MOBİL CİHAZLARDA SOSYAL MEDYA UYGULAMALARININ ADLİ BİLİŞİM AÇISINDAN ANALİZİ

Fatma GÜNEŞ ERİŞ

Yüksek Lisans Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Erhan AKBAL

TEMMUZ-2018

T.C
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MOBİL CİHAZLARDA SOSYAL MEDYA UYGULAMALARININ ADLİ BİLİŞİM AÇISINDAN ANALİZİ

YÜKSEK LİSANS TEZİ

Fatma GÜNEŞ ERİŞ

(151129101)

Tezin Enstitüye Verildiği Tarih : 3 Temmuz 2018
Tezin Savunulduğu Tarih : 18 Temmuz 2018

Tez Danışmanı : Dr. Öğr. Üyesi Erhan AKBAL
Diğer Jüri Üyeleri : Doç. Dr. Galip AYDIN (F.Ü)
Doç. Muhammed Fatih TALU (İnönü Ü.)

TEMMUZ-2018

ÖNSÖZ

Akademik hayatım ve tez çalışma aşamasında maddi manevi destek ve yardımlarını esirgemeyen kıymetli danışmanım Dr. Öğr. Üyesi Erhan AKBAL' a sonsuz teşekkürlerimi sunarım.

Bu tez çalışmasında Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü Adli Bilişim Laboratuvarına ait Oxygen Forensic, Paraben E3:DS ve Magnet Axiom lisanlı yazılımları kullanılmıştır. Çalışma sürecinde bölüm imkanlarını kullanıma açan değerli Adli Bilişim Mühendisliği Öğretim elemanlarına teşekkürü bir borç bilirim.

Bu tez çalışması süresince her an destekçim ve umut vericim olan sevgili eşim Mustafa ERİŞ' e, gülümseyişi ile hayat enerjimi veren kızım Amine Zehra'ya teşekkür ederim.

Tüm ömrüm ve tez dönemim süresince kendi sağlık ve imkanlarından feragat ederek, her türlü yardımını gördüğüm annem Emine GÜNEŞ' e ve babam Mehmet GÜNEŞ 'e, akademik hayata adım atmama vesile olan ablam Nurcan GÜNEŞ 'e ve manevi destekçim kız kardeşim Emine GÜNEŞ 'e sevgi ve teşekkürlerimi sunarım.

Fatma GÜNEŞ ERİŞ

ELAZIĞ–2018

İÇİNDEKİLER

Sayfa No

ÖZET

Mobil cihazlar son yıllarda hayatın her alanında yoğun bir şekilde kullanılmaya başlanmıştır. Piyasada birçok mobil cihaz çeşidi bulunmaktadır ve bu cihazlar için çok çeşitli işletim sistemleri, dosya sistemleri ve uygulamalar geliştirilmiştir. Bu gelişim ile birlikte bu cihazların suç faaliyetlerinde kullanım oranları da artmıştır. Sürekli değişen ve gelişen mobil cihazların suçun işlenmesinde direk veya dolaylı olarak kullanılması ile mobil cihaz incelemesini önemli bir konu haline getirmiştir. Bu ihtiyaç adli bilişimin bir dalı olarak mobil adli bilişimi ortaya çıkarmıştır.

Mobil adli bilişim, mobil bir cihazdan gelen dijital kanıtları, kabul edilmiş yöntemlerle inceleyerek veriler elde etmeyi ve bu veriler ışığında suça konu olan delilleri ortaya koymayı amaçlayan bilim dalıdır. Sosyal ağ adli bilişimi ise sosyal ağlar üzerinde delil teşkil edebilecek birçok kişisel veriye ulaşmayı ve bunları analiz edip raporlamayı içeren bilim dalıdır. Mobil cihazlardaki sosyal ağ uygulamalarının bıraktığı kişisel verilerin çokluğu düşünüldüğünde, mobil cihazlardaki sosyal medya uygulamalarının incelenmesinin önemi ortaya çıkar.

Bu tez çalışmasında mobil cihazların adli incelenmesi için gerekli süreçler incelenmiş, mobil cihazlardan veri çıkarımına ilişkin gerekli işlemler açıklanmış, mobil cihazlarda sosyal medya uygulamalarının adli bilişim açısından analizinin nasıl gerçekleştirilmesi gerektiği ortaya konulmuştur. Tez çalışmasının uygulama kısmında, günümüzde en çok kullanılan mobil işletim sistemlerinden olan Android ve iOS yüklü cihazları üzerine; Facebook, WhatsApp Messenger, Instagram, Twitter ve BiP Messenger uygulamaları yüklenmiş, temel kullanıcı davranışları gerçekleştirilmiş cihazların analizi gerçekleştirilmiştir. İnceleme yapılırken mobil adli bilişim alanında en yetkin araçlardan olan Oxygen Forensic, Paraben E3:DS, Magnet Axiom araçları kullanılmıştır.

Anahtar Kelimeler: Adli bilişim, Mobil Adli Bilişim, Sosyal Medya Uygulamaları, Adli Bilişim Araçları

SUMMARY

Forensic Analysis Of Social Media Applications On Mobile Devices

Mobile devices have begun to be used extensively in all areas of life in recent years. There are many types of mobile devices on the market, and a variety of operating systems, file systems and applications for these devices have been developed. With this development, the usage rates of these devices in criminal activities have also increased. The use of mobile devices has become an important issue, as the ever-changing and evolving mobile devices are used directly or indirectly in the process of crime. This need has revealed mobile forensic computing as a branch of forensic computing.

Mobile forensic science is a science which aims to obtain data by examining digital evidence from a mobile device with accepted methods and to reveal the succesive subject matter in the light of this data. Social networking is the science of reaching out to many personal data that can be evidence on social networks and analyzing and reporting them. Considering the multitude of personal data left by social networking applications on mobile devices, the importance of reviewing social media applications on mobile devices arises.

In this thesis study, the necessary processes for Forensic analysis of mobile devices were examined, necessary procedures for data extraction from mobile devices were explained, and how social media applications should be analyzed in terms of forensic information. In the application part of the thesis study, on the devices which have Android and iOS which are the most used mobile operating systems today; Facebook, WhatsApp Messenger, Instagram, Twitter and BiP Messenger applications were installed, and basic user behavior was performed. In the study, Oxygen Forensic, Paraben E3: DS, Magnet Axiom tools, which are among the most competent tools in the field of mobile forensics, were used.

Keywords: Forensic Informatics, Mobile Forensic Informatics, Social Media Applications, Forensic Tools

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR LİSTESİ

ADB : Android Debug Bridge

CPU : Central Processing Unit

GB : Gigabyte

iOS : iPhone Operating System

NIST : National Institute of Standards and Technology

RAM : Random Access Memory

SDK : Software Development Kit

SIM : Subscriber Identification Module

URL : Uniform Resource Locator

USB : Universal Serial Bus

LLB : Low Level Bootloader

1. GİRİŞ

Adli bilişim, yasal olarak kabul edilebilir bir şekilde elektronik veya dijital cihazlarda bulunan verilerin toplanması, analiz edilmesi ve raporlanmasına odaklanan bir bilim dalıdır [1]. Bu veriler hukuk, ceza veya idari durumlarda delil olarak kullanılmak üzere toplanır [2]. Mobil adli bilişim, mobil cihazlardan gelen dijital kanıtları, kabul edilmiş yöntemleri kullanarak, inceleyerek elde etmeyi ve ortaya koymayı amaçlayan adli bilişim dallarından biridir [3].

Mobil cihazlardaki gelişmeler; artan hız, güç ve depolama alanı, daha fazla kişiyi cihazlarını çevrimiçi alışveriş, fatura ödeme, sosyal paylaşım yapma gibi çok çeşitli kişisel işlemlerde kullanmaya yönlendirmiştir. İstatistiklere göre dünyadaki web trafiğinin %52'si mobil telefonlar üzerinden gerçekleşmektedir [4]. Mobil cihazların yaygınlaşması ile sosyal medya uygulaması kullanımı da artış göstermiştir. Sosyal medya uygulamaları kullanıcıyı kişisel verilerini paylaşması için teşvik etmektedir. Böylelikle sosyal medya uygulaması kullanan kişiler, çoğu kez farkında olmadan mobil cihazlarında çok sayıda kişisel veri kalıntısı bırakmaktadırlar [5]. Bu durum mobil cihazları bir suç tespiti sırasında incelenmesi gereken öncelikli delillerden kılmaktadır. Öte yandan mobil cihazların veri sızıntısı, kötü amaçlı yazılım, kimlik hırsızlığı, korsanlık, yasadışı ticaret, cinsel taciz, siber takip ve siber terörizm gibi kötü niyetli faaliyetler için siber suçlular tarafından kullanıldığı veya hedeflendiği bilinmektedir. Tüm bu nedenlerden ötürü mobil adli bilişim alanında yapılan çalışmalar adli bilişim incelemelerinin geleceği açısından çok önemlidir [6].

Mobil cihazlar üzerindeki sosyal medya uygulamalarının analizinin gerçekleştirilmesi tek başına bir çalışma alanı teşkil etmektedir. Piyasada mobil cihaz inceleme için geliştirilmiş çok sayıda araç bulunmaktadır. Bu araçlar sosyal medya uygulamalarındaki veriyi ayıklama yetenekleri farklılık göstermektedir. Mobil cihaz inceleme araçları cihazlardaki çeşitlilik ve uygulamaların sürekli yenilenmesinden ötürü inceleme yapan kişiye cevap veremediği durumlarda, analizi yapan kişinin dosya sisteminden verilere kendi ulaşması gerekebilir. Bu durumda inceleme yapan kişinin uygulamaların işletim sistemine göre veri saklama biçimlerinin bilinmesi gerekmektedir.

1.1 Tezin Amacı

Bu tezin amacı mobil cihazlarda sosyal medya uygulamalarının adli bilişim açısından analizinin nasıl gerçekleştirileceğini ortaya koymaktır. İnceleme için en çok tercih edilen işletim sistemlerinden Android ve iOS 'un yüklü olduğu Sony Xperia Z2 ve iPhone 6S cihazları seçilmiştir. Sosyal medya uygulamalarından ise Türkiye'de yaygın olarak kullanılan Facebook, WhatsApp Messenger, Instagram, Twitter, BiP Messenger uygulamaları kullanılmıştır. Bu tez çalışması ile bahsi geçen sosyal medya uygulamalarının analizini, hem ticari mobil adli bilişim araçları kullanarak, hem de cihazın dosya sisteminden çıkarılan uygulamalara ait dosyaların manuel olarak görüntülenmesi ile veri çıkarımının nasıl gerçekleştirileceği gösterilecektir. Bu çalışma ile kullanılan mobil adli bilişim araçlarının uygulama analizindeki başarımı kıyas edilebilecek, bu alanda çalışacak olan kişilere araç seçimi için yol gösterecektir. Bu araçlara sahip olamayanlar veya bu araçların incelemeyi yapan kişiye yeterli olamadığı durumlar için uygulama analizlerinin manuel olarak nasıl gerçekleştirileceği de ortaya konmuştur.

1.2 Tezin Yapısı

Bu tez çalışması toplamda 6 bölümden oluşmaktadır.

Bölüm 2'de Mobil Cihazlarda Adli Bilişim başlığı altında; Adli bilişim kavramı açıklanmış, adli bilişimin alt dallarına değinilmiş, bunlardan mobil adli bilişimin tanımı yapılmış, mobil adli bilişim aşamaları ve veri çıkarma yöntemleri ele alınmıştır. Bu alanda yapılan literatür çalışmalarına da yer verilmiştir.

Bölüm 3'de çalışma metodolojisinin nasıl olduğu anlatılmıştır. Öncelikle çalışma için gerekli olan donanım ve yazılımlar anlatılmış, sonrasında çalışma için gerçekleştirilen hazırlıklara yer verilmiştir. Uygulamaların cihazlara yüklenip, bir takım kullanıcı davranışları gerçekleştirildikten sonra cihazların adli görüntüleri olan imajlarının alınması işlemleri bu kısımda gerçekleştirilmektedir.

Bölüm 4'de Android işletim sisteminde sosyal medya uygulamalarının adli bilişim analizinin nasıl gerçekleştirileceği anlatılmıştır. İncelemeye hazır hale getirilen Android cihazda, analizi yapılacak her bir uygulamanın yapısı incelenmiş, adli bilişim açısından önemli olan bulgulara nasıl erişilebileceği ortaya konmuştur. Analiz manuel ve mobil adli bilişim araçları ile olmak üzere iki başlık altında anlatılmıştır.

Bölüm 5’de Bölüm4’de yapılan tüm işlemler iOS cihaz üzerinde gerçekleştirilmiştir.

Bölüm 6’da ise analiz aşamasında uygulamalar üzerinde tespit edilebilen kullanıcı davranışları ortaya konmuştur.

Bölüm 7’de ise sonuçlar değerlendirilmiştir.

2. MOBİL CİHAZLARDA ADLİ BİLİŞİM

Mobil cihazlar hayatımızın vazgeçilmez bir parçası halini almıştır. Bu cihazlar iletişim kurmak için kullanıldığı gibi internete erişmek ses ve kamera kaydı yapmak, sosyal ağlar aracılığı ile fotoğraf, video, konum, ses kaydı herhangi bir not paylaşmak için de kullanılabilmektedir. Genel olarak bakıldığında bir mobil cihaz arama geçmişi, e-posta, kısa mesaj, fotoğraf, video, takvim, hatırlatıcı not, konum bilgisi, uygulama verisi, şifre gibi birçok kişisel veri barındırmaktadır.

Mobil cihazlar birden çok şahıs tarafından kullanılsa bile yaşanabilecek herhangi olumsuz bir durumda sorumluluk cihaz sahibinindir. Bu cihazlar veri sızıntısı, kötü amaçlı yazılım, kimlik hırsızlığı, korsanlık, yasadışı ticaret, cinsel taciz, siber takip ve siber terörizm gibi akla gelebilecek birçok kötü niyetli faaliyet için siber suçlular tarafından kullanılmakta ve / veya hedeflenmektedir. Günümüzdeki mobil cihaz kullanımı ve bu cihazların içerdiği verilerin önemi düşünüldüğünde herhangi bir suç durumunda mobil cihazlar bilgi edinmek için öncelikli delillerden olmaktadır. Bu sebeple bu cihazların adli olarak incelenmesi öncelikli araştırma konularındandır.

Bu bölümde mobil cihazların delil kaynağı olarak nasıl kullanılabileceği anlatılacak, mobil cihazlardaki tehdit unsurları ele alınacak, bu cihazlardaki adli bilişim safhaları açıklanarak bu cihazlar üzerinde dijital delillerin elde edilmesinde ve incelenmesinde kullanılan yazılımlar gösterilecektir.

2.1 Adli Bilişim Kavramları

Adli bilişim, bilgisayarlarda veya dijital depolama aygıtlarında bulunan dijital verilerin yasalara uygun olarak hakkındaki gerçekleri tanımlama, koruma, kurtarma, analiz etme ve sunma bilimidir[5]. Adli bilişim başlangıçta yalnızca bilgisayar adli bilişimi ile eş anlamlı olarak kullanılırken gün geçtikçe dijital verileri depolayabilen tüm cihazların incelenmesi olarak genişletilmiştir[7]. Adli bilişimin çeşitli uygulama alanları mevcuttur. En yaygın olanı hukuk mahkemeleri önünde bir hipotezi desteklemek ya da reddetmektir. Başka bir uygulama alanı olarak özel sektörlerdir. Özel sektörde şirket içi araştırmalar veya izinsiz giriş araştırmaları gibi araştırmalarda kullanılır.

Adli bilişim bilimi inceleme yapılan cihaz, medya veya bulgulara göre çeşitli alt dallara ayrılmaktadır. Bunlar Şekil 2.1'deki gibi bilgisayar adli bilişim, mobil adli bilişim, ağ adli bilişim, veri tabanı adli bilişim, sosyal medya adli bilişim, bulut adli bilişim gibi sıralanabilir.

Şekil 2.1. Adli Bilişim Alt Dalları

2.1.1 Bilgisayar Adli Bilişim

Adli bilişimin en eski disiplinidir. Mevcut adli bilişim alt dallarının oluşmasına temel hazırlamıştır. Bilgisayar adli bilişimi dijital delilleri tanımlama, koruma, analiz etme, sunma adımlarını içeren inceleme süreçlerini içerir [5]. Dizüstü, masaüstü bilgisayarların veya sunucuların disklerinin incelenmesi, bunlardan silinen verilerin kurtarılması, canlı ram analizinin yapılması bu alanda gerçekleştirilen işlemlerdir. Ayrıca dosya sistem adli bilişimi bu alanın bir alt disiplini olarak sayılabilir. Delil dosya sistem türüne göre değerlendirilip veri kurtarma işlemi buna uygun şekilde gerçekleştirilir.

2.1.2 Mobil Adli Bilişim

Mobil adli bilişim, mobil bir cihazdan gelen dijital kanıtları, kabul edilmiş yöntemlerle inceleyerek veriler elde etmeyi ve bu veriler ışığında suça konu olan delilleri ortaya koymayı

amaçlayan bilim dalıdır[3]. Her geçen gün mobil cihazların gelişerek çeşitlenmesi ve inceleme araçlarının bu hıza ayak uyduramaması bu alandaki önemli problemlerden biridir. Mobil cihazlardaki farklı CPU mimarileri, iyi korunan işletim sistemleri, sınırlı bellek kaynakları ve çeşitli donanımlar, adli inceleme uzmanlarının üstesinden gelmek zorunda oldukları genel zorluklardır. Bu zorlukların en büyüğü ise mobil cihazlarda güvenlik amaçlı kullanılan yazılım ve donanım teknolojilerinin ilerlemesi ile kullanılan mobil adli bilişim yöntemleri etkinliğini kaybediyor olmasıdır. Tüm bu sorunlar ve zorlukla mobil adli bilişim alanında çalışılmasının ne kadar önemli olduğunu ortaya koyar.

Mobil bir cihaz delil olarak ele geçirildikten sonra dışarı ile olan bütün bağlantısı kesilmelidir. Cihaz kapalıysa, cihazın izolasyonu için özel bir malzeme olan bir faraday poşetine yerleştirilebilir. Cihaz açıksa, uçucu verileri elde etmek için cihazı açık bırakmak daha iyidir çünkü telefon şifreli veya şifre korumalıysa, kapatılması dijital kanıtların erişilememesine neden olabilir. Cihazı bir uçak moduna getirmek ve uzaktan silme komutlarını önlemek için tüm ağ bağlantılarını devre dışı bırakmak gerekir. Pil ömrü problemi cihaz üzerinde ortaya çıkabilir ve veri çıkarma işlemi sırasında mevcut harici güç kaynağına ihtiyaç olabilir[2]. Mobil cihazlarda dijital kanıt elde etmek ve analiz etmek için birçok ticari ve açık kaynak aracı bulunmaktadır. Mevcut tüm önemli verileri çıkarmak için birden fazla yöntem gerekebilir. İncelemenin her adımını belgelemek de inceleme yapan kişi için çok önemlidir. Root ve jailbreak gibi değişiklikler gerekli olabilir. Bu durum mahkemede delillerin kabul edilebilirliği için ayrıntılı olarak açıklanmalıdır. Mobil cihazların genellikle araştırmalar sırasında aktif olmasından dolayı, adli uzmanlar tarafından veri güncellemesi olasılığı göz önünde bulundurulmalıdır. Aynı cihazın imajları arasında farklılıklar oluşabilir. Ancak, tek bir dosya için aynı hash değerini elde etmesi beklenir [8].

2.1.3 Sosyal Ağ Adli Bilişimi

Sosyal ağ bireylerin internet üzerinde bulunan sosyal ağ siteleri, sanal oyunlar, sözlükler, forumlar gibi internet siteleri üzerinden birbiri ile paylaşım yapabildikleri ve iletişime geçebildikleri ortamlara verilen genel isimdir [9]. Bu ortamlarda kişisel verilerin bulunması nedeni ile adli bilişim incelemelerinde bir hazine sandığı niteliğindedir. 2018 “We are social” ajansı verilerine göre Facebook kullanıcı sayısı 2.17 milyar kişiye ulaşmıştır [4]. Sosyal medya kullanımındaki bu ciddi artış ile bu alanda inceleme yapılmasının önemi

artmıştır. Sosyal ağ adli bilişimi sosyal ağlar üzerinde delil teşkil edebilecek birçok veriye ulaşmayı ve bunları analiz edip raporlamayı içeren disiplin dalıdır.

2.1.4 Bulut Adli Bilişimi

NIST, Bulut Bilişimi minimum yönetim çabası veya servis sağlayıcı etkileşimi ile yapılandırılabilir bir kaynak havuzundaki verilere her yerden erişilebilmesini sağlayan bir model olarak tanımlar [3]. Mobil Bulut Bilişimin altyapısının araştırılması, sanallaştırma, veri dağılımı, çoklu kiracılık, birlikte işlerlik ve hareketlilik özellikleri nedeniyle zordur. Bulut adli bilişimi, mimarisi sebebi ile ağlardan ve ağa bağlı cihaz ve sistemlerden oluşması nedeniyle ağ adli bilişiminin, veri depolama olanakları ile bilgisayar adli bilişiminin, mobil cihaz üzerinde kullanımının yaygınlığı nedeni ile de mobil adli bilişiminin birleşimi bir adli bilişim alt disiplini olarak kabul edilmektedir [10]. Bulut adli bilişimde inceleme sırasında hangi bulut mimarisinin kullanıldığı göz önünde bulundurulması gerekir. İnceleme süreci bu mimari modeline göre belirlenir.

2.1.5 Ağ Adli Bilişimi

Ağ adli bilişimi bilgisayar ağ trafiğinin yasal delil bulma veya saldırı tespit amacı ile izleme ve analiz işlemlerinin yapılmasıdır [11]. Adli bilişimin diğer alanlarından farklı olarak, ağ araştırmaları uçucu ve dinamik bilgilerle uğraşır. Ağ trafiği iletilir ve sonra kaybolur, bu yüzden ağ adli bilişimi genellikle proaktif bir soruşturmadır [5].

Ağ adli bilişimi bir ağ trafiğinin yakalanması, yakalanan ağ trafiğinin analizi, aktarılan dosyaları yeniden birleştirmek, anahtar sözcük aramak ve e-postalar veya sohbet oturumlarında insan iletişimini ayrıştırmak gibi görevleri içerebileceği gibi güvenlikle ilgili olarak bir ağın anormal trafik için izlenmesini ve izinsiz girişlerin tespit edilmesini de içerebilmektedir.

2.2 Mobil Cihazlarda Adli Bilişim ve Aşamaları

Adli bilişim, bilgisayarlarda veya dijital depolama aygıtlarında bulunan dijital verilerin yasalara uygun olarak hakkındaki gerçekleri tanımlama, koruma, kurtarma, analiz etme ve sunma bilimidir [5]. Bilgisayarlar mobil cihazlardan donanım ve yazılım açısından farklıdır

fakat gün geçtikçe işlevleri giderek daha fazla benzerlik göstermektedir. Aynı işletim sistemine sahip birçok mobil cihaz uygulamalarında büyük farklılıklar gösterebilir, bunun sonucunda çok sayıda dosya sistemi ve yapı meydana gelir. Mobil cihazların yapısal farklılığı, inceleme metotlarının farklılığı, kullanım oranının artmasıyla birlikte, bu cihazların incelenmesi için adli bilişimin bir alt dalı olarak mobil adli bilişim dalı ortaya çıkmış ve süreçleri tanımlanmıştır [12].

Son yıllarda, cep telefonu ve diğer mobil cihazlardan gelen verileri inceleme taleplerinde kayda değer bir artış olmuştur [6]. Bu cihazlardan gelen verilerin incelenmesi ve çıkarılması, adli incelemeciler için çok sayıda zorluklar içermektedir. Bu zorluklar aşağıda verilmiştir.

Ticari olarak piyasada bulunan çok çeşitli mobil cihazların yanı sıra, bu aygıtlar çeşitli tescilli işletim sistemleri, dosya sistemleri, uygulamalar, hizmetler ve çevre birimleri kullanmaktadır. Bu cihazların her biri, mevcut adli inceleme yazılım araçları tarafından farklı alanlara kadar desteklenebilir veya hiç desteklenmeyebilmektedir.

Mobil cihazlarda bulunan veri türleri ve kullanılma biçimleri sürekli olarak gelişmektedir. Akıllı telefonlara olan talep ile bu cihazların tam işlevsel mini bilgisayar halini alması, potansiyel olarak çok daha fazla alakalı veri içerdiğinden yalnızca telefon defterini, arama geçmişini, kısa mesajları, fotoğrafları, takvim girişlerini, notları belgelemek yeterli değildir. Her geçen gün artan sayıda yüklü uygulamanın verisi, mevcut adli inceleme yazılım çözümleri tarafından otomatik olarak çözümlenemeyen zengin bilgi içerebilir.

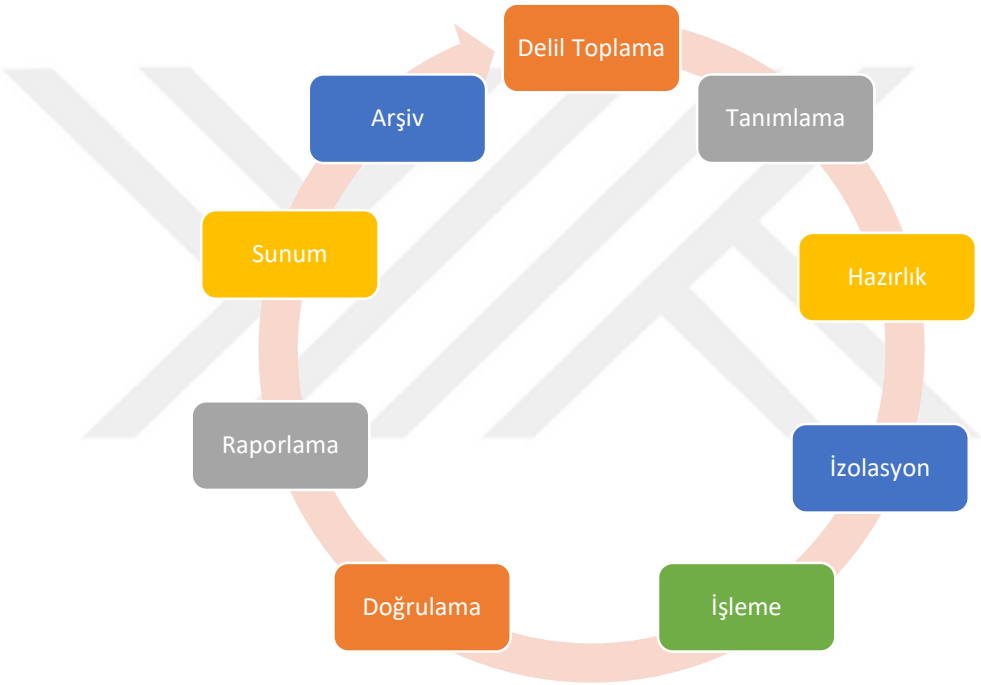
Cep telefonları ve diğer mobil cihazlar, hücresel ve diğer ağlarla radyo, Bluetooth, kızılötesi ve kablosuz (WiFi) ağı üzerinden iletişim kurmak üzere tasarlanmıştır. Verileri telefonda korumak için, çevredeki şebekelerden telefonun izole edilmesi gereklidir. Bu her zaman mümkün olmayabilir ve izolasyon yöntemleri başarısızlıkla sonuçlanabilmektedir.

