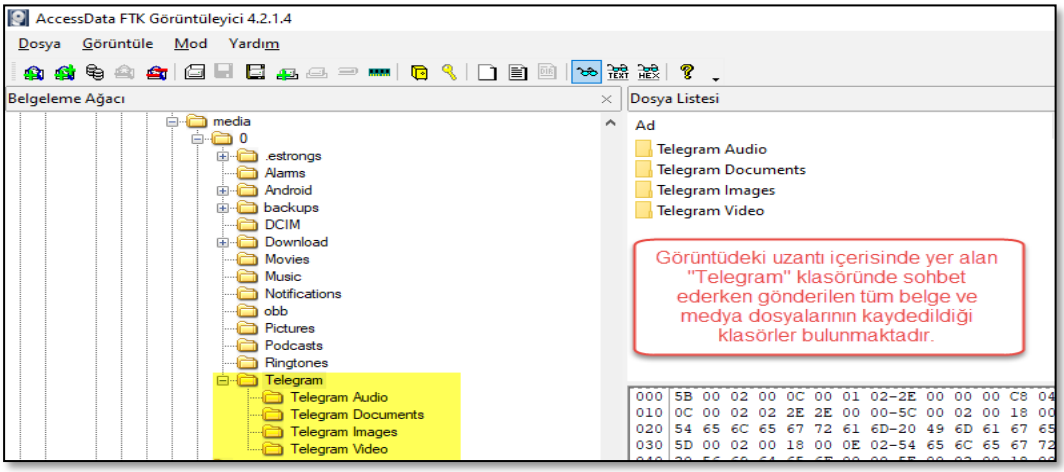
Şekil 4.39 Telegram’ a ait veri tabanı dosyasında “users” tablosu

Telegram uygulamasına ait “root/ android-4.4-r2/ data/ media/ 0/ Android/ data/ org.telegram.messanger” uzantılı klasör yolundaki “cache” isimli klasör içerisinde telegram rehberinde ekli kişilerin profil resimleri ile sohbetlerde gönderilen resim dosyalarının birer cache (bellek) halleri bulunmaktadır. “cache” klasör içeriği **Şekil 4.40**. ta gösterilmektedir.



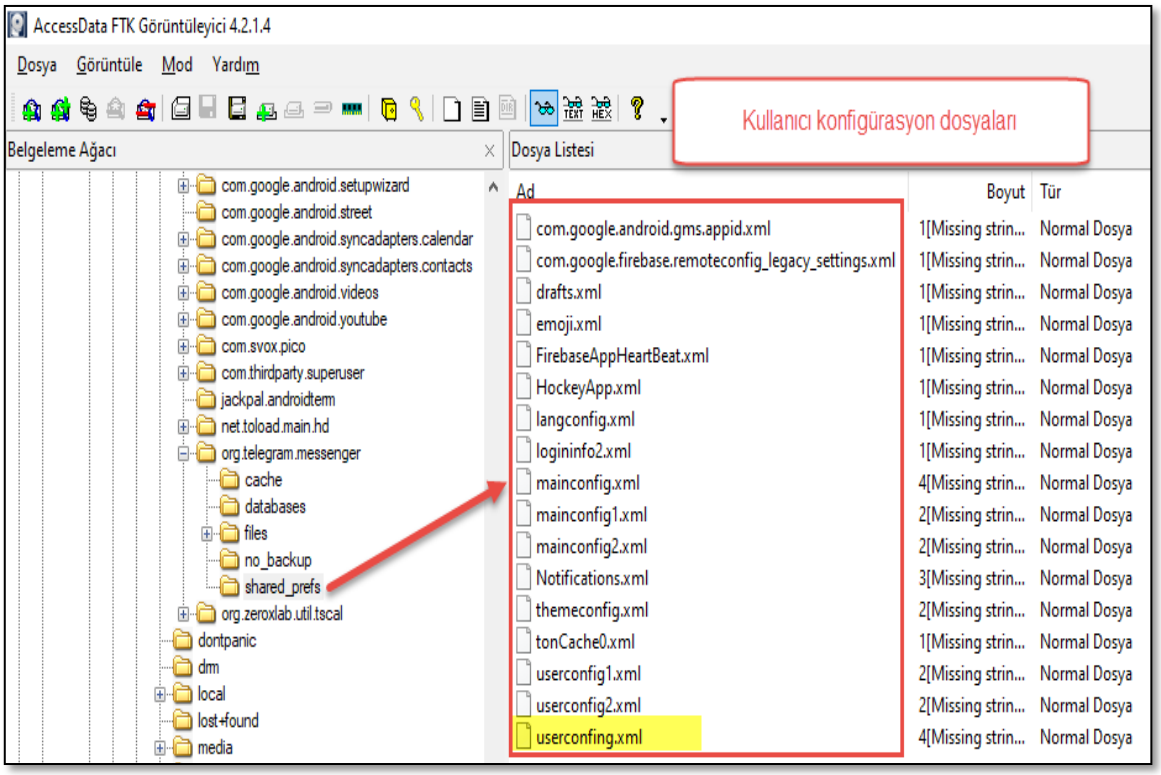
Şekil 4.40 Telegram’ a ait “cache” klasörü içeriği

Telegram uygulamasına ait “root/ android-4.4-r2/ data/ media/ 0/ Telegram/” uzantılı klasör içerisinde sohbetlerde gönderilen tüm belge ve medya dosyalarının tutulduğu görülmektedir. “Telegram” klasör içeriği **Şekil 4.41**. de gösterilmektedir.

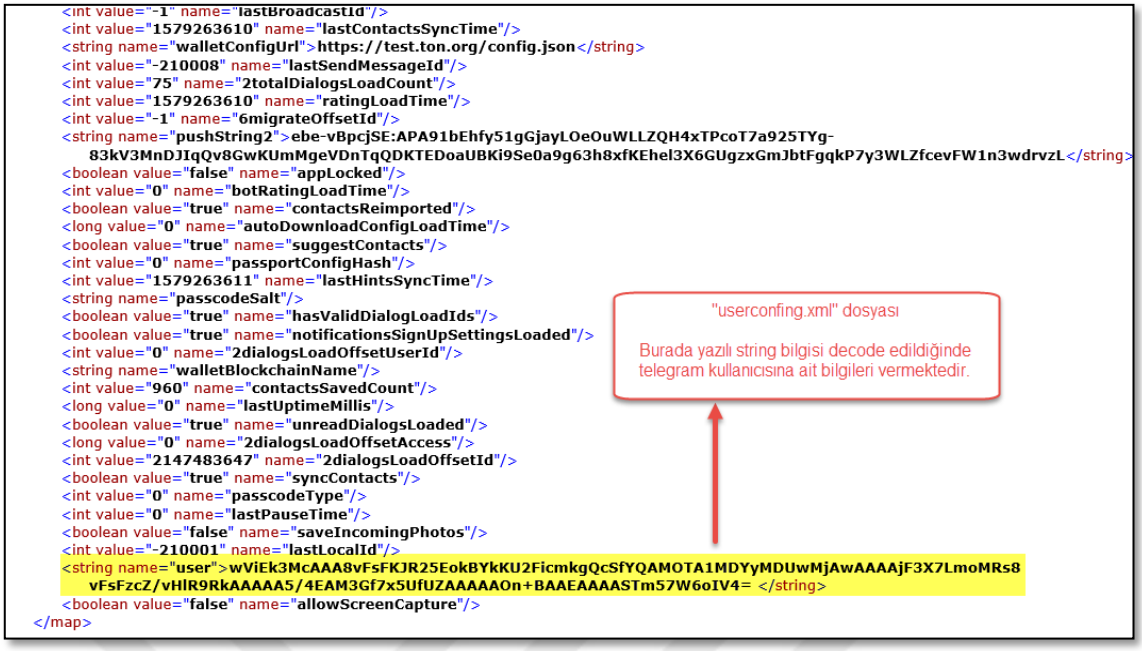


Şekil 4.41 Gönderilen tüm belge ve medya dosyalarının tutulduğu “Telegram” klasörü

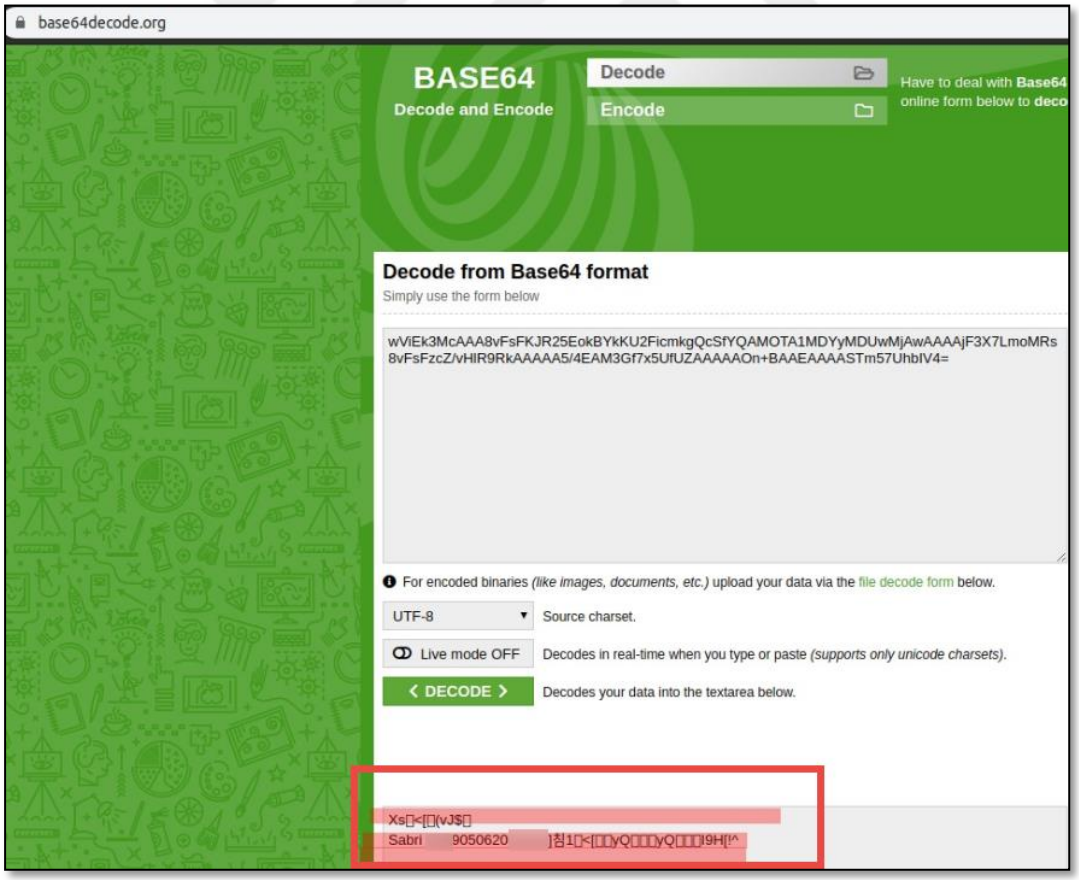
Telegram uygulamasına ait “root/ android-4.4-r2/ data/ data/ org.telegram.messanger” uzantılı klasör yolundaki “shared_prefs” isimli klasör içerisinde kullanıcı konfigürasyon dosyalarının olduğu görülmektedir. **Şekil 4.42** de gösterilen “shared_prefs” klasörü içerisinde yer alan “userconfig.xml” dosyasına bakıldığında telegram kullanıcısı bilgisinin string olarak tutulduğu görülmekte ve bu string dosyası decode edildiğinde kullanıc adı ve iletişim numarası bilgileri ortaya çıkmaktadır. “userconfig.xml” dosyasına ait içerik **Şekil 4.43** te sunulmakla birlikte “base64decode.org” [35] isimli site üzerinden decede edilen bilgiyi gösteren ekran görüntüsü **Şekil 4.44** te gösterilmektedir.