Mobil cihazlar, çeşitli dahili, çıkarılabilir ve çevrimiçi veri saklama kapasitelerini kullanmaktadır. Çoğu durumda, istenen verileri mobil cihazdan ve ilgili veri depolama ortamından ayıklamak ve belgelemek için birden fazla araç kullanmak gereklidir. Bazı durumlarda, cep telefonlarını incelemek için kullanılan araçlar çelişkili veya hatalı bilgi verebilir. Bu nedenle, mobil cihazlardan alınan verilerin bütünlüğünü doğrulamak önemlidir. Mobil cihazlar tarafından saklanan veri miktarı, geleneksel bilgisayar sabit disklerinin

depolama kapasitesine kıyasla küçük olsa da, bu cihazların depolama kapasitesi büyümeye devam etmektedir.

Bu sebeplerden ötürü, mobil cihazlardan verilerin çıkarılması ve dokümantasyonu için uygun yöntem ve metotların geliştirilmesi son derece önemlidir. Mobil cihaz teknolojisi gelişmeye ve değişmeye devam ettikçe bu süreçler periyodik olarak gözden geçirilmelidir.

Şekil 2.2'de mobil cihazlar için geçerli olan adli bilişim süreci aşamaları adımları gösterilmiştir [13].



Şekil 2.2. Mobil cihazlarda adli bilişim aşamaları

2.2.1 Delil Toplama Aşaması

Delil toplama aşaması inceleme talebinin ele alındığı aşama olarak tanımlanır. Delil toplama aşaması genellikle mülkiyet bilgilerini ve mobil cihazın olaya karıştığı olayı belgelemek üzere istek formu doldurulmasını, evrak alımını ve başvuranın aradığı bilgi türü ile ilgili genel bilgilerin belirtilmesini içerir.

İncelemenin bu safhasında önemli olan her inceleme için kendine özgü hedeflerin geliştirilmesidir. Bu yalnızca incelemecinin hedeflerini açıklığa kavuşturmak ve belgelemekle kalmaz, aynı zamanda incelemelerin özelliklerine göre ayrılmasında yardımcı

olur ve incelenen her bir cihaz için inceleme sürecinin dokümantasyonunu başlatır. Birçok ajans ve kuruluş, muayene için mobil cihaz alımını belgelemek üzere bir form kullanmaktadır.

2.2.2 Tanımlama Aşaması

İnceleme uzmanı, her bir mobil cihaz incelemesinde aşağıdakileri tanımlamalıdır:

- Cihazın inceleme için yasal yetkisi
- İnceleme amaçları
- Cihaz (lar) için marka, model ve tanımlama bilgisi
- Çıkarılabilir ve harici veri saklama alanı

2.2.2.1 Yasal Otorite

Mobil cihazlardan alınan verilerin araştırılmasını kapsayan içtihat hukuku neredeyse sürekli değişmektedir. İnceleme uzmanının cihazın incelenmesinden önce, cihazın araştırılması için yasal otoritenin varlığını ve aramaya ilişkin kısıtlamaların belirlenmesinin belgelenmesi zorunludur.

Ülkemizde uygulanan ceza hukukuna göre mobil cihazlarda adli bilişim yöntemlerine ilişkin özel bir durum yoktur. Adli Bilişime ilişkin olan hükümler ise CMK 134 maddesine göre "Kişisel Verilerimiz üzerinde sahip olduğumuz hak, ulusal ve uluslararası normlarda bireyin temel hak ve özgürlükleri arasında yer almakta ve korunmaktadır. Bu nedenle bilgisayarlar gibi elektronik aygıtların aranması veya bu aygıtlara el konulması söz konusu olduğunda bu müdahalenin ancak hâkim kararı ile yapılması gerektiği vurgulanmaktadır."

Bir inceleme yapılacağı zaman aşağıdaki hususlara dikkat edilmelidir.

- Mobil cihaz bir emir uyarınca araştırılıyorsa, inceleme uzmanı kişi arama emrinin sınırlamalara dikkat ederek inceleme yapmalıdır.
- Cihaz bir kişinin rızası gereği araştırılıyorsa, araştırma kişinin belirlediği sınırlar içinde yapılıyor ise (örneğin yalnızca arama geçmişini inceleme izni gibi) incelemeden önce onayın hala geçerli olup olmadığını belirlemelidir.

- Cihaz tutuklama olayıyla ilgili olarak araştırılıyor ise, bu alandaki mevcut içtihadın sürekli değişebilmesi bazen de yetersiz kalabilmesi durumuna karşılık inceleme yapan kişinin özellikle temkinli davranması gerekmektedir.

Bir cep telefonunun araştırılması hususunda yasal merci ile ilgili özel sorular bilgili bir savcıya ya da bilgili bir hukuk danışmanına sorulmalıdır.

Bazı durumlarda, bir arama emrinde veya rızasında ifade edilen bir aramanın özellikleri için belirtilen şartların, mevcut adli araçların yeteneklerinin ötesine geçebilir. Örneğin, bir arama emri arama geçmişi ve belirli bir tarih aralığındaki mesajlar için bir cep telefonunun veya diğer mobil cihazın aramasını sınırlarsa, çoğu adli araç, incelemecinin bir veri aralığını bir tarih aralığında yalnızca o veriyle sınırlandırmasına izin vermez. Bu durumda bir telefondaki tüm veriyi elde etmek ve bu veriden arama emrinde belirtilen veriyi ayıklamak geniş çaplı bir arama gibi gözükebilir. Bu nedenle, arama emrini hazırlarken veya bir cihazı aramak için onay almak için bu tür sınırlamaları belirtmek önemlidir.

2.2.2.2 İnceleme Amacı

Herhangi bir mobil cihazı incelemek için kullanılan genel süreç mümkün olduğunca tutarlı olmalıdır. Ancak her telefonun inceleme amacı önemli ölçüde farklı olabilir. Herhangi bir adli bilişim laboratuvarının, her vakada kanıtsal değeri gösteren verileri içeren her cep telefonunu inceleme olanağı, kapasitesi ya da kapasitesi olması mümkün olmayabilir. Bu nedenle, verilen herhangi bir cep telefonu için hangi seviyedeki incelemenin uygun olduğunu belirlemek yararlı olabilir.

Burada iki önemli husus vardır; ilki verilerin belgelendirilmesinden kimin sorumlu olacağı, ikincisi ise incelemenin derinliğinin ne kadar olacağıdır. İnceleme için laboratuvara gönderilen bu telefonlardan, davanın koşullarına göre farklılıklar olacaktır.

Belirgin bir değere sahip olan hedeflenen verilerin çıkarımı amacıyla, incelemeye cep telefonunun küçük bir alt kümesi sunulabilir. Resimler, videolar, arama öyküsü, kısa mesajlar veya diğer belirli veriler gibi özel olarak hedeflenen veriler, sorgulanmada önemli olabilirken, diğer kayıtlı veriler alakasız olabilir. Ayrıca yasal kısıtlamalar nedeni ile de verilerin yalnızca belirli bir alt kümesinin incelenmesi de gerekebilir. Her durumda, incelemenin kapsamının sınırlandırılması, muhtemelen verilerin çıkarılmasını ve belgelenmesini daha hızlı olmasını sağlayacaktır.

İncelemenin amacı, silinmiş verileri telefon belleğinden kurtarmak olabilir. Bu genellikle yalnızca, verileri fiziksel veya dosya sistemi düzeyinde ayıklayabilen bir araç mevcutsa mümkündür. Böyle bir araç mevcutsa inceleme, veri kopyalama, hex kod çözme ve SQLite veri tabanlarının incelenmesi gibi geleneksel bilgisayar adli yöntemlerini içerecektir. Bu nedenle inceleme süreci zaman alıcı ve teknik olarak karmaşık bir süreç olabilir.

İncelemenin amacı, telefonu incelemek için hangi araç ve tekniklerin kullanıldığı konusunda önemli bir fark yaratabilir. Başlangıçta incelemenin amacının belirlenmesi için harcanan zaman ve çaba inceleme sürecine verimlilik katabilir. Bu tür durumlar eğitimde ele alınmalı ve inceleme için cep telefonlarının ilk gönderimi ile ilgili triyaj süreci bireysel koşullara ve davanın ciddiyetine dayandırılmalıdır.

2.2.2.3 Bilgi Edinme, Modelleme ve Belirleme

Herhangi cep telefon incelemesinin bir parçası olarak, telefonun kendisi için tanımlayıcı bilgilerin belgelendirilmesi gerekir. Bu, denetleyicinin belirli bir telefonu daha sonra tanımlamasına ve hangi araçların telefonla çalışabileceğine ilişkin karar vermeye yardımcı olur. Çünkü adli bilişim araçları telefonun markasına ve modeline dayanarak telefon listelerini sağlarlar. Tüm telefonlar için, üretici, model numarası taşıyıcı ve cep telefonuyla ilgili mevcut telefon numarası tanımlanmalı ve belgelendirilmelidir. İlgili cep telefonu teknolojisine bağlı olarak, mevcutsa, ek tanımlayıcı bilgiler de belgelendirilmelidir.

2.2.3 Hazırlık Aşaması

İnceleme yapan kişi sürecin tanımlama aşamasında, telefon incelemesi için önemli bir hazırlık yapmıştır. Hazırlık aşamasında ise, incelenecek mobil cihaz için inceleme sırasında izlenecek metotlar belirlenir ve kullanılacak araçların seçimi yapılır. Bu aşama ayrıca tüm ekipmanların, kabloların, yazılımların ve sürücülerin hazırlanması sürecini de içerir. Eğer kullanılacaksa medya ve iş istasyonu inceleme için hazır hale getirilir ve kullanılacak araçların mümkünse en son sürümü temin edilir.

Mobil cihazın markası ve modeli tanımlandıktan sonra, inceleme uzmanı telefondan istenen verileri çıkarma kabiliyetine sahip mevcut araçların olup olmadığını belirlenir. Phonescoop.com ve mobileforensicscentral.com gibi kaynaklar, cep telefonları hakkındaki

bilgileri belirlemede ve belirli telefonlardan verileri çıkarmak ve belgelemek için hangi araçlar kullanılabileceğini bulmak için çok faydalı olabilir. SEARCH araç çubuğu (www.search.org adresinden ücretsiz olarak indirilebilir), cep telefonu incelemeleri için ek ve düzenli olarak güncellenen kaynaklar içermektedir.

Uygun Araçları Seçimi ve Özellikleri: Bir mobil cihazın incelenmesi için seçilecek araçlar, incelemenin amacı, incelemeden sorumlu kuruluş için mevcut olan kaynaklar, incelenecek cep telefonunun tipi ve herhangi bir harici hafıza birimi varlığı gibi unsurlara göre belirlenir.

Piyasada, incelemecinin karşılaşacağı ve işleme koyması gereken tüm mobil telefon modelleri ve diğer mobil cihaz modellerinden tüm verileri almak için yeterli olan bir araç mevcut değildir. Ancak, piyasada telefonda bulunan bilgilerin manuel olarak çıkartılmasının ve dokümantasyonun yapılabileceği birçok telefon vardır. Pazardaki çeşitli cep telefonundan veri çıkarma araçları, mevcut olan geniş ve değişen çeşitli cihazlar nedeniyle farklı telefonları işlemek için farklı yeteneklere sahiptir.

Ayrıca, telefonlardan veri çıkarımının tanımlanmasında yazılım üreticisinden yazılım üreticisine farklar bulunmaktadır. Bu nedenle, satıcının belirli bir aracın yetenekleri ile ilgili tanımları nasıl kullandığını bilmek önemlidir.

Mobil cihaz incelemesinde hazırlık aşaması çok önemlidir. İncelemeye uygun araçların özelliklerinin bilinip duruma, telefona ve aranan veriye ilişkin en uygun araç veya araçların seçilmesi bu aşamada yapılır. Uygun aracın seçimi için detaylı bilgi Mobil Cihazlarda Kullanılan Adli Bilişim Yazılım ve Donanımları Başlığı altında bulunmaktadır.

2.2.4 İzolasyon Aşaması

Cep telefonları şebekeler vasıtasıyla iletişim kurmak üzere tasarlanmıştır. Bu nedenle, bu iletişim kaynaklarından cihazın izolasyonu incelemeden önce önemlidir. Bundan başka diğer ağlara Bluetooth, kızılötesi ve kablosuz (Wi-Fi) ağlar aracılığı ile bağlanırlar. Telefonun izolasyonu, gelen aramaları ve kısa mesajları engellemek, bir "kill sinyali" yoluyla uzaktan erişim veya uzaktan silme yoluyla verilerin potansiyel olarak yok olmasının veya mevcut verilerin yanlışlıkla üzerine yazılması olasılığını ortadan kaldırmak için yapılan işlemlerdir. Bu işlem ile yeni aramalar ve metin mesajları geldiğinde var olan verinin üzerine yanlışlıkla veri yazılma ihtimalinin önüne geçilir. Telefon ağdan izole edildiğinde, inceleme

uzmanı yanlışlıkla sesli mesaja, e-maile, internet tarama geçmişine ya da cihazın kendisinden ziyade servis sağlayıcısının ağında depolanmış olan diğer verilere erişemez.

Cep telefonunun izolasyonu, bu amaç için özel olarak tasarlanmış olan Faraday çantası veya radyo frekanslı koruyucu bezlerin kullanımı ile gerçekleştirilebilir. Kundak kutuları veya birkaç katman folyosu gibi diğer mevcut ürünler de bazı cep telefonlarını izole etmek için kullanılabilir. Bununla birlikte hem resmi hem de gayri resmi faraday yöntemleri ve cihazları başarısız sonuçlar verebilir.-(Katz, 2010). Bu yalıtım yöntemleriyle ilgili bir diğer sorun ise, bu yöntemler kullanılırken telefonla çalışmanın zor ya da imkansız olmasıdır, bunun nedeni telefonu görünmüyor ya da telefonun tuş takımıyla çalışılamıyor olmasıdır. Faraday çadırları, odaları var olsa da maliyetleri çok yüksektir. Bu gibi cihazların kullanımı birçok organizasyon için yasadışıdır bir organizasyon için bu tür cihazların kullanımının yasal olduğunu doğruladıktan sonra uygulanmalıdır.

Bir diğer uygun seçenek, cep telefonunu radyo frekanslı koruyucu bezde sarmak ve ardından Telefonu Uçak moduna geçirmektir (Bağımsız, Radyo Kapalı, Bekleme veya Telefon Kapatma Modu olarak da bilinir). Bir telefonun Uçak moduna nasıl alınacağına ilişkin talimatlar, cep telefonu üreticisinin özel markası ve modeli için üreticinin kullanım kılavuzunda bulunabilir.

GSM cep telefonları için, izolasyon, bir SIM ID Klonunu yaratarak ve kullanarak başarılabilir. Bir SIM Kimliği Klonlaması, cep telefonunun SIM Kartının tamamen kopyalanmış bir kopyası değil, orijinal SIM'den yalnızca ICCID ve IMSI içeren bir muayene dosyasının yarattığı SIM Karttır. Bu, telefonun çevredeki cep telefonu şebekelerine bağlanmasına veya tanınmasına izin verilmeden cep telefonu içeriğinin incelenmesine olanak tanır. Cellebrite UFED, XRY / XACT ve Adli SİM Klonlayıcı da dahil olmak üzere SIM ID Klonunu oluşturmak için kullanılabilecek çeşitli ticari araçlardır.

Tüm telefonların uçak modu veya eşdeğeri yoktur ve bazen en kusursuz izolasyon yöntemleri bile başarısız olabilir. Buna ek olarak, bazı cihazlar tarih ve saatlerini cep telefonu şebekesinden alırlar, bu da yalıtım hatalı tarih ve saat bilgisine neden olabilir. Bir hücresel telefon tüm şebekelerden başarılı bir şekilde izole edilmiş olsa bile, alarmlar veya randevu duyuruları gibi otomatik fonksiyonlar ayarlanırsa, kullanıcı verileri hala etkilenebilir. Bu gibi durumlar ortaya çıkarsa, inceleme uzmanı, telefonun izole edilmesine

yönelik girişimlerini ve muayene sırasında herhangi bir gelen çağrı, kısa mesaj veya diğer veri iletiminin gerçekleşip gerçekleşmediğini belgelemelidir.

2.2.5 İşlem Aşaması

Telefon cep telefonundan ve diğer iletişim şebekelerinden ayrıldıktan sonra, telefonun işlenmesi süreci başlar. İncelemenin amacına ulaşmak için uygun araçlar daha önce açıklanan adımlarda tanımlanmıştı. Bu aşama arzu edilen verileri telefondan ayıklamanın gerçekleştiği aşamadır.

Çıkarılabilir veri depolama kartları mümkün olduğunda telefonla ayrı olarak işlenmelidir çünkü cep telefonunun incelenmesi sırasında bu kartlarda depolanan verilere erişmek veri saklama kartındaki verileri değiştirebilir. Yüklü veri depolama / hafıza kartları, telefon incelenmesinden önce cep telefonundan çıkarılmalı ve veri saklama / hafıza kartında saklanan dosyalar için tarih ve saat bilgilerinin değiştirilmemesini sağlamak için normal bilgisayar adli bilişim inceleme yöntemleri kullanılarak ayrı olarak işlenmelidir. Çıkarılabilir bir veri depolama kartını telefonla ayrı olarak işlemek mümkün olmayan durumlarda; örneğin, inceleme sırasında bunun için aletler bulunmadığında veya veri kartı telefona kilitlendiğinde veya şifrelenirse ve telefon olmaksızın veriye erişilmediğinde, telefonun ve kartın işlendiği zamanın belgeleri özellikle önemlidir.

Cep telefonu incelemesinde kullanılan yazılım ve donanım araçlarının sırasına dikkat edilmelidir. Bir cep telefonu incelemesinde kullanılan araçların sırasının düzen içinde olması avantaj sağlar. Bu düzen, inceleme yapan kişinin daha sonraki bir zamanda inceleme sırasında kullanılan araçların sırasını hatırlamasına yardımcı olur. Ayrıca, koşullara bağlı olarak, incelemenin hedeflerine bağlı olarak inceleme sırasında öncesinde veya sonrasında bazı araçlar kullanmak mantıklı olabilir. Örneğin, hedef, silinen bilgileri telefonun fiziksel belleğinden çıkarmak ise, incelemeyi belleğin fiziksel bir dökümü ile başlatmak (bu işlev için araçlar varsa), tek tek dosyaları veya dosya sistemini ayıklamaktan daha mantıklı olacaktır. Telefonun aynı cihazdan birden fazla çıkarım yapılması telefonda elde edilen verilerin şifresinin çözülmesine yardımcı olabilir.

2.2.6 Doğrulama Aşaması

Telefonu işleme aşamasında sonra, inceleme uzmanının telefondan çıkarılan verileri doğrulamak için bir takım düzenlemeleri yapması şarttır. Ne yazık ki, cep telefonu araçlarının yanlışlıkla veya eksik bir şekilde verileri rapor etmesi veya çelişen bilgileri araçlardan birine bildirmesi alışılmadık bir durum değildir. Ayıklanan verilerin doğrulanması birkaç yolla gerçekleştirilmektedir.

Ayıklanan Verilerin Telefondakiler ile Karşılaştırılması: Mobil cihazdan çıkarılan verilerin cihazın kendisinin gösterdiği veriyle eşleştiğinden emin olmak demektir. Bu, araçların telefon bilgilerini doğru bir şekilde raporladığından emin olmanın tek yetkili yoludur.

Hex Temelli Kontrol: Fiziksel veya dosya sistemi çıkarımı destekleniyorsa, geleneksel adli araçlar, sonuçların araç tarafından rapor edilenle tutarlı olmasını sağlamak için verileri elle inceleyerek ve çözdükten sonra verileri doğrulamak için kullanılabilir. Bu yöntem, verileri kontrol etmek için geleneksel adli bilişim yöntemlerini kullanır ancak daha yüksek bir uzmanlık ve deneyim gerektirir. Çeşitli mobil cihazlarda kullanılan, bu yöntemi kullanırken zorluk çıkarabilecek çok çeşitli dosya biçimleri ve kodlama yöntemleri vardır.

Birden Fazla Aracın Kullanımı, Sonuçların Karşılaştırılması: Ayıklanan verilerin doğruluğundan emin olmanın diğer bir yolu, araçtan raporlanan verileri karşılaştırarak cep telefonundan veri ayıklamak ve sonuçları doğrulamak için birden fazla araç kullanmaktır. Tutarsızlıklar varsa, inceleme uzmanı telefondan alınan verileri doğrulamak için başka yollar kullanmalıdır. İki araç bilgileri sürekli olarak rapor etse bile, cihazın manuel olarak incelenmesi yoluyla doğrulama gerçekleştirilmelidir çünkü kullanılan her iki cihazın hatalı bir şekilde raporlanması mümkündür.

Hash Değerlerini Kullanma: Dosya sistemi çıkarımı destekleniyorsa, geleneksel adli araçlar, çıkarılan verilerin çeşitli şekillerde doğrulanması için HASH kullanılabilir. Hash; değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan matematiksel algoritma programıdır ve Adli Bilişim bilim dalının vazgeçilmez doğrulama biçimidir. Adli bilişim uzmanı başlangıçta cep telefonunun dosya sistemini ayıklayabilir ve ardından ayıklanan dosyaları karışık hale getirebilir. Bireysel olarak ayıklanmış dosyalar daha sonra tek tek dosyaların bütünlüğünü doğrulamak için karışık ve orijinallerle karşılaştırılabilir.

2.2.7 Belgelendirme ve Raporlama Aşaması

İncelemenin belgelendirilmesi inceleme süreci boyunca yapılanlarla ilgili eşzamanlı şekilde yapılmalıdır. İnceleme dokümanları, temel bilgilerin kaydedilmesini sağlamak için inceleme sürecinde yardımcı olabilir.

İnceleme uzmanının notları ve dokümantasyonu aşağıdakiler bilgileri içerebilir:

- İncelemenin başlatıldığı tarih ve saat
- Telefonun fiziksel durumu
- Telefonun resimleri, bireysel içerikler (ör. SIM kart ve bellek genişletme kartı) ve tanımlayıcı bilgi etiketi
- Alındığında telefonun durumu (açık ya da kapalı)
- Marka, model ve tanımlayıcı bilgisi
- İnceleme esnasında kullanılan aletler
- İnceleme esnasında hangi verilerin belgelendiği bilgisi

Çoğu cep telefonu inceleme araçları raporlama işlevi içerir, ancak buradaki belge gereksinimleri için yeterli olmayabilir. Bazen, cep telefonu araçları, yanlış ESN, MIN / MDN numaraları, model veya hatalı tarih ve saat verileri gibi yanlış bilgileri bildirebilir. Bu sebeple veri doğrulama aşamasından sonra doğru bilgiyi belgelemek için özen gösterilmelidir.

Süreç, telefondan veri çıkarma, çıkarılan ve belgelendirilen veri türleri ve ilgili tüm bulgular raporlarda doğru bir şekilde belgelenmelidir. İnceleme, mevcut araçları kullanarak istenen verilerin çıkarılmasında başarılı olsa bile, bilgilerin fotoğraflarla ek belgelendirilmesi özellikle mahkeme sunumu amacıyla yararlı olabilir.

Saat Dilimi / Yaz Saati Uygulaması: Telefonun kendisinin yerel saati gösterdiği halde UTC veya diğer standart zaman formatlarında mobil adli yazılım araçları tarafından bildirilebilecek tarih ve zaman damgalarına özellikle dikkat edilmelidir. Çoğu araç, denetleyicinin raporlama amaçlarıyla zaman damgalarını yerel saat dilimine göre ayarlamasına izin verir, ancak bu her zaman geçerli değildir. Saat dilimi ve gün ışığından yararlanma veya standart saat için yapılan ayarlamalar açıklanmalıdır çünkü bu ayrıntılar raporları okurken başkaları tarafından kaçırılabilir veya yanlış anlaşılabilir. Bu durum, araştırmacılar tarafından kaçırılan ilgili veriler veya kanıtlayıcı telefon ile çeşitli adli araçlar

tarafından oluşturulan raporlar arasında bir tarih ve saat çatışması ortaya çıkmasına neden olabilir. Raporda zaman dilimi ayarlamaları yapıldığından veya uygulanmadığından bahsetmek, daha sonrada çıkabilecek karışıklıklara karşı zaman kazanılmasına yardımcı olacaktır.

2.2.8 Sunum Aşaması

Mobil cihazdan çıkarılan ve belgelendirilen bilgilerin açıkça nasıl çıkarıldığı ve belgelendirildiği başka bir araştırmacıya, savcılığa ve bir mahkemeye sunulabilmesi için özenle hazırlanmalıdır. Çoğu durumda, alıcı, çıkarılan verileri daha ileri analiz için başka yazılımlara hem kağıt üzerinde hem de elektronik biçimde sunulması isteyebilir.

İnceleme uzmanı verilerin alıcılar tarafından bilgileri daha iyi anlayabilmesi için, tarih ve saat bilgisi kaynağı, görüntülerden veya diğer veri formatlarından çıkarılan EXIF verisi ile ilgili referans bilgi sunabilir.

Verilerin cep telefonundaki haliyle resimlerinin ya da videolarının olması mahkemeye yarar sağlayabilir. Çıkarılan kısa mesajlar mükemmel birer kanıt olabilir ancak aynı metin mesajlarının resimleri mahkemeye görsel açıdan daha etkili olabilir.

İletişimin ilerlemesinin izleyiciye açıkça gösterilmesi için bir PowerPoint sunumu veya zaman çizelgesi yazılımı ile metin mesajları ve çağrı geçmişi günlüklerinin bir dizi serisini sunmak çok yararlı olur. Bu, bir davaya katılan çok sayıda cep telefonu durumlarda özellikle etkilidir.

2.2.9 Arşiv Aşaması

Ayıklanan ve cep telefonundan belgelenen verilerin korunması, genel sürecin önemli bir parçasıdır. Devam eden mahkeme süreci, gelecekteki referanslar ve kayıt tutma gereksinimleri için verileri iyi bir biçimde tutmak gereklidir. Bazı durumlarda, nihai bir karara varmak yıllar sürebilir ve çoğu ülke, verilerin itiraz durumları için verilerin saklanmasını ister.

Cep telefonu verilerinin çıkartılması ve dokümantasyonunda piyasadaki çeşitli araçların tescilli yapısı gereği, daha sonra kaydedilen verilere erişip erişememe durumu göz önünde bulundurulmalıdır. Mümkünse, orijinal yazılım aracının artık mevcut olmadığı durumlarda

bile verilere daha sonra erişilebilmesi için veriyi hem telifle korunan hem de korunmayan formatlarda standart ortamda saklanmalıdır. Verilerin daha sonraki bir tarihte incelenmesini kolaylaştırmak için aracın bir kopyasını saklamak iyi bir uygulamadır.

2.3 Mobil Cihazlardan Veri Çıkarma Yöntemleri

Bu kısımda 2.2 bölümünde mobil adli bilişim aşamaları olarak anlattığımız aşamalardan işleme aşamasında gerçekleştirilen veri çıkarma işleminin yöntemleri incelenecektir [3,14].

2.3.1 Mantıksal Çıkarım

Mantıksal veri çıkarma mobil bir cihazdan mantıksal depolama nesnelerinin bit bit kopyasının çıkarılması işlemidir. Mantıksal depolama nesneleri dosya sisteminde bulunan dosya ve dizinleri içerir. Veri çıkarma aracı, mobil cihazın işletim sistemiyle iletişim kurar ve bilgi ister. Mantıksal çıkarma, üreticilerin orijinal API'sini (uygulama programlama arabirimi) kullanarak gerçekleştirilir. Veri çıkarma işlemi bu yöntem ile kolay gerçekleşir ve inceleme yapan tarafından daha kolay uygulanabilir. Fakat iyi bir adli bilişim uzmanı fiziksel çıkarımdan daha çok veri elde edebilir.