Şekil 4.42 Telegram’ a ait “shared_prefs” klasörü içeriği



Şekil 4.43 Telegram' a ait "userconfig.xml" isimli dosyanın içeriği



Şekil 4.44 Telegram' a ait "userconfig.xml" dosyasındaki bilgilerin decode edilmesi

4.3.5. Mobil Cihaza Yüklenilmiş Sohbet Uygulamasının Analizi

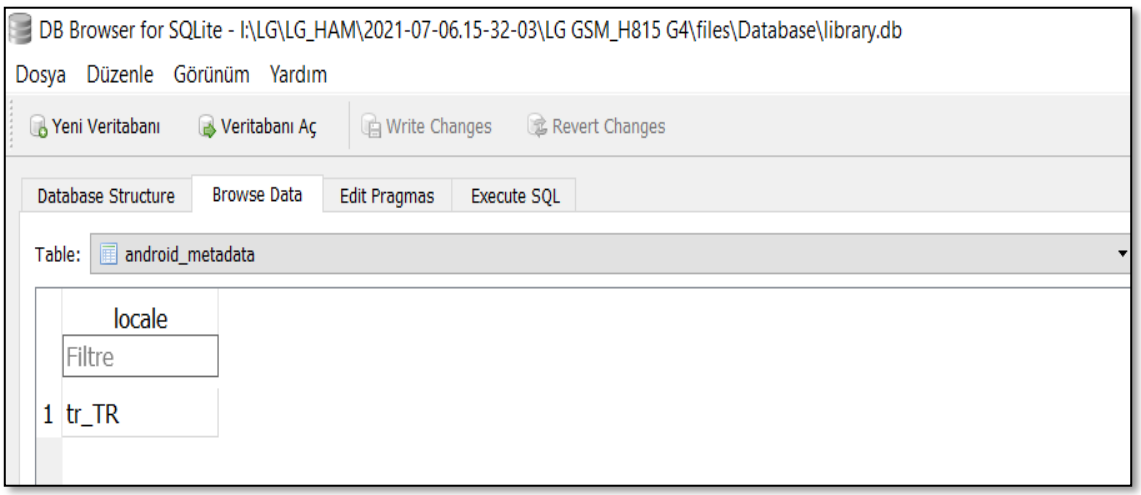
Mobil cihazlara yüklenilmiş uygulamaların tespitine yönelik yapılan çalışmalar neticesinde mobil cihaz imajı analiz yazılımlarının, fabrika ayarlarına döndürülmüş cihazlarda silinmiş olan uygulamaların tespitine yönelik verileri ortaya koymakta eksiklikleri oldukları görülmüştür.

Bununla ilgili olarak Google Play Store isimli uygulama marketine ait "Library.db" ve "Library.b-journal" veri tabanı dosyaları ile LG marka cep telefonlarına özgü olan LDB_Maindata.db veya MPT_Maindata.db veri tabanı dosyaları incelenmiştir.

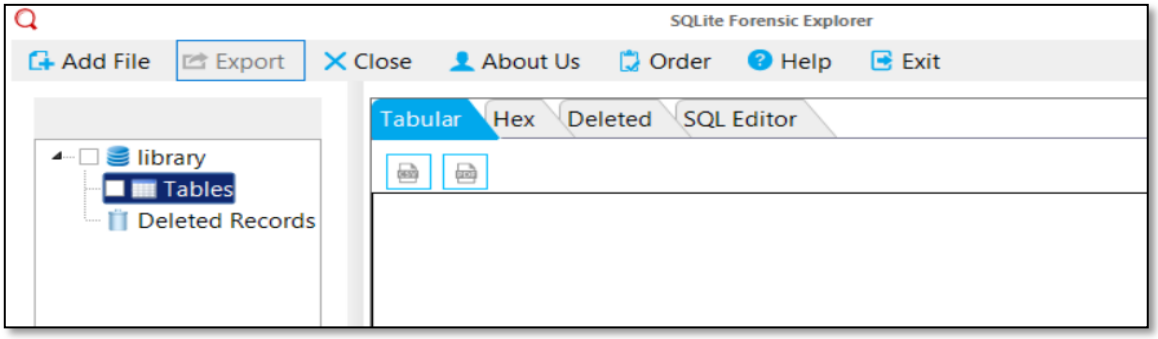
Google Play Store Uygulamasına ait Veri Tabanı Dosyası Analizi

Google Play Store isimli uygulama marketine ait "Library.db" ve "Library.b-journal" veri tabanı dosyalarına bakıldığında; mobil cihaza tanımlamış olan e-posta hesabı tarafından uygulama marketi üzerinden indirilmiş uygulamalara ait kayıtların tutulduğu görülmektedir. Burada dikkat edilmesi gereken tespiti yapılan uygulamaların imajı alınan mobil cihazda indirildiği anlamına gelmemekle birlikte o e-posta hesabının tanımlanmış olduğu herhangi bir mobil cihazda indirilmiş olabileceği göz önünde bulundurulmalıdır.

Yüklenilmiş olan sohbet uygulamasına yönelik ilk yapılan çalışmada; fabrika ayarlarına döndürüldükten sonra e-posta kullanıcı hesabı tanımlanmadan LG marka H815 G4 model cep telefonunun UFED 4PC yazılımı ile imajı alınmıştır. Sonrasında imaj içeriğinde yer alan Play Store isimli uygulama marketine ait Library.db ve Library.db-journal veri tabanı dosyaları incelendiğinde hiçbir uygulama bilgisinin gelmediği **Şekil 4.45** ve **Şekil 4.46** da görülmektedir.