2.3.2 Dosya Sistem Çıkarımı

Mantıksal bir veri edinimi mobil cihazlar dosya sistemi tarafından kaldırıldığı için silinen verileri üretmez. Android ve iOS gibi popüler işletim sistemlerini çalıştıran mobil cihazlar SQLite veritabanı platformunu kullanarak oluşturulmuştur. Veriler bir mobil cihazdaki SQLite veri tabanında saklandığında ve veriler silindiğinde, verinin üzerine yazılmaz. Veriler bu veri tabanında silindiğinde, genellikle silinmiş olarak işaretlenir ve daha sonra tekrar yazılmasına izin verilir. Bu, bir dosya sisteminin veri edinimi bir mobil cihazın senkronizasyon arabirimi aracılığıyla sağlanırsa silinen verileri kurtarmanın mümkün olacağı anlamına gelir. Mobil cihazdan dosya sistemi çıkarımı, adli denetçinin analizleri, adli bilişim araçları ve komut dosyaları kullanarak gerçekleştirmesine olanak tanır ve dosya yapısını, uygulama verilerini ve web bulgularını gösterir.

2.3.3 Fiziksel Çıkarım

Fiziksel veri çıkarımı, cihazın tüm fiziksel belleğinin (flash bellek) bit bit kopyasının alınmasını gerektiren yöntemdir ve bu metot bilgisayar adli incelemesi ile çok benzerdir. Fiziksel veri çıkarımı cihazdaki tüm dosyalara tam erişim sağlar, silinmiş dosyalara ve veri kalıntılarının incelenmesine izin verir. Mobil cihaz üreticileri, cihazın belleğinin rastgele okumasına karşı emniyetli olduklarından, fiziksel veri edinme veri çıkarma metotlarının en zor olan türüdür. Mobil adli bilişim araç üreticileri fiziksel çıkarımı gerçekleştirmek için, genellikle, mobil cihazın belleğine erişmesine ve çoğu durumda desen kilidini veya şifreleri atlamasına olanak tanıyan özel önyükleme yükleyicileri geliştirir. Fiziksel çıkarım tüm cihazlar için desteklenmemektedir.

Fiziksel teknikler (donanım tabanlı) yoluyla Android veri çıkarma temel olarak iki yöntem içerir, bunlar JTAG ve chip-off teknikleridir. Bu teknikler genellikle uygulanması zor ve soruşturma boyunca gerçek aygıtlarda denemek için büyük hassasiyet ve deneyim gerektirir.

JTAG, aygıt üzerindeki belirli bağlantı noktalarına bağlanarak ve verileri aktararak gerçekleştirilen gelişmiş veri toplama yöntemlerini donanım düzeyinde kullanmayı içerir. Analist, yanlışlık durumunda cihaz hasar görebileceğinden JTAG'yı denemeden önce uygun eğitim ve tecrübeye sahip olmalıdır.

Chip-off, verileri ayıklamak için flaş çiplerden aygıttan çıkarılabilecek başka bir fiziksel edinme türüdür. NAND flaş çiplerinin cihazdan çıkarıldığı ve bilgiyi çıkarmak için incelendiği bir tekniktir. Bu nedenle, bu teknik, cihaz şifre korumalı olduğunda ve USB hata ayıklama etkin olmadığında bile çalışacaktır. Muayene edildikten sonra cihazın normal çalıştığı JTAG tekniğinin aksine, chip-off tekniği genellikle cihazın tahrip edilmesine neden olur, yani incelemeden sonra cihaza NAND flaşın yeniden takılması daha zordur. NAND flaşını tekrar cihaza takma sürecine yeniden top kurma denir ve eğitim ve uygulama gerektirir.

2.3.4 Manuel Çıkarım

Bu yöntemde inceleme yapan kişi telefon hafızasında inceleme yapmak için kullanıcı ara yüzünü kullanır. İnceleme uzmanı her içeriğin resmini çekerek içeriği elde eder. Bu yöntem için işletim sistemine has verileri dönüştürmeyi sağlayacak araçların kullanılmasına

gerek kalmaz. Pratikte bu yöntem cep telefonlarına, PDA'lara ve navigasyon sistemlerine uygulanmaktadır. Dezavantajları, yalnızca işletim sisteminde görünen verilerin geri kazanılabilmesi ve sürecin çok zaman alıcı olmasıdır.

2.4 Mobil Cihazlarda Kullanılan Adli Bilişim Yazılımları

Bu bölümde adli bilişim incelemesinde kullanılabilecek olan adli bilişim yazılımları genel özellikleri ile değerlendirilecektir.

Mobil cihazlar için geliştirilmiş adli bilişim yazılım araçları ile elde edilebilenler, kişisel bilgisayarlarınkinden oldukça farklıdır. Aynı işletim sistemine sahip birçok mobil cihazda bile çok sayıda dosya sistemi ve farklı yapılardan oluşmaktadır. Bu yapılar, mobil adli araç üreticilerine ve inceleyicilere önemli zorluklar yaratmaktadır.

Mobil cihaz incelemesi için geliştirilmiş yazılımılar ile önceki kısımlarda bahsettiğimiz mobil adli bilişim aşamalarını gerçekleştirerek, adli deliller elde edilir. Tablo 2.1' de günümüzde en çok kullanılan mobil adli bilişim inceleme yazılımlarının veri çıkarımını nasıl gerçekleştirdiği, veri doğrulamasında ne tip algoritmalar kullandığı, analiz sonucu elde ettikleri ve tüm inceleme sonucu elde edilen sonuçların raporlama formatları ve ücretsiz veya ticari mi oldukları ile ilgili özellikleri verilmiştir.

Tablo 2.1. Mobil adli bilişim yazılımları kıyaslaması

Özellikler	**Oxygen Forensics**	**Celebrite**	**Paraben**	**MobilEdit**	**Autopsy**	**XRY**
Mantıksal /Fiziksel Veri Çıkarımı	Mantıksal	Mantıksal Fiziksel	Mantıksal Fiziksel	Mantıksal Fiziksel	Mantıksal Fiziksel	Mantıksal Fiziksel
Veri Doğrulaması	MD-5 SHA-1 SHA-256	MD-5 SHA-256	MD-5 SHA-1	MD-5 SHA-1 SHA-256	-	MD-5 SHA-1 SHA-256
Yer imi koyma	+	-	+	-	+	+
Hex Görünümü	+	+	+	+	+	+
Metin Görünümü	+	+	+	+	+	+
Veri Kazıması	-	+	+	-	-	-
Veri Kurtarma	+	+	+	+	-	+
Resim Görüntüleme	+	-	+	+	+	+

Tablo 2.1. Mobil adli bilişim yazılımları kıyaslaması (Devamı)

PC'den Yedek Dosyaları Okuma	+	+	+	+	+	+
Rapor Formatları	CSV, HTML, PDF, XLS, XML	CSV, HTML, PDF, XLS, XML	CSV, HTML, PDF, XLS, XML, TXT	HTML, PDF, XLS, XML	TXT, XLS, HTML	TXT, CSV, XLS,
Ticari/Ücretsiz	Ticari	Ticari	Ticari	Ticari / Ücretsiz sürümleri mevcut	Ücretsiz	Ticari

2.5 Yapılan Çalışmalar

Adli bilişim, bilgisayarla ilgili kanıtları mahkeme tarafından yasal olarak kabul edilebilir bir şekilde tanımlama, toplama, koruma, analiz etme ve sunma süreci olarak tanımlanan bir bilim dalıdır [3] . Mobil cihazların kullanım oranlarının artışıyla orantılı olarak mobil cihaz incelemesi ile ilgili yapılan çalışma alanı yelpazesi de genişlemiştir. Bu bölümde Mobil adli bilişim alanında yapılan çalışmalar incelenecektir. Mobil adli bilişim, adli bilişimin mobil cihazlar üzerindeki veri çıkarma, inceleme ve analiz etme gibi süreçleri içerir ve incelemenin başarılı olabilmesi için bu süreçlerin iyi modellenmesi gerekmektedir. Literatürde bununla ilgili pek çok çalışma bulunmaktadır.

Jansen ve Ayers, 2007'de cep telefonu adli bilişimi rehberi adlı çalışmasında bu modellemenin temelini atmıştır. Bu model koruma, veri edinme, inceleme & analiz ve raporlama aşamalarından oluşmaktadır [15]. Lin ve arkadaşları bu modeli esas alarak başlangıç, hazırlık, operasyon ve raporlama evresi olmak üzere dört aşamadan oluşan başka bir model önermişlerdir. Bu modelde operasyon evresi en önemlisidir ve toplama, analiz ve adli bilişim(forensics) olmak üzere üç aşamadan oluşmaktadır. [16]çalışmasında bu iki model kıyaslanmıştır ve sonuç olarak Lin tarafından önerilen modelin, dijital delillerin meşruluğu göz önüne alındığından daha güvenilir olduğunu iddia etmişlerdir.

Murphy çalışmasında, cep telefonlarının ve diğer mobil cihazların incelenmesi talebinin artmasıyla birlikte, bu cihazların incelenmesi süreçlerinin geliştirilmesi ihtiyacının ortaya çıktığını ifade etmiştir [13]. Her bir cihazın incelenmesiyle ilgili ayrıntılar farklı

olabilmesine rağmen, tutarlı inceleme işlemlerinin kabul edilmesi, inceleme uzmanına her bir telefondan elde edilen kanıtların belgelenmesine ve sonuçların tekrarlanabilir ve savunulabilir olmasına yardımcı olacağını savunmuştur. Geliştirilen süreç dokuz aşamadan oluşmaktadır, bunlar; delil toplama, tanımlama, hazırlık, izolasyon, işleme, doğrulama, raporlama, sunum ve arşiv aşamalarıdır. Oluşturduğumuz tez çalışmasındaki adli bilişim süreçleri bu çalışma temel alınarak oluşturulmuştur.

Bu konuyla ilgili başka bir çalışma da 2016 yılında Sadıq ve arkadaşları tarafından yapılmıştır [17]. Bu çalışmada daha önce kullanılan mobil adli bilişim inceleme modellerinin bazıları gözden geçirilmiş ve mevcut modellerin karşılaştırılması gerçekleştirilmiştir. Ayrıca veri çıkarmanın ve soruşturmanın önemli aşamaları tanımlanarak yeni bir birleşik mobil adli bilişim incelemesi modeli önerilmiştir. Bu model, daha önceki eserlerden esinlenmiştir ve süreç modelinin tasarımı sırasında NIST'in mobil cihaz incelemesi ile ilgili yönergeler de izlenmiştir. Önerilen modelin avantajı, önceki modellerin ekstra ve tekrarlanan evreleri ve aşamaları birleştirilmesi ve fazlar daha özlü bir noktaya getirilmesidir.

Ali ve arkadaşları çalışmalarında [18], mobil adli bilişim alanı için bir yaklaşım geliştirmiştir. Geliştirilen yaklaşım, mobil adli bilişim ortak kavramlarını tanımlamaya katkıda bulunmaktadır. Ek olarak, inceleme sürecinin basitleştirilmesini ve inceleme ekiplerinin özel adli bilgileri yakalayıp yeniden kullanmalarını sağlar, böylece eğitim ve bilgi yönetimi faaliyetlerini destekler. Ayrıca, mobil adli bilişim alanındaki zorluk ve belirsizliği azaltır. Bunların sağlanması için yazarlar sekiz adımlı bir mobil adli inceleme modeli geliştirmişlerdir.

Adli bilişimde kullanıcı veri bütünlüğünün korunması ilkesi çok önemli bir kavramdır ve delilin korunması değiştirilmemesi esas teşkil eder. Fakat mobil cihazlarda incelemenin gerçek anlamda gerçekleşmesi için cihazın root edilmesi gerekmektedir. Veri çıkarma işleminden önce cihazın root edilmesi, veri elde etme sürecini kusurlu kılar ve adli bütünlüğe karşı bir tehdit oluşturabilir. Pantaleon root işleminin android mobil cihazların kullanıcı veri bütünlüğü üzerindeki etkisini araştırmak için bir çalışma gerçekleştirmiştir [19]. Bu çalışmada, bir cihaz veri çıkarımından önce root edildiğinde kullanıcı verileriyle ilgili veri bütünlüğü sorunlarını denemek ve araştırmak için araştırmalar gerçekleştirmiştir. Sonuç olarak, root erişiminin etkinleştirildiği zaman kullanıcı verilerinde hiçbir değişikliğin gözlenmediğini ortaya konmuştur. Çalışma ayrıca, veri bütünlüğünü korumak için mobil cihazlardan verilerin fiziksel olarak alınması sırasında izlenebilecek bir çerçeve önermiştir.

Mobil cihazlarda uygulama temelli incelemelerde root işlemi elzemdir. Bu tip incelemelerin yapıldığı pek çok çalışma bulunmaktadır. Wu ve arkadaşları çalışmalarında [20] WeChat anlık mesajlaşma uygulamasının android cihaz üzerinde adli incelemesini yapmışlardır. Kullanıcı verilerinin elde edilmesi, şifrelenmiş veri tabanı kodunun çözülmesi, yapılan görüşmelerinin incelemesi yapılmıştır. Uygulamanın güncellemeleri ile değişen versiyonlarınında incelemesi gerçekleştirilmiştir. Yükseltme genellikle veri depolama yapısında ve veri koruma önlemlerinde olası değişiklikler anlamına gelir. Bu tür problemler, diğer Android uygulamalarının adli alanlarında da görülür. Bu nedenle, çalışma uygulamaların yeni gereksinimlerini karşılamak için Android uygulamalarının ters analizi ve veri koruma mekanizmaları sürekli olarak incelenmesi gerektiğini savunmuştur. Çalışmanın amacı mobil adli inceleme yapan kişilere referans olmaktır.

Başka bir uygulama analizi Ovens ve Morison tarafından gerçekleştirmişlerdir [21]. Çalışmanın amacı Kik messenger tarafından en son iOS sürümüne yüklenmiş aygıtlarda ve iTunes yedekleme dosyalarında oluşturulan veya değiştirilen bulgulara erişip yorumlayarak adli bilişim analizi için referans olmaktır. Çalışma sonucunda oluşturulan veya değiştirilen bulguların ayrıntılı bir açıklaması sağlanmıştır. Denemelerden elde edilen sonuçlar, silinen resimlerin yalnızca cihazdan kurtarılamayacağını değil, aynı zamanda Kik sunucularından da bulunabileceğini ve indirilebileceğini göstermiştir. Çalışmadan elde edilen sonuçlar, adli bilişim araştırmacıları ve adli bilişim yazılımı geliştiricileri tarafından kullanılabilir.

Gregorio ve arkadaşları [22]çalışmasında ise windowsphone üzerine kurulu olan anlık mesajlaşma uygulaması olan Telegram Messenger'ın adli analizini gerçekleştirmiştir. Çalışma, bulguların nasıl yapılandırıldığı ve uygulama tarafından oluşturulan kullanıcı, sohbet ve konuşma verilerinin, verilerden ilgili verilerin çıkarılması amacıyla düzenlenmesine odaklanırken, adli bilişim analizine genel bir bakış sunmaktadır. Çalışmada bir analiz metodu önerilmiş ve uygulama analizi bu metodolojiye göre gerçekleştirilmiştir. Uygulama en çok kullanılan mobil adli bilişim yazılımları tarafından tanınmadığı için bu uygulamaya ilişkin analiz yapacak araştırmacılara referans sağlamaktadır.

Anglano [23] çalışmasında android cihazlar üzerinde Whatsapp Messenger uygulamasının analizini gerçekleştirilmiştir. Yapılan çalışma sonucunda Whatapp uygulamasının cihazlar üzerinde bıraktığı bulguların analistler tarafından nasıl ilişkilendirileceğini, yorumlanacağını ve çözümleneceğini ortaya konulmuştur. Ayrıca veri çıkarma araçlarının karşılaştırılması da gerçekleştirmiştir.

Dezfouli ve arkadaşları yaptıkları çalışmada [24] sosyal ağ uygulamalarının android ve iOS cihazlar üzerinde incelemesini gerçekleştirmişlerdir. Cihazlara Facebook, Twitter, LinkedIn ve Google+ uygulamaları yüklenmiş, bu uygulamalar üzerinde belli başlı davranışlar gerçekleştirilmiştir. Sonrasında ise cihazlarda bir adli soruşturmada önemli olabilecek veriler aranmıştır. Bu çalışma yapılırken Martini ve Choo'nun [25] geliştirdiği bulut hesaplama için adli bilişim yapısı temel alınmıştır.

Yusoff ve arkadaşları ise Firefox işletim sitemi yüklü bir mobil cihaz üzerinde bulunan sosyal ağ ve anlık mesajlaşma uygulamaları üzerine bir çalışma [26] yapmışlardır. Bu çalışmada, her biri FxOS dahili telefon ve uçucu hafızadan yirmidört imaj alınmıştır. Elde edilen imajlar daha sonra detaylı bir şekilde analiz edildi. Sonuç olarak, adli bulguların çoğunun, geçici bellekte kaldığı gözlemlenmiştir. Bu çalışma aynı zamanda FxOS telefonundaki belleğin şifrelenmediğini, dolayısıyla adli bilişim araçları ile okunabilir olduğunu göstermiştir. Bu nedenle, özellikle Facebook ve Twitter hizmetlerinde sosyal medya hesabı kimlik bilgileri kurtarılabilmiştir. Bu araştırmadan elde edilen diğer sonuç, FxOS uygulamalarının mobil web'deki karşılığı ile aynı şekilde davranmasıydı. Bu nedenle, aynı hizmetler, hem uygulamada hem de mobil web platformunda analiz edildiğinde aynı adli deliller alınabilmektedir. Öte yandan, elde edilen imajların analizi, uygulama kalıntılarının, kaldırıldıktan sonra FxOS cihazında kaldığını göstermiştir. Uygulama klasörlerinden ve tarayıcı geçmişinden kalan veri kalıntısı ve araştırmaya katma değer eklenecek ve daha birçok bilgi başarılı bir şekilde geri alınabilecektir.

Mobil adli bilişim ile ilgili başka bir çalışma alanı da Cahyani, ve arkadaşları tarafından yapılmıştır [27]. Çalışmalarında bulut depolama hizmeti ve iletişim uygulamalarını kullanan terörizm araştırmalarında mobil adli bilişimin rolünü araştırmışlardır. Özellikle, Android ve Windows cihazlarında kontrol edilen bir dizi deneme kullanarak, kanıtlayıcı bulguları istemci cihazlardan kurtarmak için mobil adli bilişim tekniklerinin nasıl kullanılabileceğini göstermişlerdir. Çalışmada, üç simülasyon senaryosu vardır: bilgi yayılımı, bilgi gizleme ve iletişim. Denemelerde üç popüler bulut uygulaması (Google Drive, Dropbox ve OneDrive), beş iletişim uygulaması (Messenger, WhatsApp, Telegram, Skype ve Viber) ve iki e-posta uygulaması (GMail ve Microsoft Outlook) kullanılmıştır. Kanıtlayıcı verileri, mobil adli bilişim ve ağ izleme araçlarını kullanarak toplamış ve analiz etmişlerdir. Delil bulgularının korelasyonu, yasadışı mobil cihaz kullanımını ortaya çıkarmak için destek olmuştur. Bu

çalışma aynı zamanda, Android'in daha kanıtlayıcı değeri sunduğu, Android ve Windows cihazları arasında elde edilen kanıtların kapsamını vurgulamaktadır.

Daryabar ve Dehghantanha çalışmasında [28], Android ve iOS cihazlarında OneDrive, Box, GoogleDrive ve Dropbox uygulamalarının adli incelenmesini gerçekleştirmişlerdir. Bu makalede hem Android hem de iOS platformlarında (en popüler mobil işletim sistemlerinden ikisinde) dört popüler bulut istemci uygulaması olan OneDrive, Box, GoogleDrive ve Dropbox'ı incelemişlerdir. Giriş, yükleme, silme ve dosya paylaşımı sırasında üretilen bilgiler gibi adli çıkarımların artifactleri tespit etmektedirler. Bu çalışma ile elde edilen bulgular adli araştırmacılara ve uygulayıcılara, Android ve iOS platformlarında bulut istemci uygulamalarının gerçek dünyada incelenmesine yardımcı olması bekleniyor.

Azfar, Choo ve Liu, Android cihazlar ve uygulamaların popülerliğinden dolayı, Android adli bilişim üzerine çalışmışlardır [29]. Sohbet ve IP üzerinden ses (VoIP) gibi iletişim uygulamaları, suçluları da içeren mobil cihaz kullanıcıları tarafından kullanılan popüler bir uygulama kategorisidir. Bu nedenle, Android iletişim uygulamalarını içeren adli çıkarların eserlerini özetleyen bir taksonomi, bu tür uygulamalardan gelen kanıtlayıcı materyallerin zamanında çıkarmak ve analizini kolaylaştıracaktır. Bu çalışmada, Android telefon imajlarının mantıksal olarak çıkarılmasında yaygın olarak kullanılan bir mobil adli araç olan XRY kullanılarak toplanana 30 popüler Android iletişim uygulaması incelenmiştir. İletişim listeleri ve mesajların kronolojisi gibi çeşitli bilgiler toparlanmıştır. Son olarak, otuz iletişim uygulamasının çalışmasında tanımlanan bulgular taksonomi kullanılarak özetlenmiştir.

Ogazi-Onyemaechi ve arkadaşlarının [30] yaptıkları çalışmada, bir Samsung Galaxy S2 i9100 Android telefondan kanıtların kurtarılmasında mobil adli veri kurtarma araçlarının etkinliği araştırılmaktadır. Çalışmada Phone image carver, Access data FTK, Foremost, Diskdigger ve My File forensic araçlarını kullanarak kurtarılabilecek veri miktarını belirlemeye çalışılmıştır. Elde edilen bulgular, çalışılan araçların geri kazanım kapasiteleri arasındaki farkın yalnızca kendi uzmanlık alanlarındaki uygunluklarını yansıttığını göstermektedir. Bir mobil cihazdan veri kurtarmak için tek adli bilişim aracının kullanılmasının uygun olmadığı ileri sürmektedir.

Quick ve Choo yaptıkları çalışmada [9] mobil cihazlardaki depolama kapasitesindeki artışla, kanıt ve istihbarat analizi için mevcut veri hacminde devam eden artışı

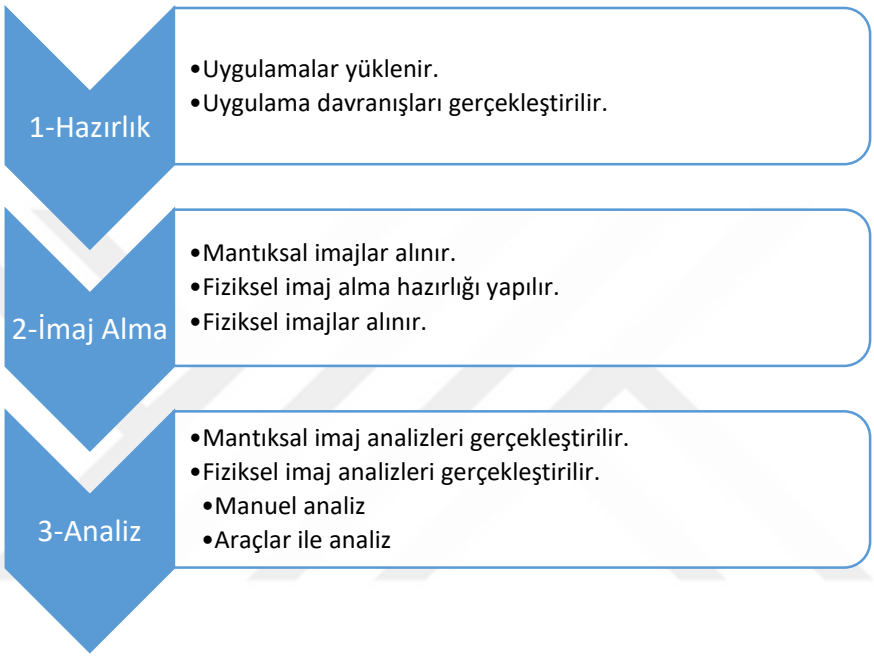
vurgulamışlardır ve Dijital Adli Zeka Analiz Döngüsünü (DFIAC) önerilmiştir. Adli vakalarda mobil cihazlardan çıkarılan verilerde olası çoklu cihaz çapraz bağlantıları ile bir dizi suçla ilgili bilgi potansiyeli bulunduğunu ifade etmişlerdir. Bir Avustralya yasa uygulayıcı kuruluşundan alınan mobil cihaz çıktıları kullanılarak, mobil cihazlardan adli olarak elde edilen veri hacmindeki bilgilerin yerini saptamak için önerdikleri yöntemi kullanarak mobil cihaz adli analizi ile gelişen eğilimler gözlemlenmiştir.

Walnycky ve arkadaşları [31] çalışmasında, ağ trafiği analizi ve sunucu / cihaz depolama analizi ile 20 Android uygulaması incelenmiştir. Bu çalışma dijital kanıtları incelemek, veri gönderip almada uygulama güvenliğini ve veri saklamada uygulama gizliliği değerlendirmek amacıyla yapılmıştır. Çalışma sonucunda Snapchat, Tinder, Wickr veya BBM'den kullanıcı ile ilgili herhangi bir bilgi alınamamıştır. Geriye kalan 16 uygulamada, en azından cihaz tarafından gönderilen ve / veya alınan şifrelenmemiş verilerin bazı kanıtlar yeniden yapılandırılmıştır. Çoğu durumda, şifreler, uygulamaların çektiği ekran görüntüleri, resimleri, videoları, gönderilen sesleri, gönderilen mesajları ve daha fazlası gibi verileri yeniden yapılandırabilir veya bunlara müdahale edebilir. Genel olarak bu çalışma, birçok popüler mesajlaşma uygulamasının, verileri nasıl depoladıkları ve ilettikleri açısından bazı önemli güvenlik açıkları olduğunu göstermektedir.

Aquila ve arkadaşları bu alanda farklı bir yaklaşımla çalışma [32] gerçekleştirmişlerdir. İntihar olaylarının incelemesine ilişkin adli soruşturmalara yardımcı olmak için sosyal mobil otopsi modeli oluşturmuşlardır. Bu model telefondan elde edilen verileri, kişisel bilgisayar veya benzeri cihazlardan elde edilebilecek verileri, Facebook profilinden elde edilebilecek verileri, diğer sosyal uygulamalardan elde edilebilecek verileri ortaya koyar.

3. ÇALIŞMA METODOLOJİSİ

Tez çalışmasının amacı mobil cihazlardaki sosyal medya uygulamalarının incelemesinin nasıl olması gerektiğini ve elde edilebilecek delillerin neler olabileceğini ortaya koymaktır. Tez çalışmasında gerçekleştirilen uygulama adımları Şekil 3.1'de verilmiştir.