Şekil 4.45 Fabrika ayarlarına döndürülmüş olan mobil cihazdaki Library.db dosyası



Şekil 4.46 Fabrika ayarlarına döndürülmüş olan mobil cihazdaki Library.db-journal dosyası

Sonrasında fabrika ayarlarına döndürülmüş cep telefonuna bir e-posta hesabı tanımlanmış olup e-posta hesabı tarafından bu zamana kadar indirilmiş olan uygulamalara dair bilgilerin yer aldığı veri tabanlarına ait tablolar **Şekil 4.47** ve **Şekil 4.48** de gösterilmektedir.

DB Browser for SQLite - I:\LG\LG_HESAP_TANIMI\2021-07-06.16-05-54\LG GSM_H815 G4\files\Database\library.db

Dosya Düzenle Görünüm Yardım

Yeni Veritabanı | Veritabanı Aç | Write Changes | Revert Changes

İndirilmiş uygulamalar

Satın Alma Zamanı (Unix zaman damgası)

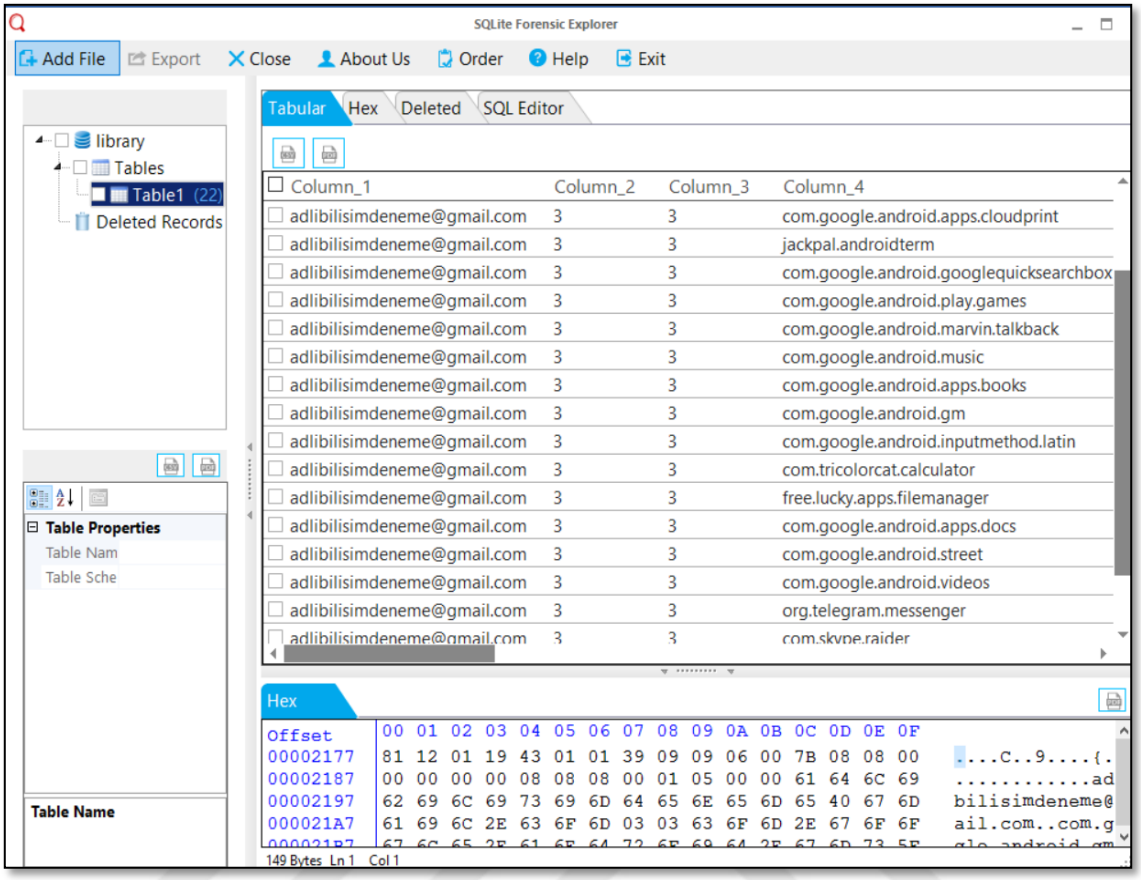
Database Structure | Browse Data

Tanımlanan E-posta Hesabı

Table: ownership

	account	library_id	backend	doc_id	purchase_time
	Filtre	Filtre	Filtre	Filtre	Filtre
1	adlibilisimdeneme@gmail.com	3	3	org.telegram.messenger	1579092465814
2	adlibilisimdeneme@gmail.com	3	3	jp.naver.line.android	1579242989515
3	adlibilisimdeneme@gmail.com	3	3	jackpal.androidterm	1542803068365
4	adlibilisimdeneme@gmail.com	3	3	free.lucky.apps.filemanager	1542806031439
5	adlibilisimdeneme@gmail.com	3	3	com.tricolorcat.calculator	1542803498997
6	adlibilisimdeneme@gmail.com	3	3	com.skype.raider	1579092489986
7	adlibilisimdeneme@gmail.com	3	3	com.linecorp.linelite	1579092550035
8	adlibilisimdeneme@gmail.com	3	3	com.google.android.youtube	1542801846246
9	adlibilisimdeneme@gmail.com	3	3	com.google.android.videos	1542808494409
10	adlibilisimdeneme@gmail.com	3	3	com.google.android.street	1542808423225
11	adlibilisimdeneme@gmail.com	3	3	com.google.android.play.games	1542803169779
12	adlibilisimdeneme@gmail.com	3	3	com.google.android.music	1542803224043
13	adlibilisimdeneme@gmail.com	3	3	com.google.android.marvin.talkback	1542803208802
14	adlibilisimdeneme@gmail.com	3	3	com.google.android.instantapps.supervisor	1625513631760
15	adlibilisimdeneme@gmail.com	3	3	com.google.android.inputmethod.latin	1542803325761
16	adlibilisimdeneme@gmail.com	3	3	com.google.android.googlequicksearchbox	1542803076077
17	adlibilisimdeneme@gmail.com	3	3	com.google.android.gms	1542801730511
18	adlibilisimdeneme@gmail.com	3	3	com.google.android.gm	1542803272441
19	adlibilisimdeneme@gmail.com	3	3	com.google.android.apps.maps	1542802862775
20	adlibilisimdeneme@gmail.com	3	3	com.google.android.apps.magazines	1542803021949
21	adlibilisimdeneme@gmail.com	3	3	com.google.android.apps.docs	1542807073335
22	adlibilisimdeneme@gmail.com	3	3	com.google.android.apps.cloudprint	1542803049425