Şekil 3.1. Tez çalışmasında gerçekleştirilen uygulama adımları

Tez çalışması uygulama metodolojisi genel olarak üç aşamadan oluşmaktadır. Bunlardan ilki hazırlık aşamasıdır. Bu aşamada incelemesi yapılacak uygulamalar yüklenmiştir. Uygulamalara giriş yapılarak, uygulamalarda adli incelemede önemli sayılabilecek davranışlar gerçekleştirilmiştir. Bu aşamada cihaz mobil inceleme sürecine girmeye hazır bir delil halini almıştır. Bundan sonra mobil cihazın uçuş modu özelliği aktif edilerek cihazın dış dünya ile iletişimi kesilmiştir. İzole edilen cihazın, hazırlanan inceleme ortamında tez çalışmasında kullanılacak adli bilişim araçları ile mantıksal imajları alınmıştır. Mantıksal imajları alınan cihazın incelemesinin gerçek anlamda gerçekleştirilebilmesi için fiziksel imajın alınması gerekir. Fiziksel imaj alabilmek için cihazların dosya sistemine erişimin sağlanması gerekir. Bu işlem Android cihazlarda root etme, iOS cihazlarda jailbreak olarak adlandırılır. Bu işlemler gerçekleştirildikten sonra mobil adli bilişim araçları ile cihazın fiziksel imajları alınır ve uygulama adımlarından imaj alma aşaması tamamlanmış

olur. Analiz aşamasında öncelikle alınan mantıksal imajlardan çıkarılabilen verilere bakılmıştır. Sonrasında ise fiziksel imajlar analiz edilmiştir. İmaj analizleri iki metot ile gerçekleştirilmiştir. Manuel analiz ile incelenecek mobil cihaz uygulamalarının her birinin yapısı, veri saklama biçimleri ele alınmış ve kalıntılara nasıl ulaşılabileceği, bunun hangi araçlar ile yapılabileceği belirtilmiştir. Araçlar ile analiz yönteminde ise, mobil inceleme araçları ile elde edilebilen uygulama verileri değerlendirilmiştir.

3.1 Çalışma Gereksinimleri

Tez çalışmasının gerçekleşebilmesi için önce inceleme yapılacak cihazlar temin edilmiştir. Bu cihazlara gerekli uygulamalar indirilmiştir, uygulamalar üzerinde uygulamaya özgü davranışlar gerçekleştirilmiştir. Bu hali ile cihazların mantıksal imajları alınmıştır. Sonrasında cihaz uygun yazılımlar ile fiziksel imaj alabilmek için bir takım hazırlıklar yapılmıştır. Sonrasında inceleme gerçekleştirilecek iş istasyonu mobil inceleme için bir takım yazılımlar yüklenmiştir. Açık kaynak ve ticari olan bu yazılımlar yardımı ile mobil inceleme gerçekleştirilmiştir. Tez çalışmasında kullanılan donanımların özellikleri Tablo 3.1'de verilmiştir.

Tablo 3.1. Tez çalışmasında kullanılan donanımlar

Donanım	Kullanım Amacı
Windows 10 Pro, 64-bit işlemci 16 RAM Monster Abra A5 bilgisayar	İş istasyonu
Sony Mobile Xperia Z2 LTE-A (D6503) 16 GB Android 6.0.1	İncelenecek Cihaz
iPhone 6s 64 GB iOS 11.3.1	İncelenecek Cihaz
Vodafone SIM kart	SIM kart

Tez çalışmasında kullanılan yazılımların özellikleri Tablo 3.2'de verilmiştir.

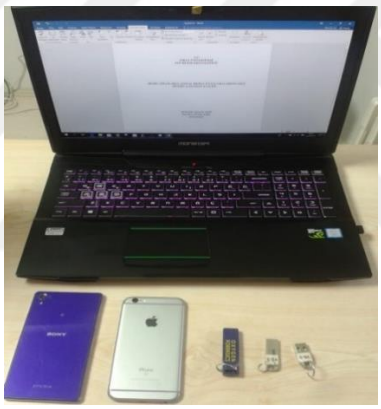
Tablo 3.2. Tez çalışmasında kullanılan yazılımlar

Yazılım	Versiyon	Kullanım Amacı
Android SDK	-	Fiziksel imaj almak
Flashtool	9.18.6	Cihazı root etmek
DB Browser for SQLite	3.10.1	SQLite veri tabanı dosyalarını incelemek
HXD Hex Editor	1.7.7.0	Dosya içeriklerini hex formatında incelemek
plistEditor pro	V2	Plist dosyaları incelemek
Oxygen Forensic Detective	8.4.0.99(USB lisans)	İnceleme Aracı
Paraben's E3:DS	Aurora 1.4 Edition	İnceleme Aracı
Magnet AXIOM Examine	v1.2.5.8637	İnceleme Aracı
Android Facebook Uygulaması	149.0.0.40.71	İncelenecek Uygulama

Tablo 3.2. Tez çalışmasında kullanılan yazılımlar (Devamı)

Android Facebook Messenger Uygulaması	143.0.0.20.69	İncelenecek Uygulama
Android WhatsApp Messenger Uygulaması	2.17.395	İncelenecek Uygulama
Android Instagram Uygulaması	22.0.0.17.68	İncelenecek Uygulama
Android Twitter Uygulaması	7.21.0	İncelenecek Uygulama
Android BiP Messenger Uygulaması	3.25.6	İncelenecek Uygulama
iOS Facebook Uygulaması	175.0.0.47.102	İncelenecek Uygulama
Facebook Messenger Uygulaması	167.0.0.57.96	İncelenecek Uygulama
WhatsApp Messenger Uygulaması	2.18.61	İncelenecek Uygulama
Instagram Uygulaması	46.0.0.14.96	İncelenecek Uygulama
Twitter Uygulaması	7.24	İncelenecek Uygulama
BiP Messenger Uygulaması	3.33.17	İncelenecek Uygulama

Tez çalışmasının gerçekleştirildiği cihazlar Şekil 3.2'de verilmiştir.



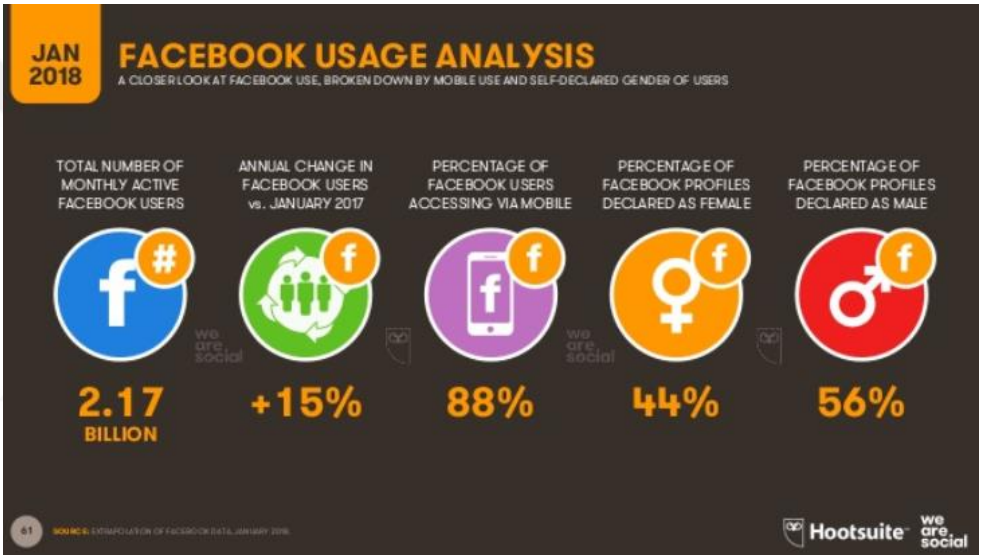
Şekil 3.2. Tez çalışmasının gerçekleştirildiği cihazlar

3.2 Hazırlık

Tez çalışmasında gerçekleştirilen uygulamanın ilk aşaması hazırlıktır. Bu aşamada çalışmada kullanılacak sosyal medya uygulamaları yapılandırılmıştır. Facebook, Facebook Messenger, WhatsApp Messenger, Instagram, Twitter ve BiP Messenger uygulamaları Android cihaza Google Play Store 'dan, iOS cihaza Apple Store 'dan indirilmiştir ve fatmatezyazar@gmail.com mail adresi ile giriş yapılmıştır. Uygulamaların yapıları incelenerek gerçekleştirilebilecek davranışlar belirlenmiştir.

3.2.1 Facebook

Facebook, insanların diğer insanlarla iletişim kurmasını ve bilgi alışverişi yapmasını sağlayan bir sosyal medya sitesidir. 2003 yılının sonlarına doğru Mark Zuckerberg tarafından yazılmaya başlanan Facebook'un ilk başlarda yalnızca Amerikadaki birkaç üniversitenin öğrencilerinin kullanımına açılmışken, Eylül 2006 tarihinden itibaren 13 yaş üstü herkes için eposta adresi ile üyelik kabul etmeye başlamıştır. Dünyada en çok kullanılan 3. Web sitesidir [33]. Şekil 3.3'de aylık aktif kullanıcı sayısına göre Facebook kullanıım analizi verilmiştir [4]. Buna göre Facebook 2.17miyar aylık aktif kullanıcı sayısına sahiptir ve bunların %88'i mobil kullanıcılardır.



Şekil 3.3. Facebook kullanım analizi

Haber akışı, kullanıcıların ağda yayınlanan tüm içeriklerin gösterildiği alandır. Uygulamaya giriş yapıldığında ilk gösterilen alan burasıdır. Güncellemelerin yanı sıra profil değişikliklerini, yaklaşan etkinlikleri ve doğum günlerini içeren bilgileri içermektedir.

Paylaşım yapma; kullanıcının fotoğrafları, videoları, durumları, anketleri, gifleri, çıkartmaları, etkinliği isteğe bağlı olarak kişileri ve konumları etiketleyerek diğer kullanıcılar ile paylaşması işlemidir. Paylaşılan gönderiler kişinin izin verdiği kişiler tarafından görüntülenebilir.

Beğenme; kullanıcıların durum güncellemeleri, yorumlar, fotoğraflar, arkadaşların, videoların ve reklamların paylaştığı bağlantılar ile kolayca etkileşimde bulunmalarını sağlar.

Yorum yapma; beğenme etkileşiminde ifade edilen tüm içeriklere yorum yapma işlemidir. Yapılan yorumlar içeriği görüntüleyebilen herkes tarafından görüntülenir.

Grup kurma; kullanıcılar tarafından diğer kullanıcıları ekleyerek oluşturulan yapılardır. Gruplar, üyelerin bağlantılar, medya, sorular, etkinlikler, düzenlenebilir belgeler ve bu öğelerle ilgili yorumlar gibi içerik yayınlamasına olanak tanır.Hikâye paylaşma; kullanıcıların fotoğraflarını ve videolarını 24 saat sonunda içeriğin kaybolacak şekilde tüm arkadaşlarıyla paylaşmasına olanak tanıyan bir özelliktir.

Mesajlaşma; Facebook Messenger uygulaması ile bağlantılı olarak Facebook kullanıcılarının birbirine mesaj gönderme işlemidir. Kullanıcıların hem birebir etkileşimlerde, hem de grup görüşmelerinde, sesli aramalar ve görüntülü görüşmeler yapmasını sağlar.

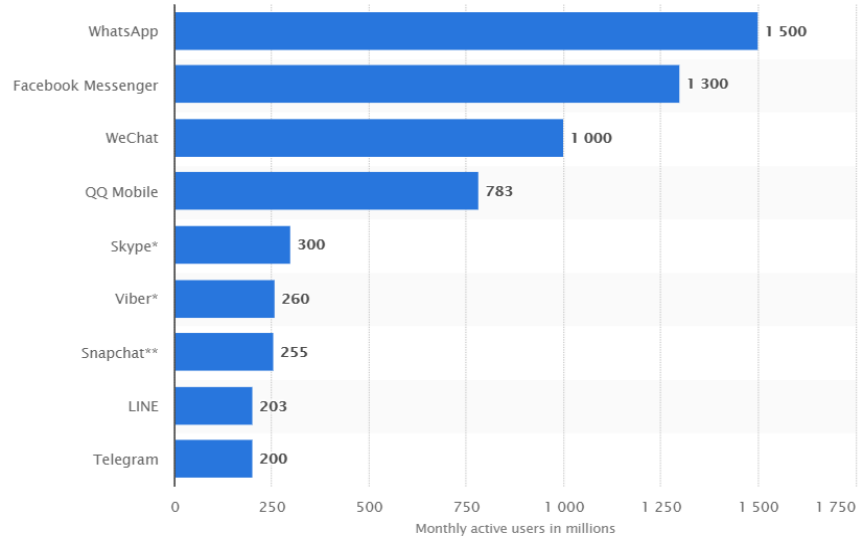
Tez çalışması için Facebook ve Facebook Messenger uygulamaları indirilmiştir. Tablo 3.3'de Facebook mobil uygulaması üzerinde gerçekleştirilen davranışlar verilmiştir.

Tablo 3.3. Facebook uygulama davranışları

Uygulama Davranışları	Çalışmada Gerçekleştirilen Kullanıcı Davranışları
Paylaşım	Durum, Fotoğraf, Konum paylaşımı yapıldı.
Yorum	Bir fotoğrafa yorum yapıldı.
Beğeni	Bir beğeni yapıldı.
Arkadaş Ekleme	Arkadaş ekleme,silme,engelleme işlemi gerçekleştirildi.
Grup kurma	Grup kuruldu, grup paylaşımlar yapıldı ve biri silindi.
Hikaye Paylaşma	Hikaye paylaşımı yapıldı.
Mesajlaşma	Bir kullanıcı ile mesajlaşıldı, bir mesaj silindi. Grup ile mesajlaşıldı, bir mesaj silindi.

3.2.2 WhatsApp Messenger

WhatsApp Messenger uygulaması mobil cihazlar için geliştirilmiş anlık mesajlaşma ve arama uygulamasıdır. Android, BlackBerry, iPhone, Windows Phone ve Nokia telefonları ile uyumludur ve platformlar arası çalışma özelliğine sahiptir. Aylık aktif kullanıcı sayısına göre. Şekil 3.4'de Nisan 2018 itibariyle dünyada en çok kullanılan mobil haberleşme uygulamaları verilmiştir ve ilk sırada yer alan uygulama WhatsApp Messenger'dır[34].



Şekil 3.4. Nisan 2018'de dünyada en çok kullanılan anlık mesajlaşma uygulamaları

Uygulama kullanıcıların birbirlerine sesli ve yazılı mesaj, fotoğraf, video, sesli ve görüntülü arama, belge göndermesini sağlamaktadır. Bunu yaparken uçtan uca şifreleme kullanarak haberleşmenin güvenliği sağlanmaktadır. Haberleşme uçtan uca şifrelendiğinde, mesajlar ve aramalar korunur, gönderiler yalnızca iletişime geçilen taraflar arasında kalır, aradaki hiçimse tarafından, WhatsApp dâhil, okunamaz veya dinlenilemez [35].

Tez çalışması için WhatsApp Messenger uygulaması indirilmiştir. Tablo 3.4'de uygulama üzerinde gerçekleştirilen davranışlar verilmiştir.

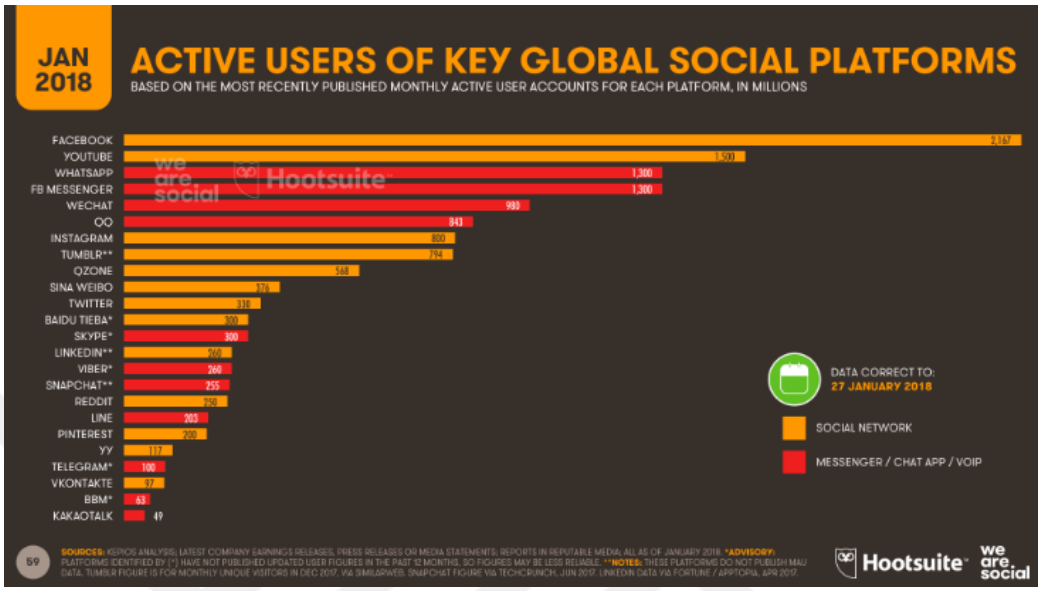
Tablo 3.4. WhatsApp Messenger uygulama davranışları

Uygulama Davranışları	Çalışmada Gerçekleştirilen Kullanıcı Davranışlar
Mesajlaşma	Mesaj, Fotoğraf, konum paylaşımları yapıldı. İçlerinden bir kaçı silindi.
Grup kurma	Mesajlaşma gerçekleştirildi. İçlerinden bir kaçı silindi.
Arkadaş engelleme	Gerçekleştirildi.
Görüntülü konuşma	Gerçekleştirildi.
Sesli Konuşma	Gerçekleştirildi.
Anı paylaşımı	Gerçekleştirildi.

3.2.3 Instagram

Instagram fotoğraf ve video paylaşımı sağlayan bir sosyal ağ uygulamasıdır. 2010 yılında hizmet sağlamaya başlayan uygulama kullanıcıya bir fotoğrafı filtreleme ve paylaşma imkânı sunmuştur. İlk başlarda yalnızca iOS'ta hizmet veren uygulama sonrasında

Android ve Windows Phone telefonlar içinde hizmet vermeye başlamıştır. Şekil 3.5'de dünyada aktif kullanıcı sayısına göre en çok kullanılan uygulamalar verilmiştir ve Instagram da bu uygulamalar arasında yer almaktadır [4].



Şekil 3.5. Ocak 2018'de en çok kullanılan sosyal platformlar

Uygulama, kullanıcıların çeşitli filtrelerle düzenleyebileceği ve etiketler ve konum bilgileri ile düzenleyebileceği fotoğraf ve videoları yüklemesine olanak tanır. Bir hesabın yayınladığı fotoğraf veya videoları herkese açık olarak veya önceden onaylanmış takipçilerle paylaşılabilir. Kullanıcılar, diğer kullanıcıların içeriklerini etiketlere ve konumlara göre tarayabilir ve trend içeriği görüntüleyebilir. Kullanıcılar, fotoğrafları beğenebilir, yorum yapabilir ve diğer kullanıcıları da içeriklerini kendi akışına eklemek için takip edebilirler. Uygulama kullanıcılarla mesajlaşma özelliğine ve birden çok görüntüyü veya videoyu tek bir gönderiye ekleyebilme özelliğine sahiptir. Ayrıca, hikâye özelliği ile 24 saat içinde kaybolacak video ve fotoğraflar paylaşmaya olanak tanır. Bunların haricinde uygulama etiket (*hashtag*) özelliği ile kullanıcıların hem fotoğrafları hem de birbirlerini keşfetmelerine yardımcı olmaktadır [36]. Instagram, kullanıcıların daha sonra görüntülenmek üzere fotoğraf kaydetmesine izin veren bir özelliğe de sahiptir. Yer işaretli gönderiler, uygulamadaki özel bir sayfaya eklenir.

Tez çalışması için Instagram uygulaması indirilmiştir. Tablo 3.5'de uygulama üzerinde gerçekleştirilen davranışlar verilmiştir.

Tablo 3.5. Instagram uygulama davranışları

Uygulama Davranışları	Çalışmada Gerçekleştirilen Kullanıcı Davranışları
Paylaşım	Fotoğraflar ve videolar paylaşıldı. Birer tanesi silindi.
Durum	Durumlar paylaşıldı. Bir tanesi silindi.
Beğeni	Fotoğrafı beğenildi.
Yorum	Fotoğraf ve duruma yorumu yapıldı.
Mesaj	Bir kullanıcıya özel mesajlar atılır.1 tanesinin gönderimi iptal edilir.
Takip	Birkaç hesap takip edilir, bir hesap takipten çıkarılır, bir hesap engellenir.
Paylaşım kaydetme	Bir paylaşım kaydedilir.
Etiket	Bir etle fotoğraf paylaşılır.

3.2.4 Twitter

Twitter kullanıcıların *tweet* olarak bilinen mesajlar yayınlayıp etkileşimde bulunduğu bir haber ve sosyal ağ hizmetidir. Twitter'ın iOS, Android, Windows Phone ve BlackBerry işletim sistemleri için mobil uygulamaları mevcuttur. Şekil 3.5 ‘de istatistiklere göre dünyada aktif kullanıcı sayısı itibarı ile en çok kullanılan sosyal platformlar verilmiştir ve Twitter bunlar arasında yer almaktadır [4].

Tweet başlangıçta 140 karakterle sınırlıydı, 7 Kasım 2017 itibariyle bu sınır 280’e çıkarılmıştır [37]. Kullanıcılar tarafından atılan tweetler eğer kullanıcı tarafından kısıtlanmadı ise herkes tarafından görülebilirler, kısıtlandı ise de sadece kendi takipçileri tarafından görülürler. Kullanıcılar başka kullanıcıların hesaplarını takip edebilirler. Yanıt bir başka kullanıcının Tweetine verilen cevap verilmesi işlemidir. Retweet bir kullanıcının takipçileri ile herkese açık olarak bir tweeti paylaşması demektir. Kullanıcı tweetleri beğenebilir, beğenilen tweet kullanıcının beğeni sayfasında görüntülenir. Kullanıcılar birbirine direk mesaj atabilir veya özel tweet paylaşabilirler.

Tez çalışması için Twitter uygulaması indirilmiştir. Tablo 3.6‘da uygulama üzerinde gerçekleştirilen davranışlar verilmiştir.

Tablo 3.6. Twitter uygulama davranışları

Uygulama Davranışları	Çalışmada Gerçekleştirilen Kullanıcı Davranışları
Tweet	Tweetler atılır, bir tweet silinir.
Yanıt	Bir tweete yanıt verilir.
Retweet	Bir tweet retweet yapılır.
Beğenmek	Bir tweet beğenilere eklendi.
Mesaj(DM)	Bir kullanıcıya özel mesajlar atılır.1 tanesi silinir.
Hesap Takip	Birkaç hesap takip edilir, bir hesap takipten çıkarılır, bir hesap engellenir.

3.2.5 BiP Messenger

BiP Turkcell tarafından iOS ve Android işletim sistemleri için geliştirilen, anlık mesajlaşma uygulamasıdır. Uygulama mobil operatör firması tarafından geliştirilmesine rağmen, tüm operatör kullanıcıları tarafından kullanılabilmektedir. Uygulamaya App Store, Google Play ve Turkcell AppMarket'ten ücretsiz olarak ulaşılabilmektedir [38]. Türkiye'de yaygın şekilde kullanılan anlık mesajlaşma uygulamalarından biridir.

Uygulamanın mesajlaşma özelliği ile kullanıcılar diğer kullanıcılarla birebir veya grup halinde mesajlaşabilmekte, video, resim, ses kaydı, konum gönderebilmektedirler. Sesli ve görüntülü arama yapabilmekte, kaybolan mesaj özelliği ile kullanıcının belirlediği süre sonunda sohbet ekranından kaybolmasını sağlayacak şekilde mesaj gönderebilmektedirler. Caps yaratma özelliği ile bir fotoğraf ile kullanıcı kendi capsini oluşturabilmektedir. BiP Her yöne arama özelliği ile Turkcell kullanıcıları BiP uygulaması olmayan aboneleri de Turkcell ses paketleri veya tarifelerini kullanarak arayabilirler, herkesle iletişim kurabilme özelliği ile uygulamayı kullanmayanlara SMS ile mesaj gönderebilirler.

Uygulamadaki Keşfet menüsü içerisinde servisler bulunmaktadır. Bun servisler ulusal markalara, TV şovlarına, ünlülere, organizasyonlara, sivil ve kamu kurumlarına, orta-küçük ölçekli işletmelere ve küçük kullanıcı gruplarına hizmet vermek için oluşturulmuştur. Servisler üzerinden; mesajlar ve medyalar toplu şekilde gönderilebilirler.

Bip uygulamasının, caps, zaman ayarlı silinebilir mesajlaşma, konum üzerinden birbirini takip edebilme özellikleri diğer anlık mesajlaşma uygulamalarından ayırmaktadır.

Tez çalışması için BiP uygulaması indirilmiştir. Tablo 3.7'de uygulama üzerinde gerçekleştirilen davranışlar verilmiştir.

Tablo 3.7. BiP Messenger uygulama davranışları

Uygulama Davranışları	Çalışmada Gerçekleştirilen Kullanıcı Davranışları
Mesajlaşma	Mesaj, Fotoğraf, konum paylaşımları yapıldı. İçlerinden bir kaçı silindi.
Grup kurma	Mesajlaşma gerçekleştirildi. İçlerinden bir kaçı silindi.
Arkadaş engelleme	Gerçekleştirildi.
Zamanlı mesaj paylaşımı	Gerçekleştirildi.
Zamanlı konum paylaşımı	Gerçekleştirildi.
Caps oluşturma	Gerçekleştirilmedi.

3.3 İmaj Alma

Tez çalışmasının ikinci aşaması hazırlık aşamasında yapılandırılan uygulamaların imajlarının (adli kopya) alınmasıdır. Adli bilişim incelemelerinde cihaz incelemeleri, delil bütünlüğünü bozmamak için o cihazın bir kopyası üzerinde gerçekleştirilir. Adli bilişimde bir diskin birebir kopyasına imaj denir [5] . İmaj alma işlemi mobil cihazlarda sabit disklere göre daha karmaşık bir yapıya sahiptir [39]. Mobil işletim sistemleri kullanıcıya verilerin bir kısmına erişim izni vermektedir. Kullanıcının erişebildiği bu alanın imajının alınması mantıksal imaj olarak adlandırılır [40]. Mobil adli bilişim araçları, yazılım bileşenlerinin nasıl etkileştiğini belirleyen API (uygulama programlama ara yüzü) kullanarak mobil cihazın işletim sistemi ile iletişim kurar ve mantıksal imaj elde ederler. Mantıksal bir imajdan elde edilebilen veriler işletim sistemine bağlı olarak değişmekle birlikte genel olarak, çağrı günlükleri, SMS, MMS, resimler, videolar, ses dosyaları gibi bilgilerdir.

Mobil cihazın tüm belleğinin birebir kopyasını alma işlemine fiziksel imaj denir [41]. Fiziksel imaj kullanıcının erişebildiği alanların yanında ayrılmamış alandaki veriler ve silinmiş verilerinde içinde bulunduğu bütün verileri içerir. Fiziksel imaj ham biçiminde edinildiğinden, farklı dosya sistemleri için bu dökümleri ayrıştırmak amacı ile adli bilişim araçları kullanılır. Bu araçlar yardımıyla fiziksel imajdan genel olarak; resimler, videolar, uygulama verileri, konum bilgileri, e-postalar ve daha fazla veri tipi elde edilebilir. Mantıksal imajdan çok sınırlı verilere ulaşılırken fiziksel imajdan çok daha kapsamlı verilere ulaşılır, silinmiş ve ayrılmamış alandaki veriler elde edilebilir.

3.3.1 Android

Gerçekleştirilen uygulamada Android 6.0.1 sürümü yüklü 16 GB kapasiteye sahip Sony Mobile Xperia Z2 LTE-A (D6503) cihazı kullanılmıştır. İmaj alma işlemleri sırasında Paraben, Oxygen Forensic, Magnet Axiom ticari yazılımları ile ddtool açık kaynak aracı kullanılmıştır. Cihazın sırası ile mantıksal imajları alınmış, rootlama işlemi gerçekleştirilmiş ve sonrasında fiziksel imajları alınmıştır.

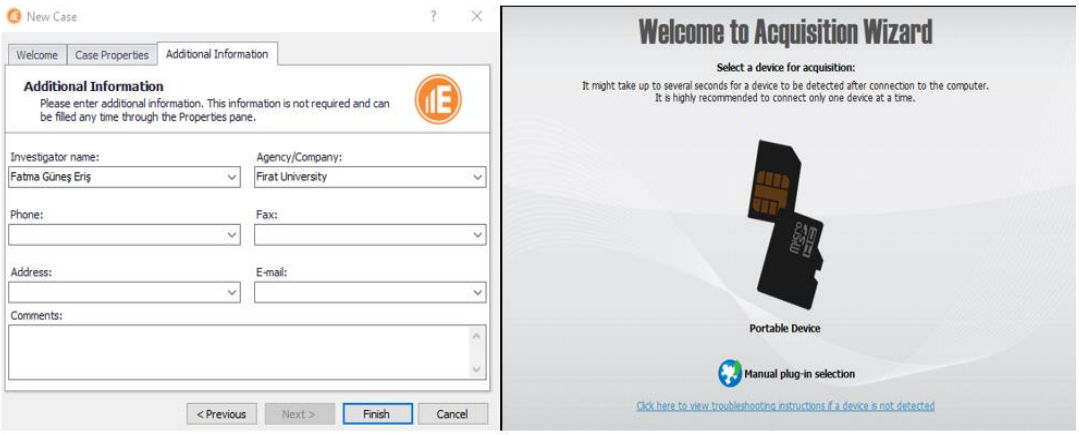
3.3.1.1 Mantıksal İmaj Alımı

Mantıksal imaj işletim sisteminin kullanıcıya erişebilmesi için izin verdiği dosyaları içeren alanın kopyasının alınması işlemidir. Bu imaj tipinde dosya sistemine ait olan ve

kullanıcı ile paylaşılmayan, program veri tabanları, log dosyaları, işletim sistemi dosyaları gibi veriler elde edilememektedir. Ancak alınması kolaydır. Mantıksal imaj ile erişilemeyen dosyaların erişilebilmesini sağlamak amacıyla yapılan işlemler bazı durumlarda verilerin kaybedilmesine yol açabileceği için, delil incelenmeye başlanırken ilk olarak alınması gereken imaj tipi mantıksal imajdır. Bu sayede elde edilmesi zor olmayan verilerin kaybedilmesinin önüne geçilmektedir. Bu nedenle incelenecek her mobil cihazın mantıksal imajı alınmalıdır. Kolay bir şekilde elde edilmesi, fiziksel imajdan daha hızlı olması ve çoğu zaman delil olarak yeterli olabilecek mesajlar, resimler, notlar, kişiler, arama kayıtları gibi verilerin elde edilebilmesi açısından mobil cihaz incelemelerinde önemli bir yere sahiptir. Yapılan uygulamada cihazın Paraben E3:DS ve Oxygen Forensic yazılımları ile mantıksal imajları alınmıştır.

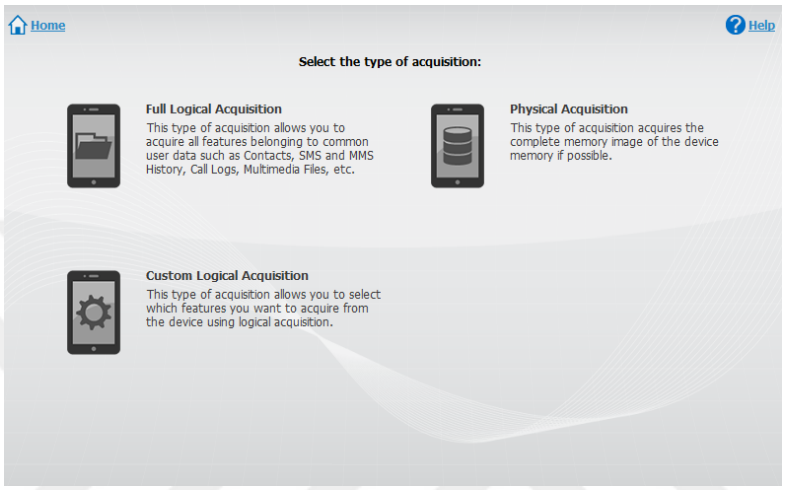
Paraben E3: DS mobil adli bilişim incelemesinde çokça tercih edilen bir ticari adli bilişim aracıdır. Paraben ile mantıksal imaj alma işlemi aşağıdaki adımlar izlenerek gerçekleştirilir.

- Yeni bir *Case* oluşturulur. Şekil 3.6'da sol kısımda, inceleme ve incelemeyi yapan kişiyle ilgili bilgiler girilir.
- *Start acquaction* seçeneği tıklanır. Şekil 3.6'da sağ kısımda, cihazın delil olarak eklenme adımı verilmiştir.



Şekil 3.6. Paraben aracı ile imaj alırken bilgi girme ve cihaz ekleme ekranları

- Bu adımda işleme devam edebilmek için mobil cihazda önce geliştirici seçeneği ve USB ayıklama modu aktif hale getirilir. Sonrasında Güvenlik seçeneğinin altında bilinmeyen kaynaklar seçeneği aktif edilir.
- Yazılımda *start acquaction* butonuna tıklanır. Burada *full logical acquaction* seçeneği tıklanır. Hem uygulamada hem cihazda *full back up* için istenilen izinler onaylanır. Şekil 3.7'de veri çıkarma tipini seçme ekranı verilmiştir.



Şekil 3.7. Paraben'de veri çıkarma tipini seçme ekranı

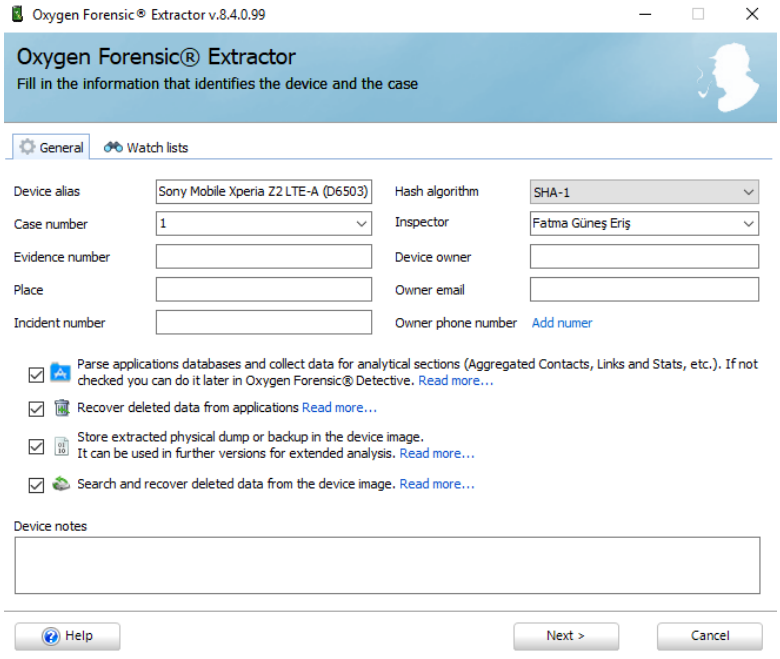
- Sonuç olarak Paraben programına özgü *.e3* uzantılı mantıksal imaj alınmış olur.

Oxygen Forensic: Mobil cihazlardan gelen veriyi ayıklamak ve analiz etmek için gelişmiş ticari bir mobil adli bilişim aracıdır. Oxygen Forensic aracı ile mantıksal imaj alma işlemi aşağıdaki adımlar izlenerek gerçekleştirilir.

- *Connect device* seçeneği tıklanır. Şekil 3.8'de Oxygen Forensic aracı ile imaj alma sırasında veri çıkarma metodunu belirleme ekranı verilmiştir. Açılan sayfada otomatik cihaz bağlantısı tıklanır.

Şekil 3.8. Oxygen Forensic'de veri çıkarma metodu seçme ekranı

- Mobil cihaz üzerinde USB hata ayıklamasına izin verilir ve *bu bilgisayarda her zaman izin ver* tıklanır ve yazılımdaki *connect* butonu tıklanır.
- Şekil 3.9'de incelemeyle ilgili genel bilgilerin doldurulma ekranı verilmiştir. Uygulama veritabanlarından veri çıkarımı seçeneği, silinmiş uygulama verilerini kurtarma seçeneği, cihaz imajından silinmiş verileri aratıp kurtarma seçeneği seçilir bir sonraki sayfaya geçilir.



Şekil 3.9. Oxygen Forensic'de inceleme ile ilgili bilgi doldurma ekranı

- Açılan sayfada *advanced mode* seçilerek bir sonraki sayfaya geçilir, çıkan sayfada mantıksal çıkarım seçilir ve bir sonraki sayfaya geçilir.
- Açılan sayfadaki tüm veri tipleri seçilir.
- Sonuç olarak Oxygen Forensic aracına özgü .ofb uzantılı mantıksal imaj oluşturulmuş olur.

3.3.1.2 Fiziksel İmaj Alımı

Herhangi bir cihazın fiziksel imajını elde etmek, orijinal cihazın belleğinin bit-bit kopyasını tam olarak çıkarmak demektir. Fiziksel imajdan, mantıksal imaja ek olarak ayrılmamış alandaki verilere, silinmiş verilere ve uygulama veri tabanlarına erişim sağlamaktadır. Fiziksel imajın alınabilmesi için Android cihazların root erişimine sahip olması gerekmektedir. Root işlemi cihaz üzerinde bir takım değişiklikler gerçekleştireceği için adli bilişim açısından uygun değildir, fakat cihazın fiziksel imajının almak ve cihaz üzerindeki tüm verilere ulaşabilmek için gereklidir. Örneğin bir cihaz üzerindeki tüm veriler manuel olarak silinmiş ise bu verilere yeniden ulaşabilmek için mantıksal çıkarım yeterli olmayacaktır ya da kimi uygulamalar veri tabanı dosyalarını root izni ile saklı tuttukları için o uygulamadan gelecek verilere ulaşılamayacaktır. Bu yüzden uygulamanın bu aşamasında cihazda root işlemi gerçekleştirilecek sonrasında Paraben E3:DS ve Oxygen Forensic ticari araçları ve dd tool açık kaynak aracı ile fiziksel imajlar elde edilecektir.

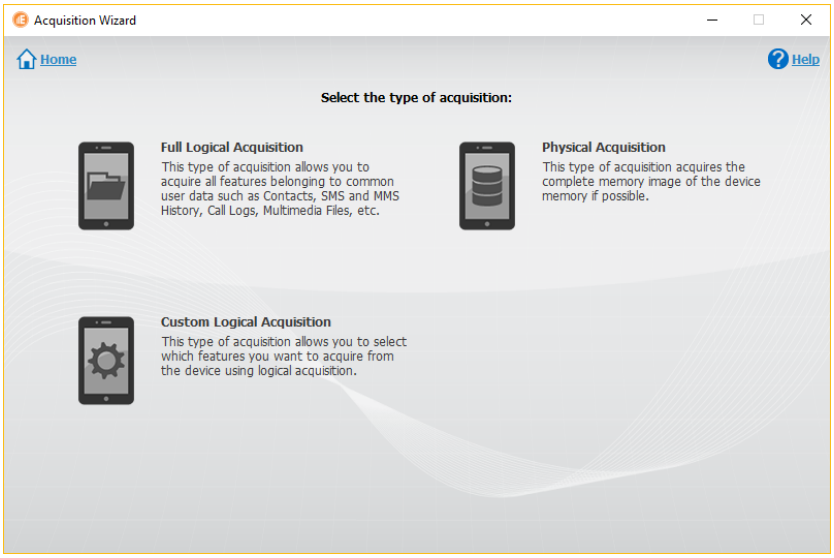
Root Etme İşlemi: Mevcut adli bilişim araçları belirli cihazlar için root erişimini sağlayabilmekle birlikte Android sürüm ve cihaz sayısının fazlalığından dolayı yüzde yüz başarım sağlanamamaktadır. Uygulama için kullanılan Sony Xperia Z2 cihazı root etme işlemleri uygulamada kullanılan adli bilişim yazılımları tarafından otomatik olarak gerçekleştirilemediği için harici bir çekirdek yazılımı yüklenerek root işlemi gerçekleştirilmiştir. Cihazı root etme işlemi aşağıdaki adımlardaki gibi sağlanmıştır.

- Telefon ayarlarından geliştirici seçenekleri aktif edilir.
- USB hata ayıklaması açılır.
- Root işleminin yapılabileceği çekirdek yazılımı ve SuperSu uygulaması daha sonra geri yüklemek için SD karta atılır.
- Telefonun bilgisayar bağlantısı kesilir.

- Bilgisayara Flashtool kurulur.
- Telefon kapatılır, Flashtool yazılımı açılır ve Flashmod'da bağlanır.
- Flashmode: Telefon kapalı iken ses kısma tuşuna basılı tutarak bilgisayara bağlanıldığında bu moda girer.
- Fastboot mode: Telefon kapalı iken ses açma tuşuna basılı tutarak bilgisayara bağlanıldığında bu moda girer.
- Telefon Flashmoda alarak çekirdek dosyası Flashtool programı ile flashlanır.
- Bilgisayara uygun yazılım yüklenerek cihazın TWRP recovery moda geçmesi sağlanır.
- Recovery modda Install diyerek sd kartta bulunan SuperSu kurulumu yapılır ve çıkmadan sd karttaki çekirdek kurulur. Sistem yeniden başlatılarak root erişimi gerçekleştirilir.

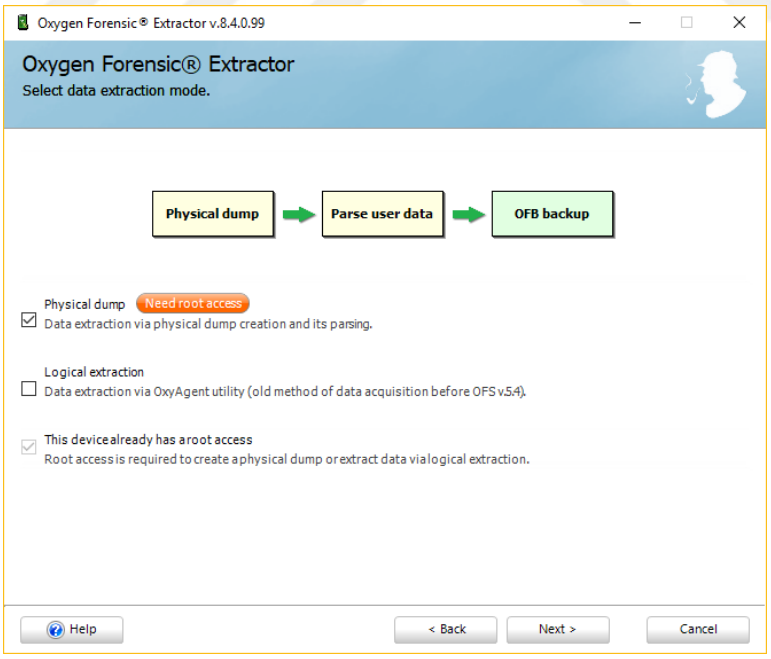
Cihaz root edildikten sonra fiziksel imaj elde etme aşamasına gelinir.

Paraben E3:DS aracı ile fiziksel imaj alma adımları mantıksal imaj alma işlemleri ile benzer şekilde gerçekleştirilmektedir. Mantıksal imaj alma adımlarından *select type of acquaction* sayfasında fiziksel çıkarımı sağlayacak olan *physical acquistion* seçeneği seçilerek imaj alma işlemi yapılır ve .e3 formatında bir imaj elde edilir. Şekil 3.10, bu aşamada Full "Logical Acquisition" seçeneği tıklandığında fiziksel imajın yanış sıra yazılımın detaylı ayrıştırarak bulduğu bütün anlamlı veriler araç kullanıcısına sunulmaktadır.



Şekil 3.10. Paraben aracı ile fiziksel imaj alma

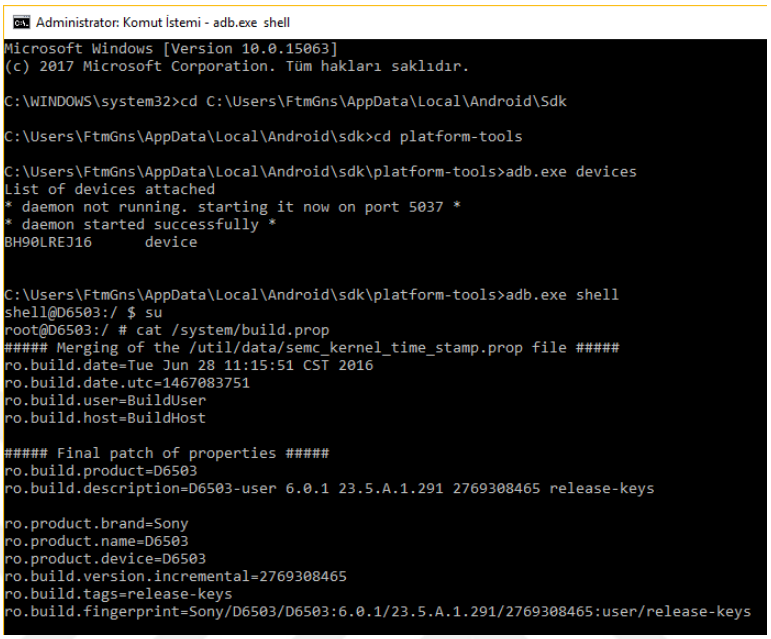
Oxygen Forensic aracı ile fiziksel imaj alma adımları mantıksal imaj alma işlemleri ile benzer şekilde gerçekleştirilmektedir. Mantıksal imaj alma adımlarından *select data extraction* sayfasında fiziksel çıkarımı sağlayacak olan *physical dump* seçeneği tıklanarak imaj alma işlemi gerçekleştirilir. Şekil 3.11'de fiziksel imaj alma ekranı verilmiştir.



Şekil 3.11. Oxygen Forensic aracı ile fiziksel imaj alma ekranı

d tool imaj almada kullanıla açık kaynak bir adli bilişim aracıdır. Android Sdk platform araçları root edilmiş bir cihazın fiziksel imajının alınması için kullanılabilmektedir. *adb.exe*

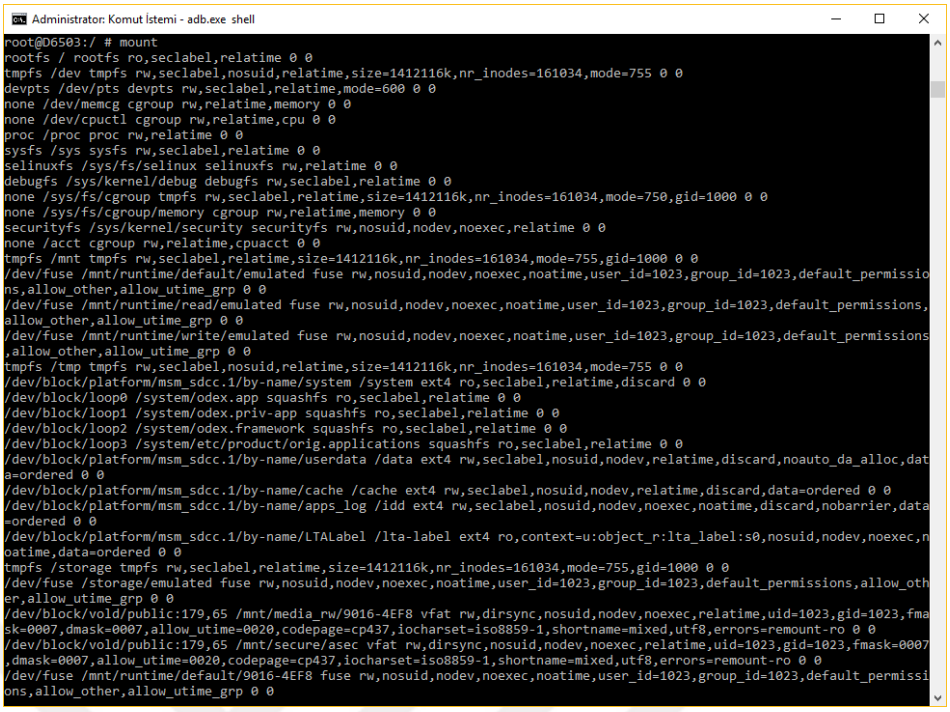
komutu yardımı ile bağlı cihazları listeledikten sonra su komutu ile root kullanıcı olunur ve *cat* komutu ile /system/buil.prop dosyasındaki cihaz bilgileri görüntülenir. Şekil 3.12'de adb.exe komutu kullanımları gösterilmiştir.



Şekil 3.12. adb.exe komutu kullanımı

mount komutu ise cihaza mount edilmiş bölümleri gösterir. Bu bölümlerden uygulama analizi için gerekli olan userdata dosyasının bulunduğu bölümün dd tool yardımı ile dd imajı alınır. Ekrana *dd if=/dev/block/platform/msm_sdcc.1/by_name/userdata of=storage/9016-*

adb.exe pull /storage/1AC4-A3B2/Android/data/sonyfizikseluserdata.dd komutu yazılarak dd imaj alınmış olur. Şekil 3.13'de dd aracı ile imaj alma işlemi gösterilmiştir.



Şekil 3.13. dd tool ile fiziksel imaj alma

Oluşturulan bu dd imajı herhangi bir adli bilişim inceleme aracı ile analiz edilebilir.

3.3.2 iOS

Gerçekleştirilen uygulamada üzerinde iOS 11.3.1 iletim sistemi bulunan 64 GB kapasitesi bulunan bir iPhone 6s cihazı kullanılmıştır. İmaj alma işlemleri sırasında Paraben, Oxygen Forensic, Axiom ticari yazılımları kullanılmıştır. Cihazın sırası ile mantıksal imajları alınmış, jailbreak işlemi denemiş, fakat iOS sürümü henüz bu işleme uygun olmadığı için fiziksel imajları alınamamıştır.

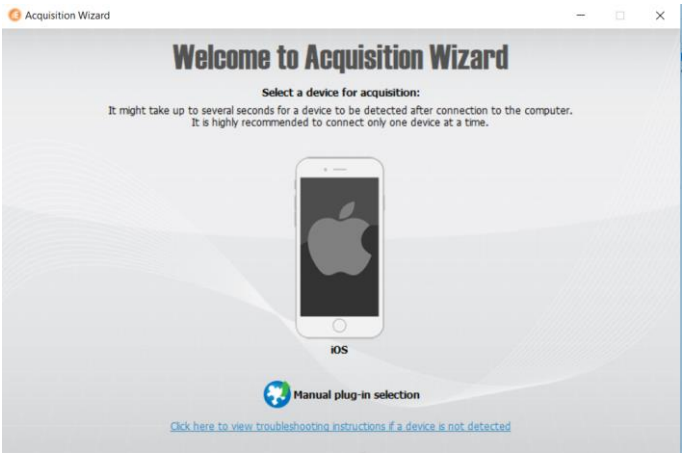
3.3.2.1 Mantıksal İmaj Alımı

Mantıksal imaj işletim sisteminin kullanıcıya erişebilmesi için izin verdiği dosyaları içeren alanın kopyasının alınması işlemidir.

Paraben E3: DS ile mantıksal imaj alma işlemi aşağıdaki adımlar izlenerek gerçekleştirilir.

- Yeni bir *Case* oluşturulur. Burada inceleme ve incelemeyi yapan kişiyle ilgili bilgiler girilir.

- *Start acquaction* seçeneği tıklanır. Cihaz bilgisayara bağlanır ve karşımıza Şekil 3.14'deki gibi cihaz ekleme ekranı çıkar.

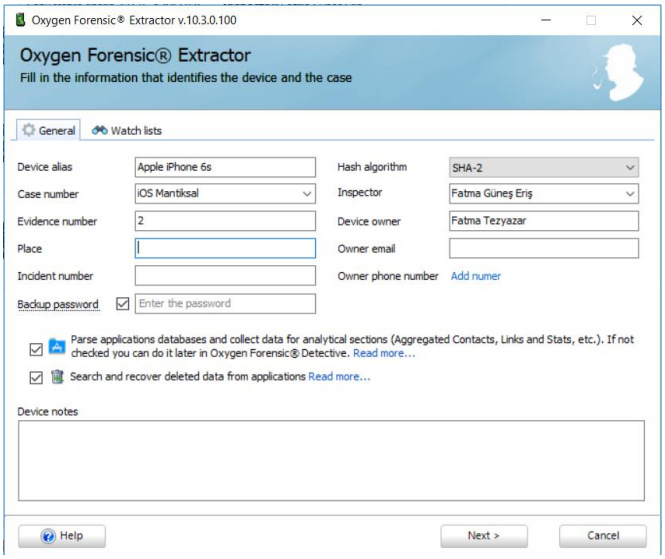


Şekil 3.14. Paraben'de ios cihazı ekleme ekranı

- Cihaz seçildikten sonra veri çıkarma tipi olarak *full logical acquaction* seçeneği tıklanır.
- iPhone üzerinde çıkan bilgisayara güven seçeneği tıklanır.
- Sonuç olarak Paraben programına özgü *.e3* uzantılı mantıksal imaj alınmış olur.

Oxygen Forensic ile mantıksal imaj alma işlemi aşağıdaki adımlar izlenerek gerçekleştirilir.

- *Connect device* seçeneği tıklanarak cihaz kablo ile bilgisayara bağlanır.
- Çıkan ekranda cihazı otomatik bağlama seçeneği seçilerek cihazın otomatik olarak tanınması sağlanır.
- Şekil 3.15'de incelemeyle ilgili genel bilgilerin doldurulma ekranı verilmiştir. Uygulama veritabanlarından veri çıkarımı seçeneği, silinmiş uygulama verilerini kurtarma seçeneği seçilir. Eğer incelenen iPhone cihazının bilinen iTunes yedekleme şifresi varsa yine bu sayfada girilir. Bir sonraki sayfaya geçilir.

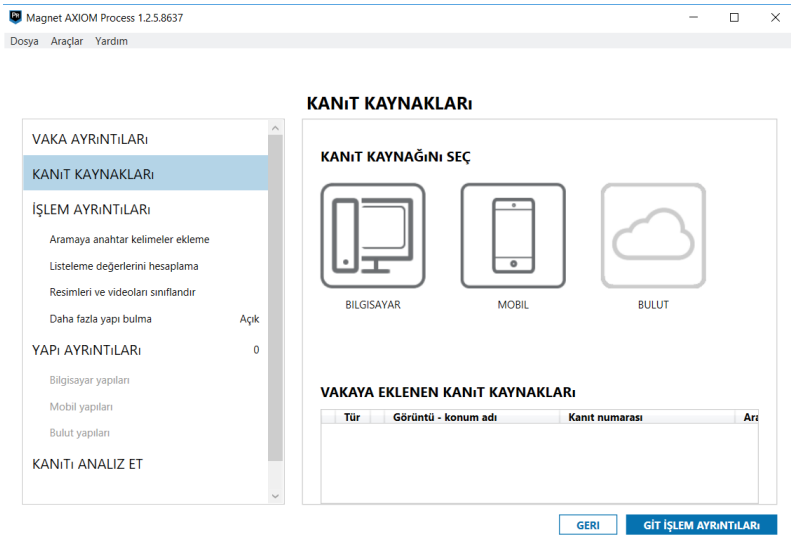


Şekil 3.15. Oxygen Forensic'de iOS cihaz ile ilgili bilgi doldurma ekranı

- Sonuç olarak Oxygen Forensic aracına özgü .ofb uzantılı mantıksal imaj oluşturulmuş olur.