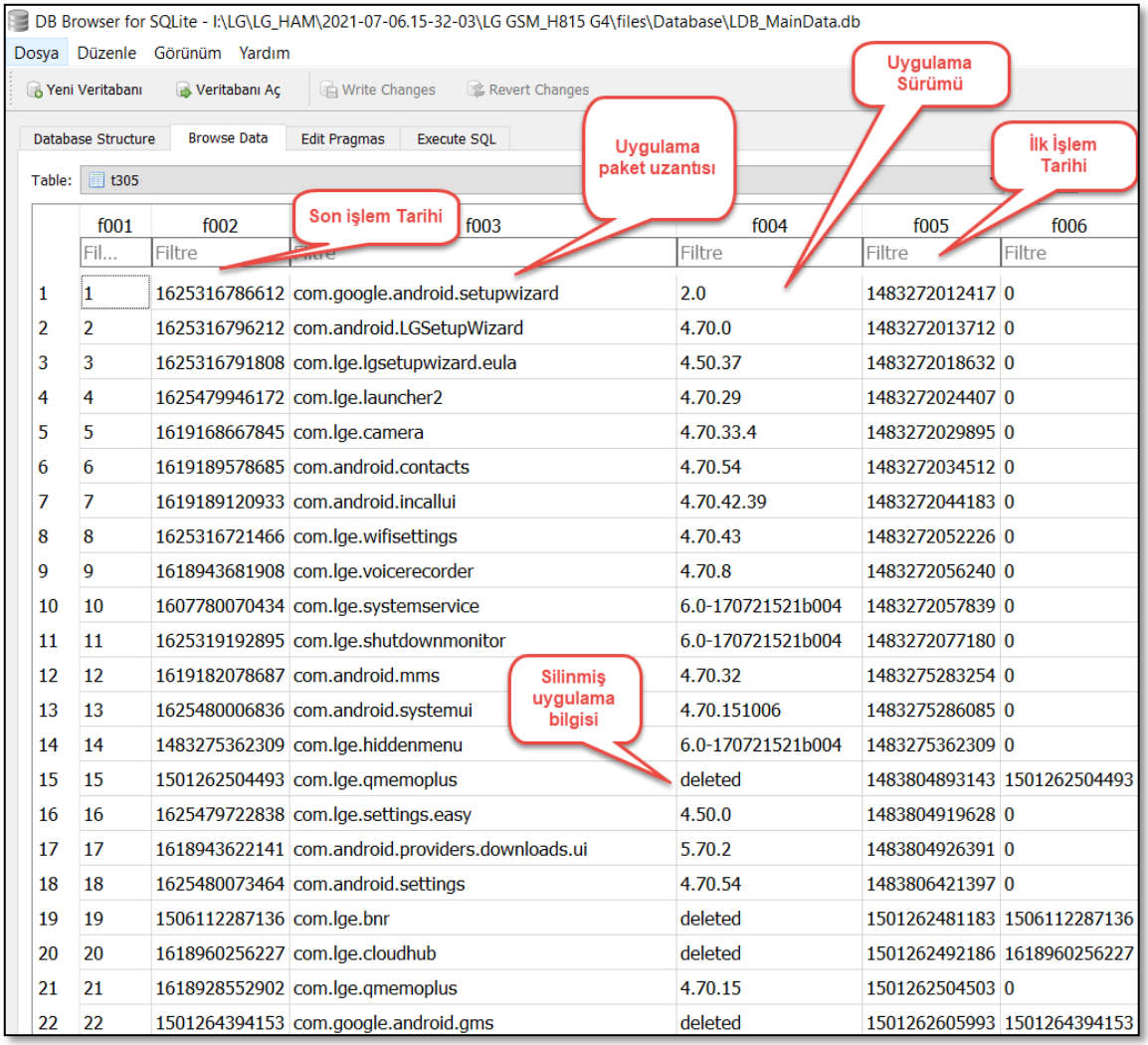
Şekil 4.47 E-posta hesabı tanımlamış olan mobil cihazdaki Library.db dosyası



Şekil 4.48. E-posta hesabı tanımlamış olan mobil cihazdaki Library.db-journal dosyası

LG Marka Cep Telefonlarına Özgü Veri Tabanı Dosyası Analizi

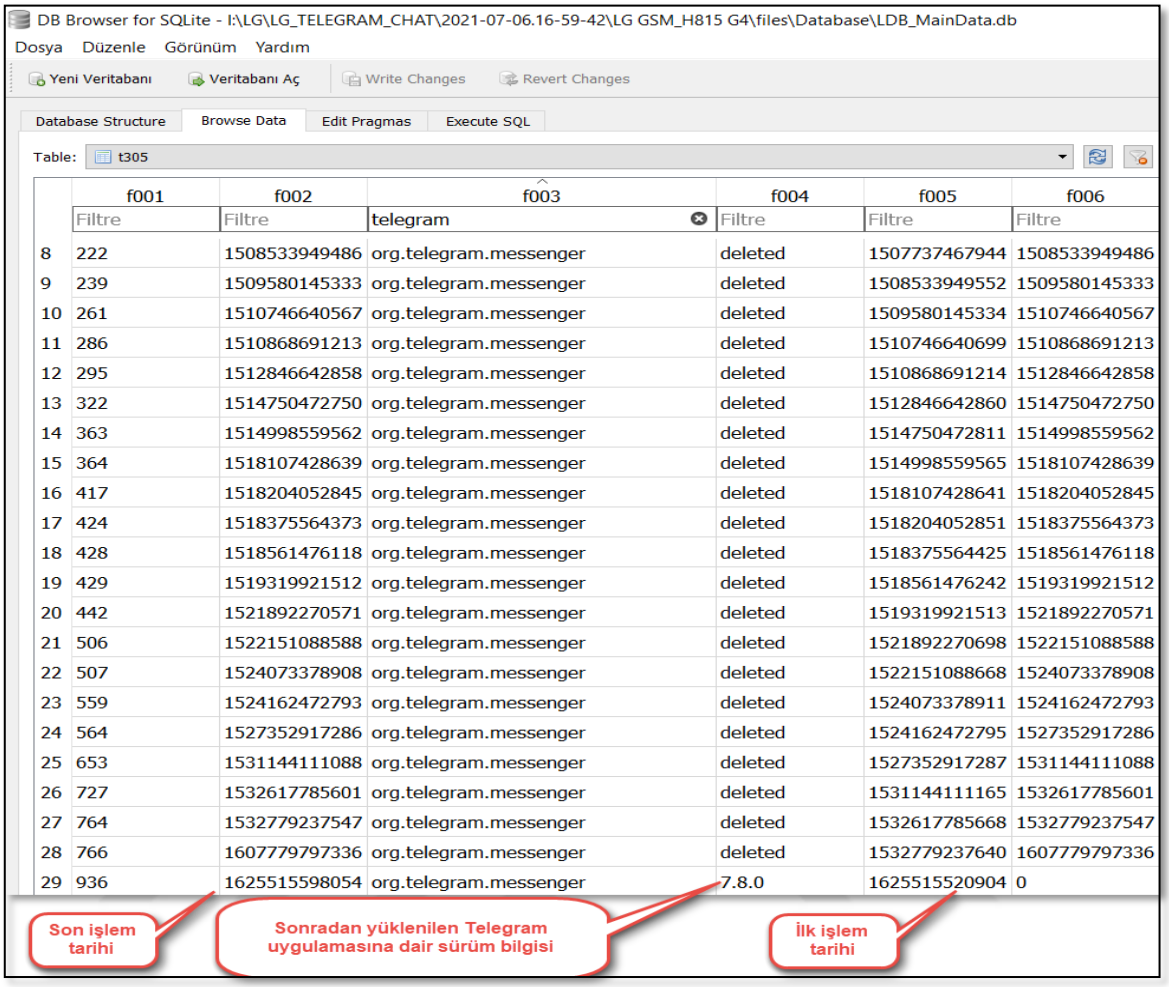
LG marka cep telefonlarında kendilerine özgü olan LDB_Maindata.db ya da MPT_Maindata.db veri tabanı dosyalarından bir tanesi bulunmaktadır. Bu dosyalar cep telefonun ilk kullanım anından itibaren yüklenilen tüm uygulamalara dair bilgileri tutmaktadır. Cep telefonu fabrika ayarlarına döndürülse de bu bilgiler veri tabanında kalmaktadır. Böylelikle tespit edilmesi gereken sohbet uygulamasının cep telefonuna yüklenilip yüklenilmediğine yönelik tespitler mümkün olabilmektedir. Fabrika Ayarlarına döndürülmüş olan cep telefonuna ait LDB_Maindata.db veri tabanı dosyasından gelen bilgilere bakıldığında, Yüklenilmiş uygulama dair paket ismi, yüklenilen versiyon bilgisi, silinmiş ise silinme bilgileri, Unix zaman damgası şeklindeki uygulamaya dair ilk işlem ve son işlem bilgilerinin yer aldığı görülmekte olup **Şekil 4.49** da gösterilmektedir.



	f001	f002	f003	f004	f005	f006
	Fil...	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	1625316786612	com.google.android.setupwizard	2.0	1483272012417	0
2	2	1625316796212	com.android.LGSetupWizard	4.70.0	1483272013712	0
3	3	1625316791808	com.lge.lgsetupwizard.eula	4.50.37	1483272018632	0
4	4	1625479946172	com.lge.launcher2	4.70.29	1483272024407	0
5	5	1619168667845	com.lge.camera	4.70.33.4	1483272029895	0
6	6	1619189578685	com.android.contacts	4.70.54	1483272034512	0
7	7	1619189120933	com.android.incallui	4.70.42.39	1483272044183	0
8	8	1625316721466	com.lge.wifisettings	4.70.43	1483272052226	0
9	9	1618943681908	com.lge.voicerecorder	4.70.8	1483272056240	0
10	10	1607780070434	com.lge.systemservice	6.0-170721521b004	1483272057839	0
11	11	1625319192895	com.lge.shutdownmonitor	6.0-170721521b004	1483272077180	0
12	12	1619182078687	com.android.mms	4.70.32	1483275283254	0
13	13	1625480006836	com.android.systemui	4.70.151006	1483275286085	0
14	14	1483275362309	com.lge.hiddenmenu	6.0-170721521b004	1483275362309	0
15	15	1501262504493	com.lge.qmemoplus	deleted	1483804893143	1501262504493
16	16	1625479722838	com.lge.settings.easy	4.50.0	1483804919628	0
17	17	1618943622141	com.android.providers.downloads.ui	5.70.2	1483804926391	0
18	18	1625480073464	com.android.settings	4.70.54	1483806421397	0
19	19	1506112287136	com.lge.bnr	deleted	1501262481183	1506112287136
20	20	1618960256227	com.lge.cloudhub	deleted	1501262492186	1618960256227
21	21	1618928552902	com.lge.qmemoplus	4.70.15	1501262504503	0
22	22	1501264394153	com.google.android.gms	deleted	1501262605993	1501264394153