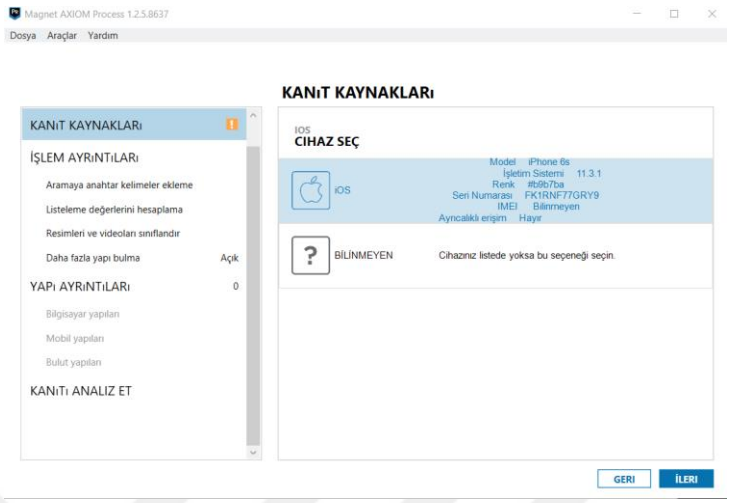
Magnet Axiom aracı ile mantıksal imaj alma işlemi aşağıdaki adımlar izlenerek gerçekleştirilir.

- İlk olarak *Yeni Vaka Oluştur* tıklanır.
- *Kanıt kaynağı seç* kısmında Şekil 3.16'deki ekranda mobil olan seçenek tıklanır.



Şekil 3.16. Axiom'da kanıt kaynağı seçme ekranı

- Gelen sayfada *iOS* seçilir ve *Kanıt Al* ile Şekil 3.17'daki cihaz seçme ekranından *iOS* seçilir.



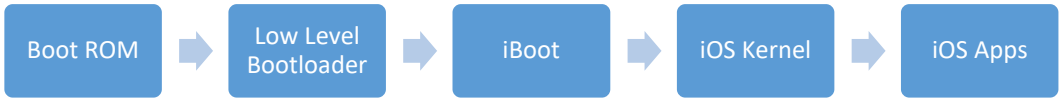
Şekil 3.17. Axiom'da cihaz seçme ekranı

- İmaj alma tipi burada *Hızlı* ve *Tam* olarak kullanıcıya sunulur. Mantıksal imaj almak için hızlı olan seçilir.
- Kullanıcıdan Var ise iTunes yedekleme şifresi istenir. Şifre varsa girilir yoksa boş geçilir.
- Sonrasında *iPhone 6s* cihazı seçilerek *Kanıtı analiz et* seçeneği ile mantıksal imaj oluşturulur.

3.3.2.2 Fiziksel İmaj Alımı

Herhangi bir cihazın fiziksel imajını elde etmek, orijinal cihazın belleğinin bit-bit kopyasını tam olarak çıkarmak demektir. Fiziksel imajın alınabilmesi için iOS cihazın jailbreak edilmesi gerekir. Jailbreak Apple ürünlerinin iOS işletim sistemi dosyalarına erişmek için kullanılan bir tekniktir [42]. iOS işletim sistemi yüklü Apple ürünleri, işletim sisteminin ayarlarını kasıtlı olarak veya istemeyerek değiştirerek ve hatalara neden olmaktan kaçınmak için kendi koruma mekanizmalarını uygulamıştır. Bu nedenle, kullanıcılar sistem dosyalarına ve ayarlarına doğrudan erişemez. Kullanıcılar en yüksek yetkiyi elde etmek, iOS sistem dosyasına erişmek ve GSM sağlayıcıları ve ağ kullanımları üzerindeki kısıtlamaların kilidini açmak için bu tekniği kullanmaktadırlar. iOS fiziksel imaj alabilmek için de bu teknik kullanılmaktadır.

iOS işletim sistemine sahip cihazların açılması, uygulamaların yüklenmesi ve çalıştırılması sırasında bir boot kontrol mekanizması bulunmaktadır. Boot zinciri olarak adlandırılan bu mekanizma; Apple tarafından, iOS cihazda sadece imzalı veya güvenilir kodun yüklenmesini sağlamaya çalışan bir sistemdir. Boot zinciri, birbirini tetikleyen ve her tetikleme esnasında izinsiz erişimin kontrol edildiği noktaların bulunduğu çeşitli modüllerden oluşmaktadır. Bu modüller Şekil 3.18'de verilmiştir.



Şekil 3.18. Boot kontrol mekanizması

Bootrom (Apple tarafından "SecureROM" olarak adlandırılır), bir iDevice üzerinde çalışan ilk koddur. Bootrom salt okunurdur. Bu modülde bir exploit ile yapılacak değişiklikler yalnızca donanım düzeyinde düzeltilebileceğinden bu modülde gerçekleştirilebilen jailbreakler en kuvvetli olanlardır. Yani bu modüldeki jailbreakler hiçbir yazılım güncellemesi ile devre dışı bırakılamaz. Bootrom LLB'yi çalıştırmadan önce LLB'nin imzasını kontrol eder.

Low Level Bootloader(Düşük seviyeli bootloader) yazılımın bir parçasıdır ve bazı başlangıç programlarını çalıştıran modüldür. Firmware sürüm 2.0 ve üstü sürümlerde, önyükleme yapmadan önce iBoot modülünün imzasını kontrol eder. Bu modülde bir açıklık bulunduysa, Apple yeni bir firmware yazılım sürümünü yayınlayarak güvenlik açıklarını kapatabilir.

iBoot, 2. aşama önyükleyicidir. Kurtarma modunu çalıştırır. Kullanıcıya sunulan bir ara yüz mevcuttur. iBoot iOS Kernel modülünün imzasını kontrol eder.

iOS Kernel bir uygulama başlatıldığında geçerli bir imzaya sahip olup olmadığını kontrol eder. Kernel uygulamaların çalışmasını denetler ve düzenler. Kernel'den sonraki aşama iOS uygulamalarıdır. Günümüzde iOS işletim sistemine sahip tüm cihazlar sadece Apple tarafından, Apple Store ile sunulan Apple tarafından imzalanmış uygulamaları çalıştırabilmektedir. Ancak kullanıcılar Jailbreak yardımı bahsedilen bu doğrulama modüllerinden birisini değiştirerek cihaz üzerinde yönetici iznine sahip olabilir, imzasız uygulamalar kullanabilir ve cihazın tüm hafıza birimlerine erişim sağlayabilir. Bu yüzden

tüm delillere ulaşabilmek açısından jailbreak işlemi mobil cihaz adli incelemelerinde önemli bir yere sahiptir.

Uygulamada kullanılan iPhone 6S cihazı 11.3.1 işletim sistemine sahiptir. Bu işletim sistemi için geliştirilmiş olan bir jailbreak bulunamadığı için bu işlem gerçekleştirilememiştir. Dolayısı ile iOS cihazın fiziksel imajı alınamamıştır.

4. ANDROID İŞLETİM SİSTEMİNDE SOSYAL MEDYA UYGULAMALARININ ADLİ BİLİŞİM ANALİZİ

Bu bölümde Android işletim sistemine sahip bir mobil cihazda analizi yapılacak her bir uygulamanın yapısı incelenecek, adli bilişim açısından önemli olan bulgulara nasıl erişilebileceği ortaya konacaktır. Root edilen bir telefonda uygulama analizi, manuel elde etme ve adli bilişim araçları ile elde etme olarak iki farklı şekilde gerçekleştirilmiştir. Manuel elde etme telefona yüklenen bir dosya analiz programı yardımı ile root dizinine erişerek ilgili dosyalar bilgisayara aktarıldıktan sonra dosya tipine uygun editör programı ile okuyarak yapılabilmektedir. Bu işlem ticari yazılımın kolaylığını sunmaz fakat ticari yazılım maliyetinin yüksekliği düşünüldüğünde analiz yapacak kişiye önemli bir fırsat ortaya koyar. Uygulama yapısı incelendikten sonra, adli bilişim araçları yardımı ile alınan imajlardan uygulama verilerinin ne kadarına erişilebildiği bu bulgular ışığında inceleme yazılımlarının kullanışlılık açısından avantajları ve dezavantajları ifade edilecektir.

4.1 Manuel Elde Etme

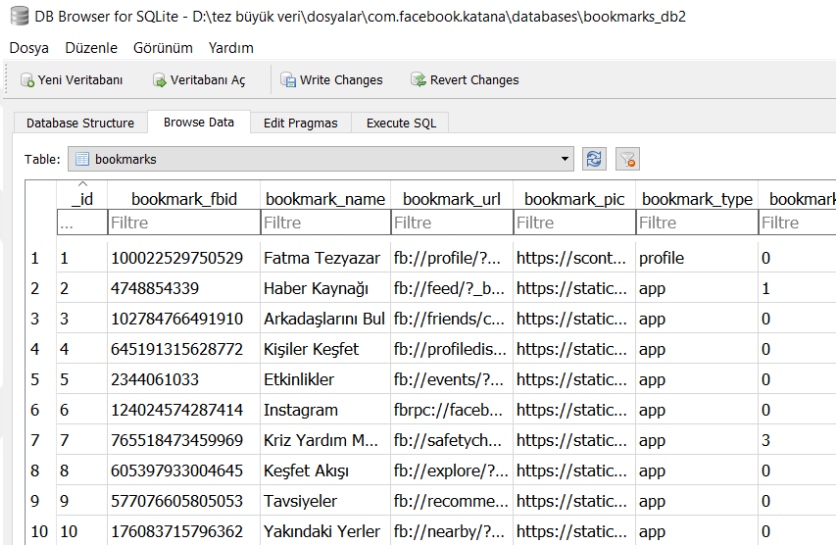
4.1.1 Facebook

Facebook mobil uygulamasının adli incelemesi için sadece fiziksel imaj alınarak ulaşılabilen "/data/data/com.facebook.katana" ve "/data/data/com.facebook.orca" klasörleri incelenmiştir. "/data/data/com.facebook.katana" klasörü Facebook uygulamasına ilişkin verileri barındırırken "/data/data/com.facebook.orca" Facebook Messenger uygulaması verilerini barındırır. Bu klasörler cache, files, databases klasörleri gibi alt dizinler içermektedir. "Cache" klasörleri önbellekte bulunan ses ve görüntü dosyalarını, "files" klasöründe uzantısız olarak video-cache dosyalarını, "databases" klasörleri iletişim kurulan kişilerin listesi, bildirimler listesi, kaydedilen videolar, sık kullanılanlara eklenen sayfalar, kurulan gruplar, yönetilen sayfalar, gibi birçok kişisel veri içeren veri tabanı dosyalarını içinde barındırmaktadır. Bu dizinler içerisinden mobil adli incelemelerde özellikle önem arz eden dosya ve klasörler bulunmaktadır. Bunlar aşağıda verilmiştir.

"/files/NewsFeed" klasörü kullanıcının ana sayfaya düşen video verilerini içermektedir. Ancak bu video dosyalarının kim tarafından gönderildiği bilgisi elde edilememektedir.

"/cache/image" klasörü kullanıcının ana sayfasında bulunan, kendi profilinden, bağlantı kurulan kişilerin profilinden ve görüntülenen diğer sayfalardan önbelleğe alınan resim dosyalarını bulunmaktadır. Bu dosyalar, ".cnt" uzantısı ile kaydedilmektedir.

"/databases" klasörü veritabanı dosyalarını bulundurur. "bookmarks_db2" veri tabanında kullanıcının abone olduğu sayfalar ve grupların listesini içermektedir. Bulunan verilerin bir kısmı Facebook uygulaması tarafından otomatik olarak oluşturulmakla birlikte kullanıcının kendisinin oluşturduğu veriler de bu veri tabanında bulunabilmektedir. Bu veri tabanının en önemli tablosu Şekil 4.1'de verilen "bookmarks" tablosudur.


DB Browser for SQLite - D:\tez büyük veri\dosyalar\com.facebook.katana\databases\bookmarks_db2

Dosya Düzenle Görünüm Yardım

Yeni Veritabanı | Veritabanı Aç | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: bookmarks

	_id	bookmark_fbid	bookmark_name	bookmark_url	bookmark_pic	bookmark_type	bookmark
	...	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	100022529750529	Fatma Tezyazar	fb://profile/?...	https://scont...	profile	0
2	2	4748854339	Haber Kaynağı	fb://feed/?_b...	https://static...	app	1
3	3	102784766491910	Arkadaşlarını Bul	fb://friends/c...	https://static...	app	0
4	4	645191315628772	Kişiler Keşfet	fb://profiledis...	https://static...	app	0
5	5	2344061033	Etkinlikler	fb://events/?...	https://static...	app	0
6	6	124024574287414	Instagram	fbrpc://faceb...	https://static...	app	0
7	7	765518473459969	Kriz Yardım M...	fb://safetych...	https://static...	app	3
8	8	605397933004645	Keşfet Akışı	fb://explore/?...	https://static...	app	0
9	9	577076605805053	Tavsiyeler	fb://recomme...	https://static...	app	0
10	10	176083715796362	Yakındaki Yerler	fb://nearby/?...	https://static...	app	0

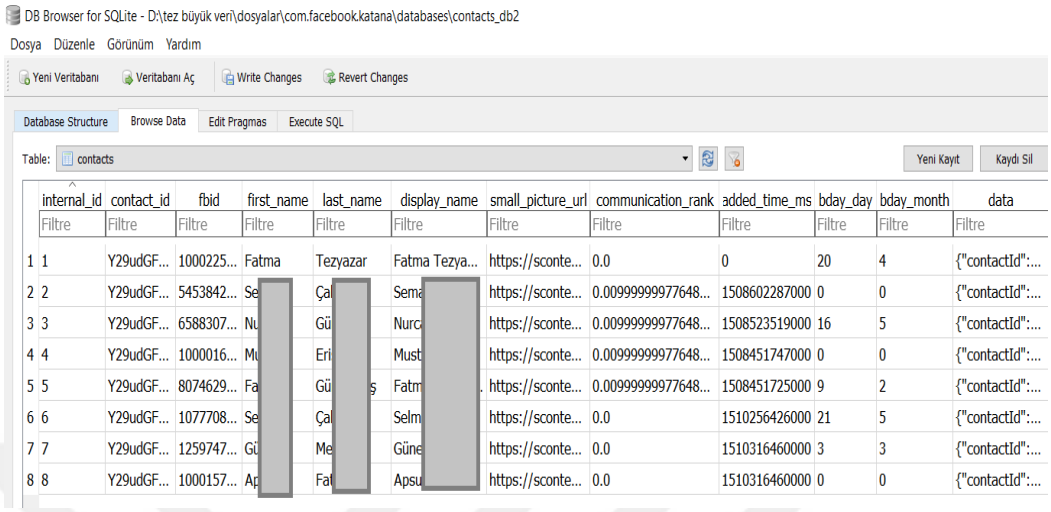
Şekil 4.1. Facebook bookmarks_db2 veritabanı bookmark tablosu

Tablo 4.1'de gösterildiği gibi bookmarks tablosunda; "bookmark_name" sütunu yer işareti isimlerini, "bookmark_url" sütunu yer işaretleri url'sini, "bookmark_pic" yer işareti ikonunun url'sini, "bookmark_type" sütunu yer işareti tipini içermektedir. "bookmark_unread_count" sütunu yer işaretinde kaç adet mesajın kullanıcı tarafından görülmediğini göstermektedir.

Tablo 4.1. Facebook bookmarks_db2 veritabanı bookmark tablosu sütun özellikleri

Sütun adı	Sakladığı değer
bookmark_fbid	Yer işareti id'si
bookmark_name	Yer işareti isimleri
bookmark_url	Yer işareti url'si
bookmark_pic	Yer işareti ikonunun url'si
bookmark_type	Yer işareti tipi
bookmark_unread_count	Yer işareti okunmamış mesaj adedi

“contacts_db2” veritabanı Şekil 4.2 de gösterildiği gibi kullanıcının bağlantı kurduğu kişiler ile ilgili tüm bilgileri tutmaktadır.



	internal_id	contact_id	fbid	first_name	last_name	display_name	small_picture_url	communication_rank	added_time_ms	bday_day	bday_month	data
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	Y29udGF...	1000225...	Fatma	Tezyazar	Fatma Tezya...	https://sconte...	0.0	0	20	4	{"contactId":...
2	2	Y29udGF...	5453842...	Se	Ça	Sema	https://sconte...	0.00999999977648...	1508602287000	0	0	{"contactId":...
3	3	Y29udGF...	6588307...	Nu	Gü	Nurc	https://sconte...	0.00999999977648...	1508523519000	16	5	{"contactId":...
4	4	Y29udGF...	1000016...	Mu	Eri	Must	https://sconte...	0.00999999977648...	1508451747000	0	0	{"contactId":...
5	5	Y29udGF...	8074629...	Fa	Gü ş	Fatm	https://sconte...	0.00999999977648...	1508451725000	9	2	{"contactId":...
6	6	Y29udGF...	1077708...	Se	Çal	Selm	https://sconte...	0.0	1510256426000	21	5	{"contactId":...
7	7	Y29udGF...	1259747...	Gü	Me	Güne	https://sconte...	0.0	1510316460000	3	3	{"contactId":...
8	8	Y29udGF...	1000157...	Ap	Fat	Apsu	https://sconte...	0.0	1510316460000	0	0	{"contactId":...

Şekil 4.2. Facebook contacts_db2 veritabanı contacts tablosu

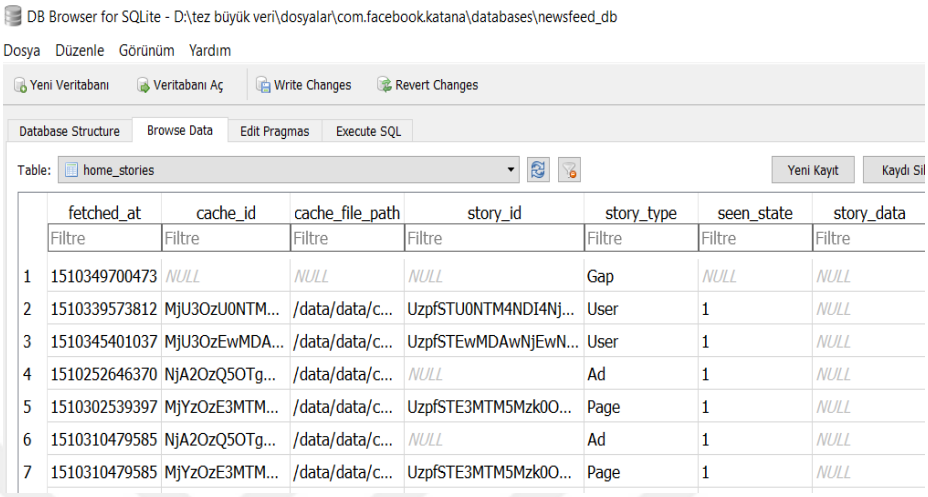
“contacts” tablosu sütunlarının içerikleri Tablo 4.2‘de verilmiştir. “fbid” sütunu diğer veritabanlarındaki kişileri tanımlamak için kullanılan benzersiz kimlikleri içermektedir. “first_name”,” last_name”, “display_name” sütunları kişilerin isimlerini gösterir. “The small_picture_url”, “big_picture_url”, “huge_picture_url” sütunları kişilerin profil resimlerinin linklerini içerir. “Communication_rank sütunu”, kişinin kullanıcıyla mesajlar, yorumlar ve olası diğer faktörler hesaba katılarak ne sıklıkta iletişim kurduğunu belirten oranları içerir.“Added_time_ms” sütunu, kişinin arkadaş olarak eklenme zamanını içerir. “Bday_day” ve “bday_month” sütunları kişinin doğum tarihini gün ve ay olarak gösterir. “Data” sütunu veri tabanındaki tüm verilerin bir kopyası ile birlikte kişilerin konum bilgisini içerir.

Tablo 4.2. Facebook contacts_db2 veritabanı contacts tablosu sütun özellikleri

Sütun adı	Sakladığı değer
contact_id	Kullanıcılar arası iletişime atanan id
fbid	Facebook tarafından kullanıcıya atanan id
first_name	İletişim kurulan kişinin ismi
last_name	İletişim kurulan kişinin Soy isimi
display_name	İletişim kurulan kişinin profilde görüntülenen isim
the small_picture_url	İletişim kurulan kişinin profil resim linki
communication_rank	İletişim kurulan kişi ile iletişim sıklığı oranı
added_time_ms	İletişim kurulan kişi ile arkadaş olma zamanı
bday_day	İletişim kurulan kişinin doğum günü
bday_month	İletişim kurulan kişinin doğum ayı
data	Veri tabanındaki tüm verilerin bir kopyası

“newsfeed_db” ana sayfada kullanıcıya gösterilen verileri içeren veri tabanıdır.

Şekil 4.3‘de verilen veri tabanı uygulamanın kullanımına göre çok büyük boyutta veri içerebilmektedir.



	fetched_at	cache_id	cache_file_path	story_id	story_type	seen_state	story_data
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1510349700473	NULL	NULL	NULL	Gap	NULL	NULL
2	1510339573812	MjU3OzU0NTM...	/data/data/c...	UzpfSTU0NTM4NDI4Nj...	User	1	NULL
3	1510345401037	MjU3OzEwMDA...	/data/data/c...	UzpfSTEwMDAwNjEwN...	User	1	NULL
4	1510252646370	NjA2OzQ5OTg...	/data/data/c...	NULL	Ad	1	NULL
5	1510302539397	MjYzOzE3MTM...	/data/data/c...	UzpfSTE3MTM5Mzk0O...	Page	1	NULL
6	1510310479585	NjA2OzQ5OTg...	/data/data/c...	NULL	Ad	1	NULL
7	1510310479585	MjYzOzE3MTM...	/data/data/c...	UzpfSTE3MTM5Mzk0O...	Page	1	NULL

Şekil 4.3. Facebook newsfeed_db veritabanı home_stories tablosu

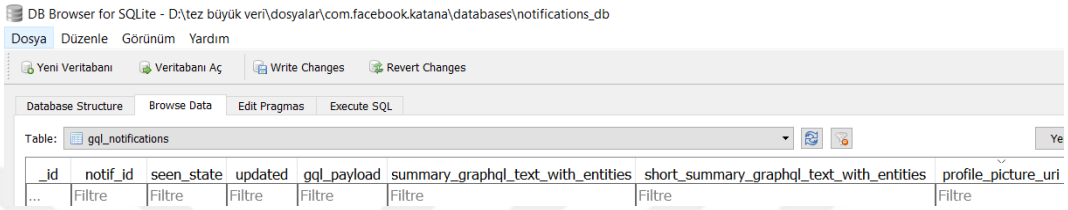
Tablo 4.3’de bu tablonun sütun özellikleri verilmiştir. Burada “fetched_at” sütunu, gönderilerin sunuculardan çekildiği zamanı gösterir ve kullanıcının uygulamayı kullandığı veya gönderiyi gördüğü zamanla ilişkilidir. “story_data” sütunu, veri bloğu olarak depolanan gönderiyi içerir. Bir hex veya metin editöründe görüntülendiğinde, gönderiyi gönderen kişinin kullanıcı adı bulunabilir ancak bu sütunda yapılan uygulamada herhangi bir veri bulunamamıştır. “cache_file_path” sütununda gönderiler ve işlemlerle ilgili önbelleğe alınan dosyaların veri yolları bulunmaktadır. Bu dosyalar bulunarak hex editör ile incelendiğinde gönderi ile ilgili bilgilere ulaşılabilmektedir.

Tablo 4.3. Facebook newsfeed_db veritabanı home_stories tablosu sütun özellikleri

Sütun adı	Sakladığı değer
fetch_at	Gönderilerin sunuculardan çekildiği zaman
cached_id	Gönderinin önbellekteki id’si
cache_file_path	Gönderilerle ilgili önbelleğe alınan dosyanın veri yolu
story_id	Gönderi id’si
story_type	Gönderi tipi
seen_state	Gönderinin görülme durumu
story_data	Veri bloğu olarak depolanan gönderi

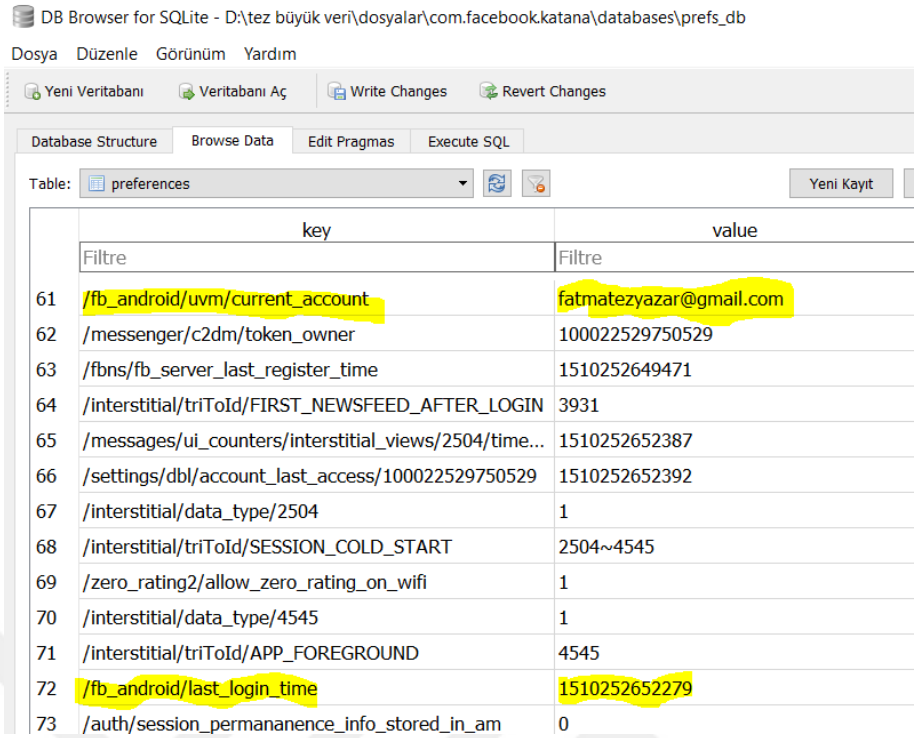
“notifications_db” veri tabanı bildirimler ile ilgili bilgileri barındırır. “gql_notifications” tablosundaki “seen_state” sütunu, bildirimin görünüp görünmediğini gösterir.”updated”, bildirimin okunmamışsa ne zaman gönderildiğini, okunmuşsa ne zaman

okunduğunu Linux epoch formatında gösteren sütundur. Gql_payload sütunu, newsfeed_db dosyasındaki story_data sütununa benzer şekilde gönderenin yanı sıra bildirimin içeriğini de içerir. Bildirim metni "summary_graphql_text_with_entities" ve "short_summary_graphql_text_with_entities" sütunlarından daha kolay bir şekilde elde edilebilmektedir. "profile_picture_url" gönderenin profil resmini görüntülemek için herkese açık bir URL içerir. Şekil 4.4'de görüldüğü gibi tez için oluşturulan çalışmada bildirim olmadığı için bu veritabanı boş gelmiştir.