Şekil 4.49 LDB_Maindata.db veri tabanı dosyası

Sonrasında daha önceden Telegram sohbet uygulaması yüklenilmiş olan LG marka cep telefonuna tekrardan Telegram uygulaması yüklenilmiştir. UFED 4PC yazılımı ile imajı alınan cep telefonuna ait LDB_Maindata.db veri tabanı dosyası incelendiğinde; cep telefonundan silinmiş olan Telegram uygulamasına ait ilk işlem ve son işlem bilgileri yer almakla birlikte sonradan yüklediğimiz Telegram uygulamasına dair sürüm bilgisi, ilk işlem ve son işlem bilgilerinin yer aldığı görülmüş olup **Şekil 4.50** de gösterilmektedir. Buradan anlaşılacağı üzere sürüm bilgisi yer alan uygulamanın hali hazırdaki cep telefonunda yüklü olduğu anlamına gelmektedir.



Şekil 4.50 LDB_Maindata.db veri tabanı dosyasındaki Telegram Uygulaması

4.4. Karşılaştırma Tablosu

Whatsapp, Telegram ve Skype ile hali hazırda uygulama marketlerinde olmayıp ancak kurulum dosyası bulunan Falcon simli sohbet ile ilgili olarak analiz çalışmaları yapılmış ve yapılan analizler sonucunda uygulamaların karşılaştırılması **Tablo 4.1** de sunulmuştur.

Tablo 4.1 Analizi yapılan uygulamaların karşılaştırılmasına ait tablo

UYGULAMA	Veri tabanı Dosyası	Veri tabanı dosyası şifreli	Sesli/Görüntülü Arama	Dosya Gönderme	Gizli Sohbet
Falcon	var	evet	hayır	evet	evet
Whatsapp	var	evet	evet	evet	hayır
Skype	var	hayır	evet	evet	hayır
Telegram	var	hayır	evet	evet	evet

5. SONUÇ

Teknolojinin insan hayatının her evresine girdiği günümüzde, insanlar yaşamının her anında teknolojik bir cihazla doğrudan ya da dolaylı olarak temas halinde bulunmaktadır. Özellikle tamamen kişiselleştirilen mobil cihazlar ve uygulamalar ile tamamen kişisel mahremiyet içeren cihazlar haline dönüşen teknoloji beraberinde suç konusu olmayı, suçun delili niteliğinde olmayı da getirmektedir. Yasalarımız gereği delil sayılabilmesi açısından dijital bir cihazın usulüne uygun olarak elde edilmiş olması, şeffaf ve güvenilir bir delil zinciri içerisinde yargıya ulaşmış olması gerekmektedir. Bu çalışma içerisinde hukuki sorunların yanı sıra mobil cihazların türleri, işletim sistemleri, adli kopyanın ne şekillerde alınabileceği konularına değinilmiştir. Son olarak da çalışmanın asıl konusu olan mobil cihazlar içerisindeki sohbet uygulamalarının analizleri anlatılmıştır. Günümüzde mobil cihazlar üzerinde en yaygın kullanılan sohbet uygulamaları, her türlü suçun konusu veya aydınlatıcısı olabilmektedir.

Mobil sohbet uygulamalarının yaygın kullanımı, ülkelerin mevcut sistemler ile iletişim tespiti ve suçun aydınlatması konularında yetersiz kalması mobil cihazların incelenmesi gerekliliğini doğurmaktadır. Bu incelemelerde ise ortaya birtakım zorluklar çıkmaktadır. Sohbet uygulamalarının başka bir uygulama gibi gösterilmesi, şifrelenmesi, veri tabanlarının şifrelenmesi gibi birçok durum söz konusu olmakta ve bu adli incelemelerde sorun teşkil etmektedir. Kullanılan popüler inceleme yazılımları bu zorlukları kısmen aşmakta fakat aşamadığı ve tanımlayamadığı durumlarda herhangi bir veri getirememektedir. Böyle bir inceleme sonucunda var olan inceleme yazılımları tarafından yapılan incelemenin eksik kaldığı ve soruşturma konusuna hiçbir fayda sağlamamaktadır.

Yapılan bu tez çalışmasında imajı alınabilen mobil cihazların imajları üzerinden, imajı alınamayan mobil cihazların işletim sistemlerine uygun olarak sanal makinelerde oluşturulan işletim sistemleri üzerinden istenilen incelemeler gerçekleştirilmiştir. Her bir sohbet uygulaması için oluşturulan senaryolar üzerinden birinci aşamada mevcut inceleme yazılımları ile mobil sohbet uygulamalarının analizleri yapılmış olup ikinci aşamada ise mobil sohbet uygulamalarına ait veri tabanı dosyaları manuel olarak incelenmiş, sohbet uygulamasına ait kullanıcı verilerini tutan veri tabanı dosyalarına bakılarak hangi bilgilerin elde edilebileceği tespit edilmiştir.

Elde edilen bu bilgiler doğrultusunda adli bilişim incelemesi gerçekleştirirken mobil cihaz imajı içeriğindeki veri tabanı dosyalarının tek tek ele alınmasının gerekliliği ortaya konulmuştur. Sadece ücretli popüler inceleme yazılımlarının getirdiği veriler ile yetinilmemelidir. Fabrika ayarlarına döndürülmüş bir mobil cihazda dahi yüklü veya daha önce yüklenmiş uygulamalara dair bilgilerin tutulduğu veri tabanı dosyaları bulunmaktadır. Yapılan tez çalışması ile adli bilişim açısından çok önemli olabilecek bu verilerin tespit edilmesi aşamalarında yaygın olarak kullanılan

yazılımların yetersiz kaldığı gösterilmiş, çalışmada veri türlerinin ne şekilde ve nerelerden elde edilebileceğine dair yöntemler ortaya konulmuştur.

Sonuç olarak incelenen sohbet uygulamalarından elde edilen bu bilgiler doğrultusunda bir karşılaştırma tablosu oluşturularak manuel yöntemler ile mobil sohbet uygulamalarının adli analizi modeli ortaya konulmuştur.

KAYNAKLAR

[1] Xiaodong Lin, Ting Chen, Tong Zhu, Kun Yang, Fengguo Wei 2018. Automated forensic analysis of mobile applications on Android devices, *Digital Investigation*, S59-S66

[2] Digital Evidence and Forensics https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx. Ulusal Adalet Enstitüsü Erişim: 20-08-2019.

[3] World of Warcraft İtiraf ve Dijital Kanıt İzi, https://www.wired.com/2011/11/world-of-warcraft-confession, Erişim: 22-08-2019.

[4] Nardoni David, http://www-scf.usc.edu/~uscsec/images/DigitalEvidence&Computer Forensics version 1.2 USC.pdf, Erişim: 15-03-2020.

[5] Nardoni David - Dijital Kanıtlar ve Bilgisayar Adli Tıp, http://www-scf.usc.edu/~uscsec/images/DigitalEvidence&ComputerForensicsversion1.2USC.pdf. Erişim: 22-08-2019.

[6] Türk Ceza Muhakemesi Kanunu 134, http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm, Erişim: 18-08-2019.

[7] Muzammil Hussain, A:A: Zaidan, B.B Zidan, S. Iqbal, M.M. Ahmed, O.S Albahri, A.S. Albahri 2018. Conceptual *framework for the security of mobile health applications on Android platform,Telematics and Informatics*, Volume 35, Issue 5, August 2018, 1335-1354

[8] Akıllı Telefon Tanımı, https://searchmobilecomputing.techtarget.com/definition/smartphone. Erişim: 18-07-2019.

[9] Smartphone, https://en.m.wikipedia.org/wiki/Smartphone Erişim: 20-08-2019.

[10] IBM Simon, https://tr.wikipedia.org/wiki/IBM_Simon Erişim: 20-08-2019.

[11] FBI details how drones are being used for crime, https://www.techradar.com/news/criminal-intent-fbi-details-how-drones-are-being-used-for-crime Erişim: 21-08-2019.

[12] Extracting Forensic Data From Drones, https://insideunmannedsystems.com/extracting-forensic-data-from-drones, Erişim: 22-08-2019.

[13] Uyuşturucu Kaçakçılığında Drone Kullanımı Haberi, https://www.hurriyet.com.tr/dunya/iranda-iraka-drone-ile-uyusturucu-kacakciligi-40770160, Erişim: 24-08-2019.

[14] Sebastian Nemetz, Sven Schmitt, Felix Freiling. A standardized corpus for SQLite database forensics. *Digital Investigation.* March 2018, 121-130

[15] IOS Tarihçesi, https://en.wikipedia.org/wiki/IOS_version_history, Erişim: 24-08-2019.

[16] IOS Mimarisi, https://en.wikipedia.org/wiki/IOS, Erişim: 24-08-2019.

[17] Architecture of Blackberry Mobile OS, https://www.researchgate.net/figure/Architecture-of-Blackberry-Mobile-OS_fig3_280310649 Erişim: 24-08-2019.

[18] Dohyun Kim, Sangjin Lee. Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Science International: Digital Investigation,* January 2020,200897

[19] Radhika Padmanabhan, Karen Lobo, Mrunali Ghelani, Dhanika Sujan, Mahesh Shirole. Comparative analysis of commercial and open source mobile device forensic tools, *Contemporary Computing (IC3), International Conference on.* 1-6

[20] Cellebrite UFED, http://www.forensicswiki.org/wiki/Cellebrite_UFED. Cellebrite_UFED 24-08-2019.

[21] https://www.breakingnews.ie/ireland/ira-membership-trial-hears-mobile-phone-evidence-549779.html Erişim: 23-08-2019.

[22] Recovered Blackberry Had Received Call, https://www.theborneopost.com/2011/12/01/recovered-blackberry-had-received-call-from- %e2%80%98datuk-pathma-2%e2%80%99-high-court-told/ Erişim: 23-08-2019.

[23] Deft Linux, http://www.deftlinux.net/ Erişim: 27-08-2019.

[24] concise-courses, http://www.concise-courses.com/security/mobile-forensics-tools Erişim: 27-08-2019.

[25] BitPim, http://www.bitpim.org/ Erişim: 27-08-2019.

[26] Kipper, G, (2007). Wireless Crime and Forensic Investigation, Newyork.

[27] Caine Linux, https://www.cyberpunk.rs/gnu-linux-digital-forensics-distro-caine Erişim: 27-08-2019.

[28] Mobıle/Pda Forensıc Tools, http://securitytools.wikidot.com/mobile-pda-forensic-tools Erişim: 27-08-2019.

[29] OSAF-Toolkit, https://sourceforge.net/projects/osaftoolkit/ Erişim: 27-08-2019.

[30] Simon Baechler, Marie Morelato, Simone Gittelson, Simon Walsh, Pierre Margot, Claude Roux, Olivier Ribauxa. Breaking the barriers between intelligence, investigation and evaluation: A continuous approach to define the contribution and scope of forensic science, *Forensic Science International*, April 2020, 110213

[31] Khushboo Rathi, Umit Karabiyik, Temilola Aderibigbe, Hongmei Chi. Forensic analysis of encrypted instant messaging applications on Android. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1-6

[32] WhatsApp Viewer, https://github.com/andreas-mausch/whatsapp-viewer, Erişim: 12-11-2019.

[33] Apktool, https://github.com/iBotPeaches/Apktool, Erişim: 08-09-2019.

[34] Cosimo Anglano, Massimo Canonico, Marco Guazzone. Forensic analysis of Telegram Messenger on Android smartphones. *Digital Investigation.* December 2017, 31-*49*

[35] Decode and Encode Site, base64decode.org, Erişim: 15-09-2019.

ÖZGEÇMİŞ

Sabri ERDEMİR

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]