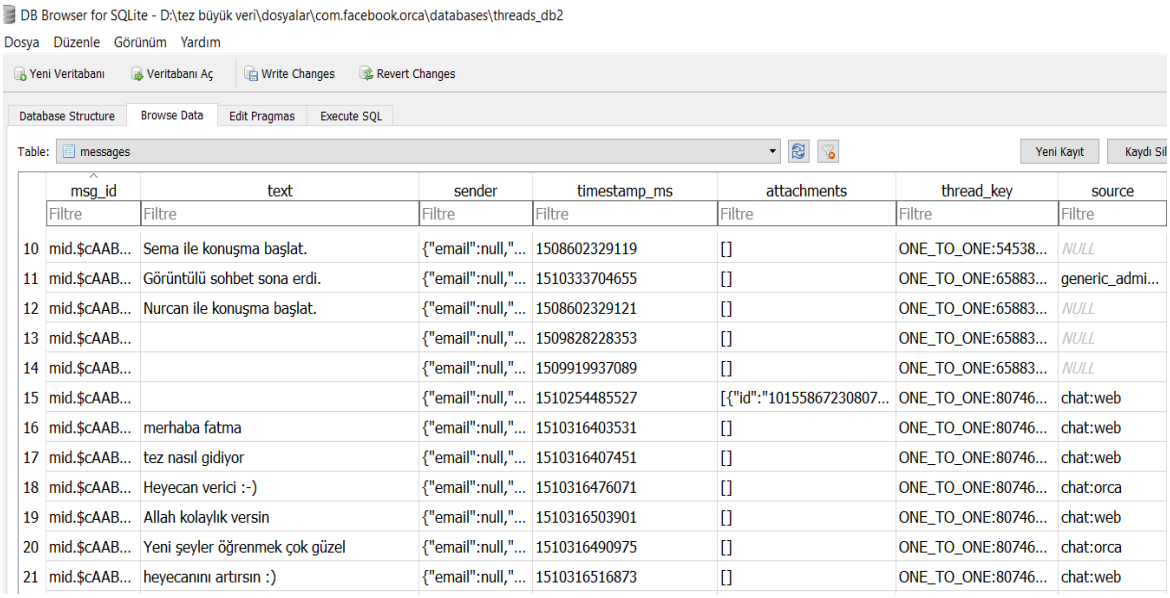
Şekil 4.4. Facebook notifications_db veritabanı gql_notifications tablosu

"prefs_db" veri tabanı uygulama ayarlarını Şekil 4.5'de gösterilen "preferences" tablosunda kaydeder. Ayarlar isimleri "key" sütununda bulunurken "value" sütununda ayarın aldığı değer bulunmaktadır. Adli incelemelerde önemli olan kullanım zaman bilgileri bu veri tabanında fazlaca yer almaktadır. "/config/gk/last_fetch_time_ms" satırı uygulamanın en son Facebook sunucuları ile iletişime geçtiği bilgisini tutan zaman damgasını gösterir. Ancak bu bilgi her zaman kullanıcının uygulamayı bu zamanda kullandığını garanti etmez kullanıcının uygulamayı son kullandığı zaman bilgisi "/fb_android/user_last_used_app_time" satırında yer almaktadır. "/fb_android/last_login_time" satırı kullanıcının uygulama üzerinde en son ne zaman giriş yaptığını gösterir. Bunun gibi zaman bildiren birçok veriyle birlikte uygulamanın kullanım profili elde edilebilmektedir. "/audience_prefs/selected_voice_name" satırında ise kullanıcının ismi, "/fb_android/uvm/current_account" satırında e-mail adresi bulunmaktadır.



Şekil 4.5. Facebook prefs_db veritabanı preferences tablosu

"threads_db2" com.facebook.orca klasörü içerisinde yer alır. Bu veritabanın Şekil 4.6 'de verildiği gibi Facebook Messenger ile ilgili iletişim kurulan kişiler veya gruplar, mesaj içerikleri gibi veriler içermektedir. İletişim kurulan kişilerin listesi "thread_users" tablosunda bulunurken, mesaj içerikleri ve arama bilgileri "messages" tablosunda yer almaktadır.



Şekil 4.6. Facebook threads_db veritabanı messages tablosu

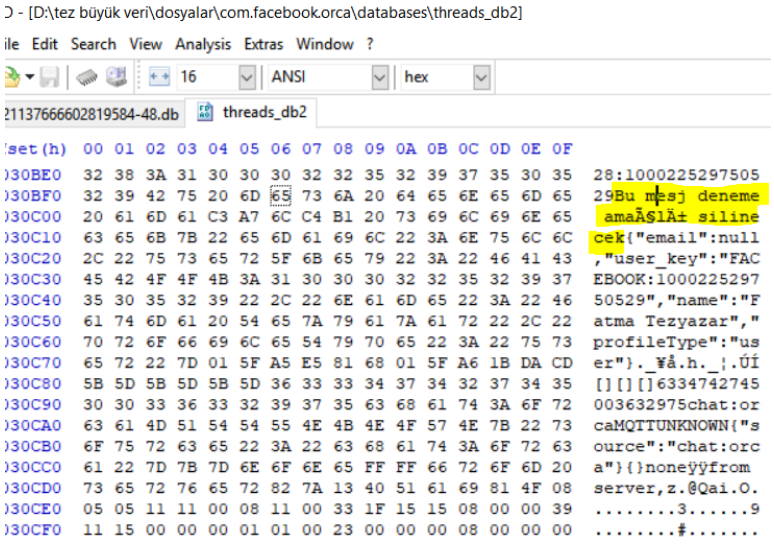
Tablonun sütun özellikleri Tablo 4.4'de yer almaktadır. Kullanıcıya gelen ve kullanıcı tarafından gönderilen her mesaj için benzersiz bir kimlik oluşturularak "msg_id" sütununda kaydedilmektedir. Mesajların açık hali "text" sütununda bulunmaktadır. Bunların yanında mesajı gönderen kişinin ismi, mesaj ekleri, mesajın gönderilme veya alınma zamanı, grup veya kişi arasında geçtiği, mesajın uygulama veya web sitesi ile gönderildiği bilgileri sırasıyla "sender", "attachmets", "timestamp_ms", "thread_key" ve "source" sütunlarında bulunmaktadır.

Tablo 4.4. Facebook threads_db veritabanı messages tablosu sütun özellikleri

Sütun adı	Sakladığı değer
msg_id	Her mesaj için benzersiz bir id
text	Mesaj içeriği
sender	Mesajı gönderen kişinin ismi
attachmets	Mesaj ekleri
timestamp_ms	Mesajın gönderilme veya alınma zamanı
thread_key	Mesajlaşma taraflarının grup veya kişi id'leri
source	Mesaj kaynağı

"call_logs_db" veritabanı yapılan aramalara ilişkin log kayıtlarını tutar. Buradaki "user_table" tablosu arama zamanı ve ne kadar sürdüğü ile ilgili bilgileri barındırmaktadır.

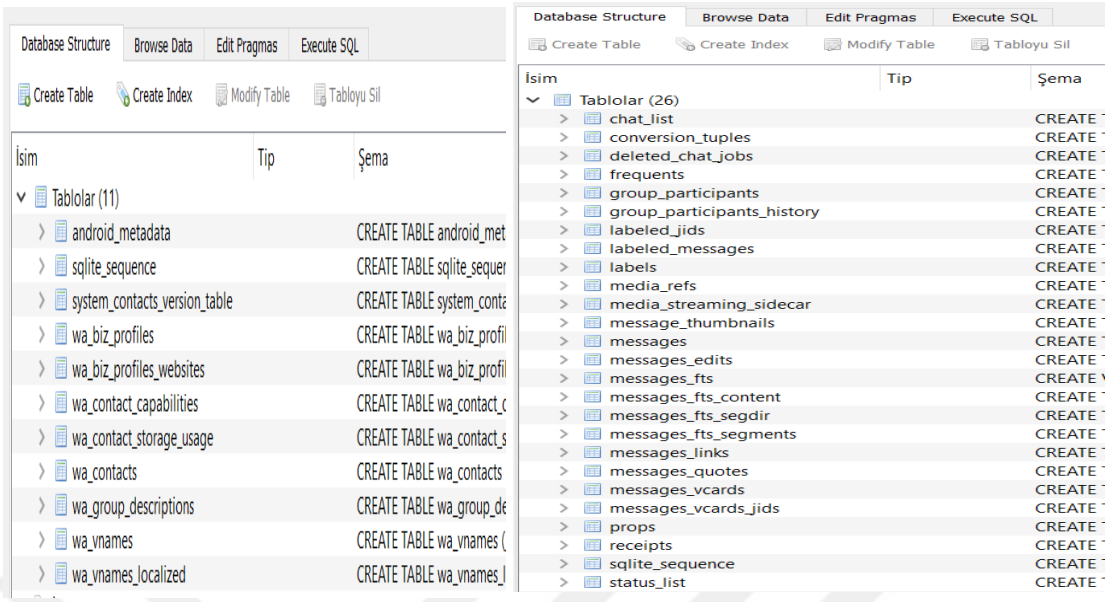
Kullanıcı davranışlarından olan silinen mesajları bulmak için threads_db veri tabanı hexadecimal olarak görüntülendiğinde, Şekil 4.7'deki gibi silinen mesaja erişilebildiği tespit edilmiştir.



Şekil 4.7. Facebook silinen mesaj görüntüsü

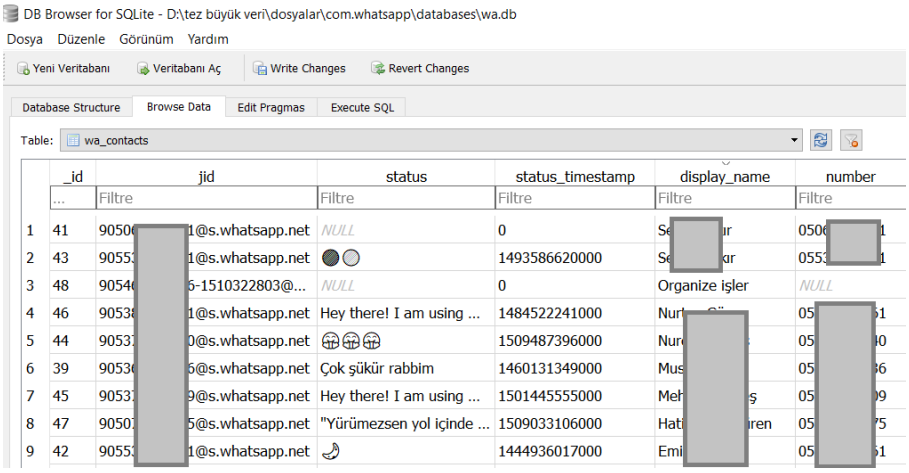
4.1.2 WhatsApp Messenger

Android cihazlarda WhatsApp uygulamasının verilerine fiziksel imajdan /data/data/com.whatsapp/databases/ klasörü altındaki veri tabanlarından ulaşılabilmektedir. Buradaki “mgstore.db” ve “wa.db” SQLite veri tabanları mobil adli bilişim açısından önem arz eden kullanıcı etkileşimine dair verileri barındırmaktadır. “wa.db” WhatsApp kişileri hakkında detaylı bilgiler barındırırken , “msgstore.db” bir kullanıcı ve kişiler arasındaki sohbet görüşmeleri hakkında ayrıntılı bilgileri saklar. “wa.db” ve “msgstore.db” veri tabanlarının tabloları Şekil 4.8 verilmiştir.



Şekil 4.8. Whatsapp wa.db ve msgstore.db veritabaları tabloları

"wa.db" veri tabanı incelendiğinde tablolardan en önemlisi olan "wa_contacts" tablosunun Şekil 4.9'de görüldüğü gibi kişi bilgilerini barındırdığı görülmektedir. WhatsApp, kullanıcının telefon rehberindeki bilgileri kendi veritabanında depolar ve kişilerin WhatsApp kullanıcıları olması durumunda adlarını ve telefon numaralarını ve durumlarını bu tabloya depolar.



Şekil 4.9. WhatsApp wa.db veritabanı wa_contacts tablosu

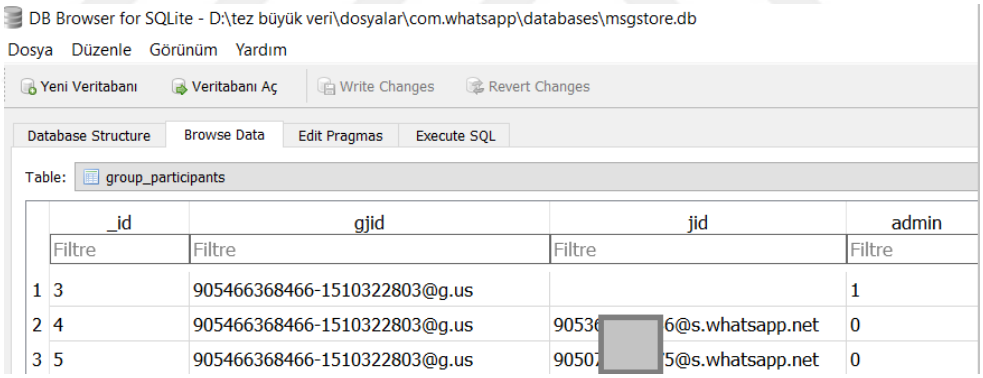
Tablo 4.5'de görüldüğü gibi jid, durum bilgisi, durum zaman bilgisi, kişi ismi, telefon numarası tablo sütunlarında yer almaktadır. Jid bilgisi WhatsApp uygulamasının kullanıcılarına ve guruplara atadığı bir kimliktir. Kullanıcılar için "kullanıcının telefon

numarası @s.whatsapp.net” şeklinde gruplar için ise “grubu kuran kişinin telefon numarası @g.us” şeklinde atanır.

Tablo 4.5. WhatsApp wa.db veritabanı wa_contacts tablosu sütun özellikleri

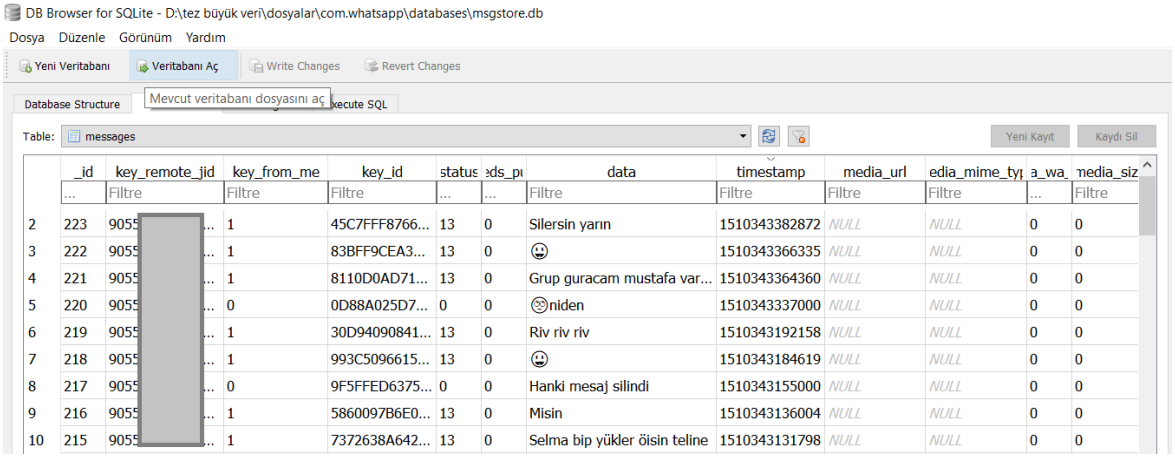
Sütun adı	Sakladığı değer
jid	Whatsapp tarafından kişiye ya da gruba atanan id
status	Kişi durum bilgisi
Status_timestamp	Durumun en son güncelleme zamanı
Display_name	Kişinin görünen ismi
number	Kişi telefon numarası

“msgstore.db” veri tabanı incelendiğinde ise “chat_list” tablosu iletişime geçilen kişilerin bilgilerini içermektedir. Buradaki “key_remote_jid” sütunu, kullanıcının iletişim kurduğu her hesabı telefon numarası ile başlayacak şekilde, iletişim kurulan bir grup ise grup numarası ile başlayacak şekilde depolamaktadır. “group_participants” tablosu grupların üye bilgilerini depolamaktadır. Şekil 4.10’da görüldüğü gibi “gjid” sütunu group idsini, “jid” sütunu gruba dahil olan kişilerin id’lerini, “admin” sütunu ise grubu kuran kişinin karşısında 1 diğerleri için 0 değerini içerir.



Şekil 4.10. WhatsApp mgstore veritabanı groups_participants tablosu

“messages” tablosu Şekil 4.11’de verildiği üzere, mesajlaşma kayıtlarının detaylarını bulundurmaktadır.



	_id	key_remote_jid	key_from_me	key_id	status	...ds_pi	data	timestamp	media_url	...edia_mime_typ	...a_wa_	...media_siz
	...	Filtre	Filtre	Filtre	...	...	Filtre	Filtre	Filtre	Filtre	...	Filtre
2	223	9055...	1	45C7FFF8766...	13	0	Silersin yarın	1510343382872	NULL	NULL	0	0
3	222	9055...	1	83BFF9CEA3...	13	0	😀	1510343366335	NULL	NULL	0	0
4	221	9055...	1	8110D0AD71...	13	0	Grup guracam mustafa var...	1510343364360	NULL	NULL	0	0
5	220	9055...	0	0D88A025D7...	0	0	😢niden	1510343337000	NULL	NULL	0	0
6	219	9055...	1	30D94090841...	13	0	Riv riv riv	1510343192158	NULL	NULL	0	0
7	218	9055...	1	993C5096615...	13	0	😀	1510343184619	NULL	NULL	0	0
8	217	9055...	0	9F5FFED6375...	0	0	Hanki mesaj silindi	1510343155000	NULL	NULL	0	0
9	216	9055...	1	5860097B6E0...	13	0	Misin	1510343136004	NULL	NULL	0	0
10	215	9055...	1	7372638A642...	13	0	Selma bip yükler öisin teline	1510343131798	NULL	NULL	0	0

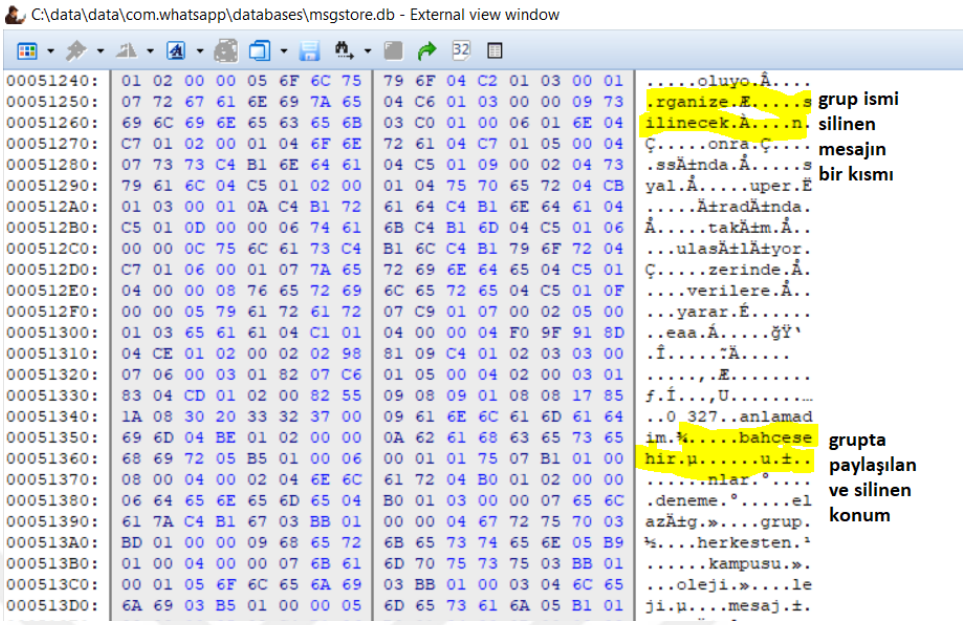
Şekil 4.11. WhatsApp mgstore veritabanı messages tablosu

"Messages" tablosunun sütun detayları Tablo 4.6'da verilmiştir. Burada "key_remote_jid" sütunu "wa.db" veri tabanında bahsedilen ile aynıdır. "Key_from_me" sütunu mesajın yönünü belirtir. Bu değer 0 ise alınan, 1 ise gönderilen olduğunu ifade eder. "data" sütunu mesaj metnini içerir. "timestamp" sütunu ise Linux epoch formatında gönderilen veya alınan zamanı içermektedir. Ayrıca gönderilen mesajların sunucuya ve karşı tarafa, alınan mesajların sunucuya ve kullanıcıya iletildiği zamanlar da ayrı ayrı sütunlarda zaman damgası olarak saklanmaktadır. Gönderilen ya da alınana ekler ile ilgili olarak "media_mime_type" dosya formatını içermektedir. "media_size" ve "media_name" sütunları eklenen dosyanın boyutunu ve ismini içerir. Ek bir konum ise, "latitude" ve "longitude" sütunlarında saklanır.

Tablo 4.6. WhatsApp mgstore veritabanı messages tablosu sütun özellikleri

Sütun adı	Sakladığı değer
key_remote_jid	Whatsapp tarafından kişiye ya da gruba atanan id
key_from_me	Mesajın yönü (0 ise alınan, 1 ise gönderilen)
data	Mesaj içeriği
timestamp	Gönderilme veya alınma zamanı
media_mime_type	Ekteki dosya formatı
media_size	Ekteki dosya boyutunu
media_name	Dosya ismi
latitude longitude	Ek konum ise enlem boylam

Silinen mesajlar için mgstore.db veritabanı hexadecimal olarak incelendiğinde, guruba atılan ve silinen text mesajının ve konum bilgisinin Şekil 4.12'deki gibi görüntülenebildiği tespit edilmiştir.



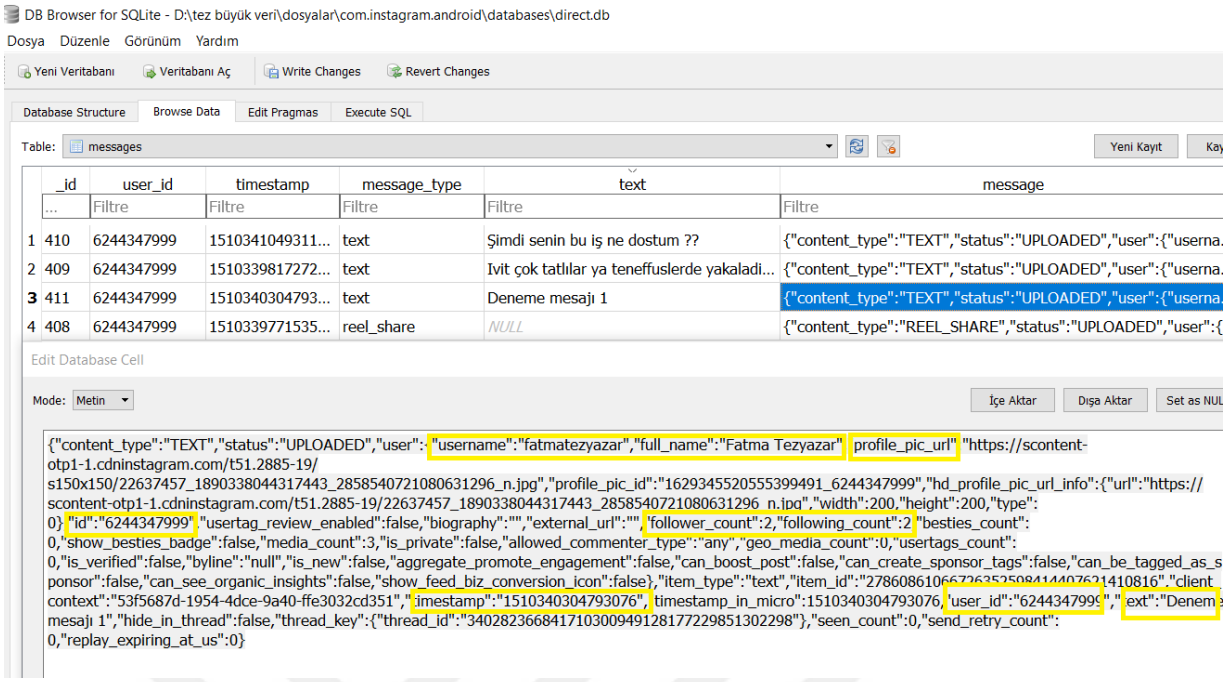
Şekil 4.12. WhatsApp silinen mesaj görüntüsü

WhatsApp uygulamasının genel medya saklama standardına bakıldığında ise/ Sdcard / WhatsApp / Media klasörü her bir medya türü için (Ses, Çağrılar, Görüntüler, Video ve Sesli mesajlar) bir klasör içerdiği görülür ve bu türdeki tüm ekleri klasörde saklar. Gönderilen medya ise Sent dizinde saklanır. Alınan medya ise direk o klasörde saklanır.

4.1.3 Instagram

Instagram mobil uygulamasının adli analizi için sadece fiziksel imaj alınarak ulaşılabilen /data/data/com.instagram.android klasörü ve /data/media/0/Android/data/com.instagram.android/ klasörü incelenmiştir. /data/data/com.instagram.android klasörü cache, files, databases, shared_prefs klasörleri gibi alt dizinleri barındırır.

"databases" klasöründe Instagram uygulamasının SQLite veritabanında sakladığı tek dosya olan "direct.db" dosyası bulunmaktadır. Bu veri tabanı Şekil 4.13'deki gibi kişilerle olan mesajları detayları ile saklamaktadır.



Şekil 4.13. Instagram direct.db veritabanı messages tablosu

"direct.db" veritabanının "messages" tablosunun sütunlarının sakladığı değerler Tablo 4.7'de verilmiştir.

Tablo 4.7. Instagram direct.db veritabanı messages tablosu sütun özellikleri

Sütun adı	Sakladığı değer
User_id	Instagram tarafından kişiye atanan id
timestamp	Mesajın gönderilme zamanı
message_type	
text	Mesaj içeriği
message	Mesaj ve mesajı gönderen kişiye ilişkin tüm detayları barındırır.

Adli bilişim açısından önemli veriler bulunduran dosyaları barındıran diğer bir klasör "shared_prefs" dir. Bu klasör XML dosyaları bulundurur.

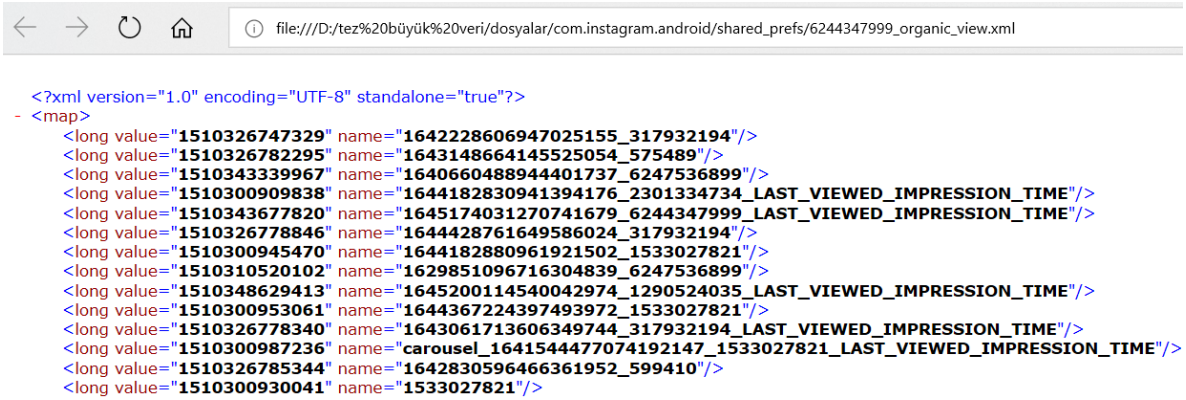
/shared_prefs/com.instagram.android_preferences.xml dosyası Şekil 4.14 kullanıcıya ait isim, biyografi, takipçi ve takip sayıları, profil resmi urlsi, kaç medya paylaştığı gibi detaylı bilgileri barındırmaktadır.

Şekil 4.14. Instagram com.instagram.android_preferences.xml dosyası

6244347999_USER_PREFERENCES.xml kullanıcının uygulama ile ilgili ayarlarını bulunduran, zamanları ile birlikte en son yapılan aramaları içeren, yüklenmiş hikayelerin zamanları damgaları gibi bilgileri barındıran bir dosyadır ve Şekil 4.15'de gösterilmiştir.

Şekil 4.15. Instagram 6244347999_USER_PREFERENCES.xml dosyası

6244347999_news_feed_notifications.xml dosyası yeni bildirimleri detayları ile içermektedir. 6244347999_video_view.xml dosyası izlenmiş videoların izlenme zamanları ile birlikte bulunduğu dosyadır. 6244347999_organic_view.xml dosyasında görüntülenen fotoğraflar ve videolar zaman damgaları ile birlikte bulunmaktadır ve Şekil 4.16 gibidir. 6244347999_AutoCompleteHashtagService.xml aranmış ve otomatik tamamlanan hashtaglerin bulunduğu dosyadır. unauthenticated.xml dosyası hangi hesap ile giriş yapıldığı kaç kez giriş işlemi denemesi yapıldığını tutan dosyadır.



Şekil 4.16. Instagram 6244347999_organic_view.xml dosyası

Instagram ile ilgili önemli veri bulunduran diğer bir dosya *MainFeed.json.0003* dosyasıdır /data/data/com.instagram.android/cache/ klasörü içerisinde bulunur. Bu dosya içerisinde kullanıcının ana sayfasına düşen medyaların URL'si, medyayı paylaşan kişinin kullanıcı ismi, profil resmi URL'si, hesabın gizli olup olmadığı, beğenilip beğenilmediği, yorum sayısı, zaman bilgisi, takip edilip edilmediği, toplam yorum sayısı, beğeni sayısı gibi detaylı bilgileri barındırmaktadır. Dosya içeriği Şekil 4.17 'de verilmiştir.

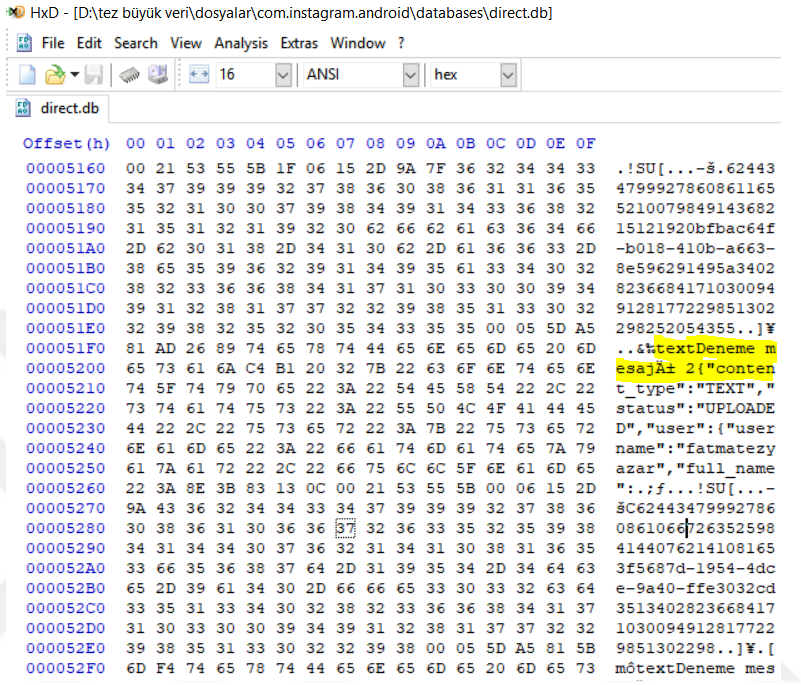
{"width": 240, "height": 300, "url": "https://scontent-otp1-1.cdninstagram.com/t51.2885-15/e35/p240x240/22802628_1686040838107681_6622354419516178432_n.jpg?ig_cache_key=MTYzNTQwNjA5ODE4MTQyNDc2NQ%3D%3D.2\u0026se=5"}]},
"original_width": 1080, "original_height": 1350, "user":
{"pk": 252054355, "username": "ftmgns", "full_name": "Fatma G\u00fcne\u015f", "is_private": true, "profile_pic_url":
"https://scontent-otp1-1.cdninstagram.com/t51.2885-19/11202988_826060930841316_428637984_a.jpg", "friendship_status":
{"following": true, "outgoing_request": false, "is_bestie":
false}, "is_verified": false, "has_anonymous_profile_picture":
false, "is_unpublished": false, "is_favorite": false},
"caption": {"pk": 17906101189042097, "user_id": 252054355,
"text": "Ne g\u00fczel gelmi\u015f buraya sonbahar \ud83c\udf42", "type": 1, "created_at": 1509175621,
"created_at_utc": 1509175621, "content_type": "comment",
"status": "Active", "bit_flags": 0, "user": {"pk": 252054355,
"username": "ftmgns", "full_name": "Fatma G\u00fcne\u015f",
"is_private": true, "profile_pic_url": "https://scontent-otp1-1.cdninstagram.com/t51.2885-19/11202988_826060930841316_428637984_a.jpg", "friendship_status": {"following": true,
"outgoing_request": false, "is_bestie": false}, "is_verified":
false, "has_anonymous_profile_picture": false,
"is_unpublished": false, "is_favorite": false},
"did_report_as_spam": false, "media_id": 1635406098181424765},
"caption_is_edited": false, "like_count": 93, "has_liked":
true, "top_likers": ["haticeksuren"], "comment_likes_enabled":
true, "comment_threading_enabled": true, "has_more_comments":
false, "max_num_visible_preview_comments": 2,
"preview_comments": [], "comment_count": 0, "photo_of_you":
false, "can_viewer_save": true, "organic_tracking_token":

Şekil 4.17. Instagram MainFeed.json.0003 dosyası

Instagram uygulamasının medya dosyalarının nasıl tutulduğunu incelemek gerekirse, /data/data/com.instagram.android/ cache kullanıcının Instagramda paylaştığı resimleri içermektedir. /data/data/com.instagram.android/cache/blur_icons dosyası paylaşılan resmin filtre seçeneklerini içerir. /data/data/com.instagram.android/cache/images/ klasörü

Instagram ile ilgili resim dosyalarını içermektedir. /data/media/0/Pictures/Instagram/ dosyası kullanıcının Instagramda paylaştığı resimleri içerir.

Silinen mesajların içeriğini görüntülemek için direct.db veritabanı hexadecimal görüntülenerek incelendiğinde ise Şekil 4.18'deki gibi görüntülendiği tespit edilmiştir.



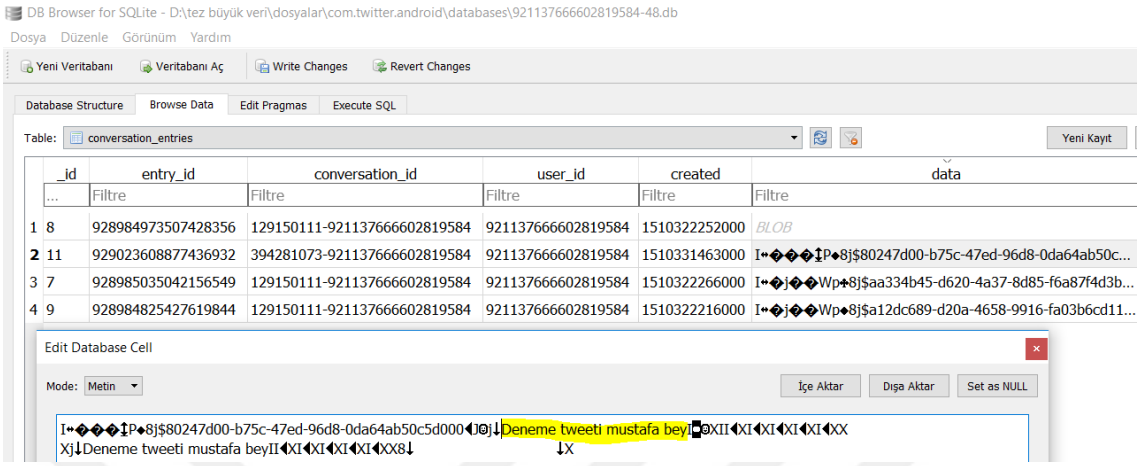
Şekil 4.18. Instagram silinmiş direk mesaj görüntüsü

4.1.4 Twitter

Twitter mobil uygulamasının adli analizi için sadece fiziksel imaj alınarak ulaşılabilen /data/data/com.twitter.android/ klasörü ve /data/media/0/Android/data/com.twitter.android/ klasörleri incelenmiştir. /data/data/com.twitter.android/ klasörü cache, files, databases, shared_prefs klasörleri gibi alt dizinleri barındırır. Bu dizinler içerisinden mobil adli incelemelerde özellikle önem arz eden dosya ve klasörler genel olarak /data/data/com.twitter.android/ klasörü altındaki databases içerisindeki veri tabanları, shared_prefs klasörü altındaki dosyalar ve /data/media/0/Android/data/com.twitter.android/ klasörü altındaki dosyalardır.

Databases klasöründe uygulamanın veri tabanları yer almaktadır. Bu veri tabanlarından 921137666602819584-48.db veri tabanındaki önemli bilgiler barındırmaktadır. Bu veri tabanı kullanıcının "user id" olarak geçen kullanıcı kimliği olan 921137666602819584 ile başlayarak isimlendirilmiştir. Buradaki "conversation_entiries" tablosu Şekil 4.19'da

gösterildiği gibi kullanıcının kişilerle yaptığı dm(direk message) olarak adlandırılan konuşmaların içeriğini ve Linux epoch formatında oluşturulma zamanını bulundurmaktadır.



Şekil 4.19. Twitter 921137666602819584-48.db veritabanı

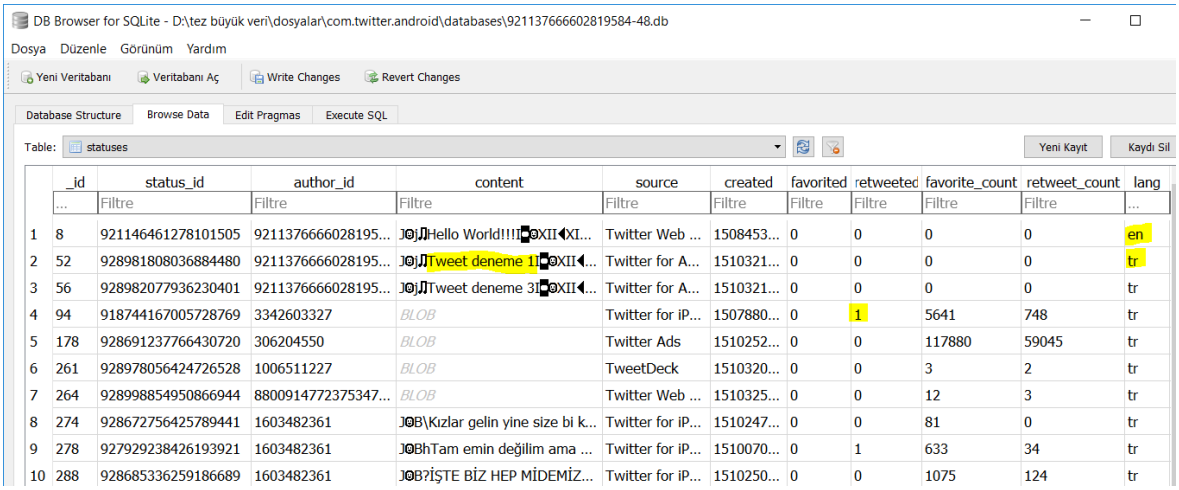
Tablonun sütun özelliklerinin sakladığı değerler Tablo 4.8'de yer almaktadır.

Tablo 4.8. Twitter 921137666602819584-48.db veritabanı conversation_entiries tablosu sütun özellikleri

Sütun adı	Sakladığı değer
entry_id	Mesaja atanan id
conversation_id	Mesajlaşan kullanıcıların user_id'lerini içeren id
user_id	Mesajı atan kişinin id'si
created	Mesajın oluşturulma zamanı
data	Mesaj içeriği

"conversation_participants" tablosu ise konuşmaların gerçekleştirildiği kişilerin kullanıcı kimliğini içerir. "Conversations" tablosu görüşmelerin kimliğini bulundurur. Buradaki "conservation_id" görüşmenin yapıldığı kişi ve kullanıcının kendi kimliğini içermektedir.

"statuses" tablosu Şekil 4.20'de gösterildiği gibi kişinin ana sayfasında düşen tweetleri içerir.



	_id	status_id	author_id	content	source	created	favorited	retweeted	favorite_count	retweet_count	lang
1	8	921146461278101505	9211376666028195...	JOjJHello World!!!I▪OXII◀XI...	Twitter Web ...	1508453...	0	0	0	0	en
2	52	928981808036884480	9211376666028195...	JOjJTweet deneme 1I▪OXII◀...	Twitter for A...	1510321...	0	0	0	0	tr
3	56	928982077936230401	9211376666028195...	JOjJTweet deneme 3I▪OXII◀...	Twitter for A...	1510321...	0	0	0	0	tr
4	94	918744167005728769	3342603327	*BLOB*	Twitter for iP...	1507880...	0	1	5641	748	tr
5	178	928691237766430720	306204550	*BLOB*	Twitter Ads	1510252...	0	0	117880	59045	tr
6	261	928978056424726528	1006511227	*BLOB*	TweetDeck	1510320...	0	0	3	2	tr
7	264	928998854950866944	8800914772375347...	*BLOB*	Twitter Web ...	1510325...	0	0	12	3	tr
8	274	928672756425789441	1603482361	JOB\Kızlar gelin yine size bi k...	Twitter for iP...	1510247...	0	0	81	0	tr
9	278	927929238426193921	1603482361	JOBhTam emin değilim ama ...	Twitter for iP...	1510070...	0	1	633	34	tr
10	288	928685336259186689	1603482361	JOB?İŞTE BİZ HEP MİDEMİZ...	Twitter for iP...	1510250...	0	0	1075	124	tr

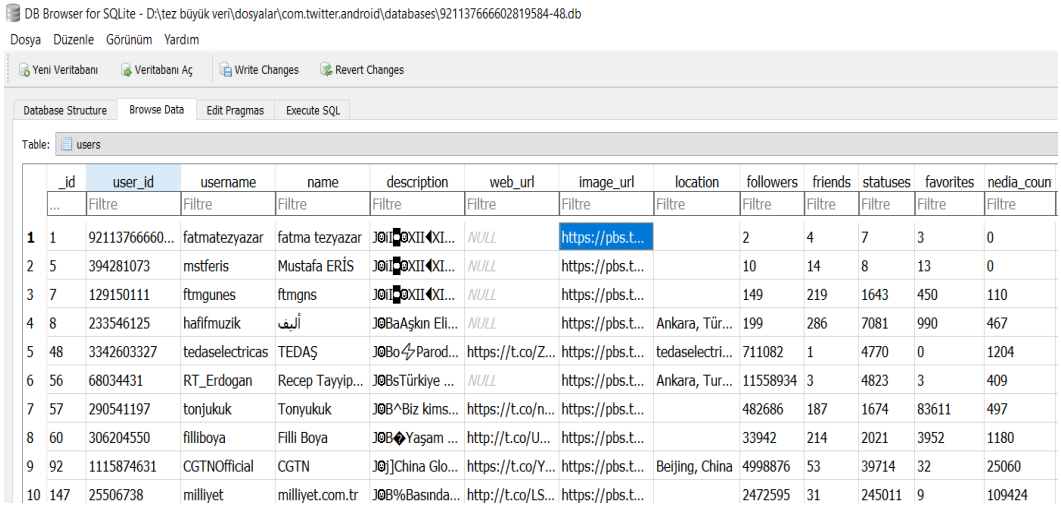
Şekil 4.20. Twitter 921137666602819584-48.db veritabanı statuses tablosu

Tablonun sütun özellikleri Tablo 4.9'da verilmiştir. "status_id" sütunu atılan tweetlerin her birine atanan benzersiz bir kimlik numarasını, "authour_id" sütunu tweeti atan kişinin kimliğini, "content" sütunu tweetin içeriğini, "source" sütunu twetin atıldığı kaynak bilgisini, "created" sütunu oluşturulma zamanını içerir. Ayrıca, kullanıcı tarafından favorilere eklenme bilgisini, retweet bilgisini, toplam beğeni, toplam retweet, tweet dili, eğer tweete konum eklendi ise enlem boylam bilgileri gibi bilgilerin bulunduğu sütunları da barındırmaktadır.

Tablo 4.9. Twitter 921137666602819584-48.db veritabanı statuses tablosu sütun özellikleri

Sütun adı	Sakladığı değer
status_id	Tweete atanan benzersiz id
author_id	tweeti atan kişinin kimliğini
content	tweetin içeriğini
source	tweetin atıldığı kaynak bilgisini
created	Tweetin oluşturma zamanı
favorited	Beğenilme durumu(1 ise beğenilmiş 0 isebeğenilmemiş)
retweeted	Retweet durumu(1 ise beğenilmiş 0 isebeğenilmemiş)
fovorit_count	Tweetin toplam beğenilme sayısı
retweet_count	Tweetin toplam retwetlenme sayısı
lang	Tweet dil bilgisi
latitude	Konum enlem bilgisi
longitude	Konum boylam bilgisi

"Users" tablosu Şekil 4.21'de gösterildiği üzere kullanıcının etkileşimde bulunduğu kişilerin bilgilerini bulundurmaktadır.



	_id	user_id	username	name	description	web_url	image_url	location	followers	friends	statuses	favorites	media_coun
	...	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	92113766660...	fatmatezyazar	fatma tezyazar	J◘i◘◘XII◀XI...	NULL	https://pbs.t...		2	4	7	3	0
2	5	394281073	mstferis	Mustafa ERİS	J◘i◘◘XII◀XI...	NULL	https://pbs.t...		10	14	8	13	0
3	7	129150111	ftmgunes	ftmgns	J◘i◘◘XII◀XI...	NULL	https://pbs.t...		149	219	1643	450	110
4	8	233546125	hafifmuzik	ألبف	J◘BaAşkın Eli...	NULL	https://pbs.t...	Ankara, Tür...	199	286	7081	990	467
5	48	3342603327	tedaselectricas	TEDAŞ	J◘Bo⚡Parod...	https://t.co/Z...	https://pbs.t...	tedaselectri...	711082	1	4770	0	1204
6	56	68034431	RT_Erdogan	Recep Tayyip...	J◘BsTürkiye ...	NULL	https://pbs.t...	Ankara, Tur...	11558934	3	4823	3	409
7	57	290541197	tonjukuk	Tonyukuk	J◘B^Biz kims...	https://t.co/n...	https://pbs.t...		482686	187	1674	83611	497
8	60	306204550	filliboya	Filli Boya	J◘B◆Yaşam ...	http://t.co/U...	https://pbs.t...		33942	214	2021	3952	1180
9	92	1115874631	CGTNOfficial	CGTN	J◘j]China Glo...	https://t.co/Y...	https://pbs.t...	Beijing, China	4998876	53	39714	32	25060
10	147	25506738	milliyet	milliyet.com.tr	J◘B%Basında...	http://t.co/LS...	https://pbs.t...		2472595	31	245011	9	109424

Şekil 4.21. Twitter 921137666602819584-48.db veritabanı users tablosu

Tablo 4.10'da tablonun sütun özellikleri verilmiştir. Kullanıcı ID'si, ismi kullanıcı ismi profilde tanımlı bilgiler profil resmi URL'si tanımlı ise konum bilgisi takipçi sayısı takip ettikleri toplam tweet sayıları, toplam beğeni sayısı, profilin oluşturulma zamanı en son güncelleme zamanı gibi bilgileri barındırır.

Tablo 4.10. Twitter 921137666602819584-48.db veritabanı users tablosu sütun özellikleri

Sütun adı	Sakladığı değer
user_id	Twitterın kullanıcıya atadığı benzersiz id
username	Kullanıcının benzersiz ismi
name	Kullanıcının ismi
description	Kullanıcının profilindeki tanımlama kısmı
web_url	Profil kısmında eklenen web sitesi
image_url	Profil resmi url'si
location	Profildeki konumu
followers	Toplam takipçi sayısı
friends	Takip ettiği kişi sayısı
statuses	Paylaştığı tweet sayısı
favorites	Kişinin toplam beğeni sayısı
media_count	Paylaşılan toplam medya sayısı

"0-scribe.db" veritabanı, scribe tablosundaki günlükleri ve kimlikleri içerir. "global.db" kullanıcının hesap bilgilerini barındırmaktadır.

"shared_prefs" dosyası ise içerisinde xml dosyaları barındırmaktadır. Bu dosyalar içerisinde com.twitter.android_preferences.xml, 921137666602819584.xml dosyaları twitter ayar ve seçenekler içermektedir.

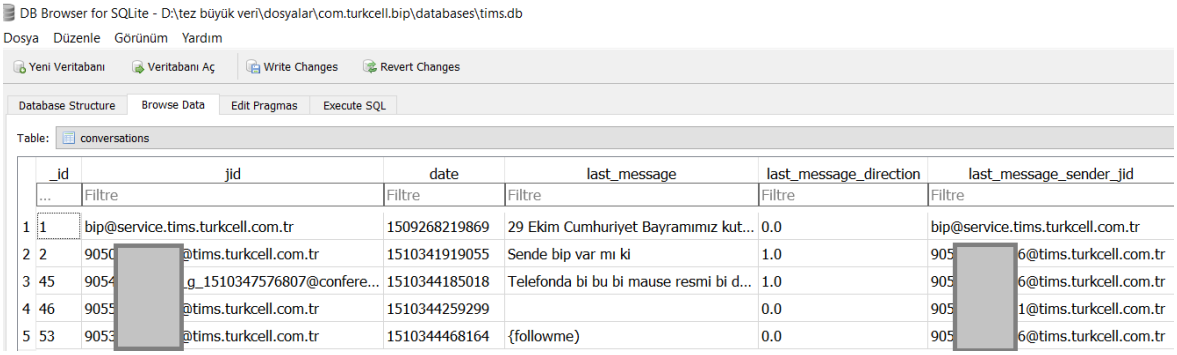
/data/media/0/Android/data/com.twitter.android/cache/ dosyasında ise multimedya dosyaları saklanmaktadır.

4.1.5 BiP Messenger

BiP uygulaması için mantıksal imaj incelendiğinde ilgili dosyaların Depolama/BiP klasörü altında bulunduğu görülmektedir. Audio klasörü altında Bip üzerinden gönderilen ve alınan ses verileri, Contact klasörü altında gönderilen ve alınan kişi kartvizit bilgisi, BİP klasörü altında gönderilen ve alınan resim, doküman gibi veriler, Bip Video gönderilen ve alınan video bilgilerini tutmaktadır. History klasörü altında ise Bip geçmişi ile ilgili veriler tutulmaktadır. Bip uygulaması yedekleme işlemini bulut depolama sistemi üzerinden yaptırdığı için kullanıcıya, cihazın içinde oluşabilecek bir yedekleme dosyasına izin vermemektedir.

Fiziksel imajdaki incelendiğinde ise uygulama verilerinin data/data/com.turkcell.bip klasörü altında bulunduğu görülmüştür. Bu klasör altındaki databases kalsöründe veritabanları yer alır ve bunlardan tims.db klasörü kullanıcı etkileşimleri ile ilgili önemli verileri barındırmaktadır. “Android_metadata” tablosu ülke bilgisini tutar.

Şekil 4.22’de verilen “Conversations” tablosunda, kullanıcının iletişime geçtiği kişilerin bilgisi tutulmaktadır. Burada “last_message” sütununda en son gelen veya gönderilen mesajın içeriği, “date” sütununda zamanı, “jid” sütununda gönderen jid(benzersiz kişi id bilgisi) , “last_message_direction” sütununda mesaj yönünü(0 ise gelen 1 ise giden) bulundurur. Tablo sütun özellikleri Tablo 4.11’de verilmiştir. Bu kısımda jid bilgisi uygulama tarafından belli bir formatta tutulmaktadır. Jid bilgisi kişi ise “KişininNumarası@tims.turkcell.com.tr”**,** grup ise “GrubuKuranKişiJidBilgisi_g_Grubun KurulduğuZaman@conference.tims.turkcell.com.tr “@conference.tims.turkcell.com.tr**”** **,** servis ise sonu “@service.tims.turkcell.com.tr” olarak belirlenir.



Şekil 4.22 Bip tims.db veritabanı conversations tablosu

Burada "last_message" sütununda en son gelen veya gönderilen mesajın içeriği, "date" sütununda zamanı, "jid" sütununda gönderen jid(benzersiz kişi id bilgisi) , "last_message_direction" sütununda mesaj yönünü(0 ise gelen 1 ise giden) bulundurur. Tablo sütun özellikleri Tablo 4.11'de verilmiştir. Bu kısımda jid bilgisi uygulama tarafından belli bir formatta tutulmaktadır. Jid bilgisi kişi ise "KişininNumarası@tims.turkcell.com.tr"**,** grup ise "GrubuKuranKişiJidBilgisi_g_GrubunKurulduğuZaman@conference.tims.turkcell.com.tr "@conference.tims.turkcell.com.tr"**,** servis ise sonu "@service.tims.turkcell.com.tr" olarak belirlenir.

Tablo 4.11 Bip tims.db veritabanı conversations tablosu sütun özellikleri

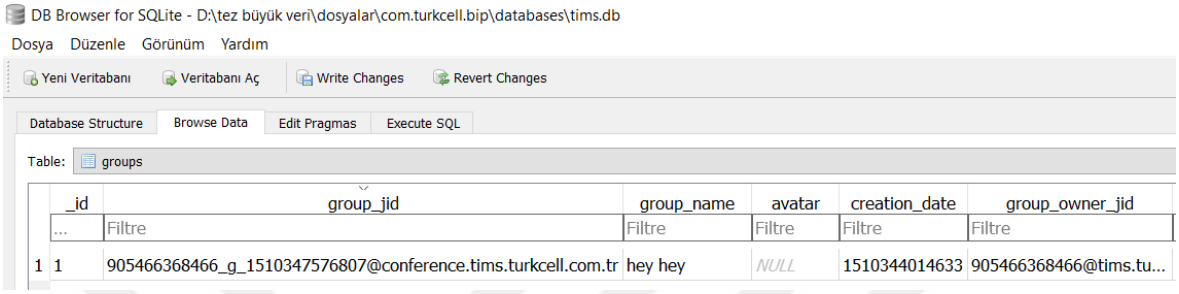
Sütun adı	Sakladığı değer
jid	BiP tarafından kullanıcılara verilen benzersiz id
date	Mesaj gönderme zamanı
Last_message	Son gönderilen mesaj içeriği
Last_message_direction	Son gönderilen mesajın yönü (0 ise gelen 1 ise giden)
Last_message_sender_jid	Konuşmadaki son mesajı gönderenin jid'si

"delivery_states" tablosu iletilen ve alınan mesajların durumlarını saklamaktadır. Tabloda "ds_jid" sütununda iletişim halinde olunan kullanıcı bilgileri, "deliver_date" sütununda gönderilen ve teslim alınan mesajların teslim edilme bilgileri ve "display_date" sütununda ise görülme zaman bilgileri tutmaktadır.

"follow_me_saved_sessions" tablosu ise takip et özelliğinin "jid" sütununda hangi kullanıcı ile takip özelliğinin başlatıldığı "start_time" sütünü başlatma zamanı ve "end_time" ise bitirme "duration" özelliğin ne kadar sürdüğü bilgilerini tutmaktadır. "follow_me_saved_locations" tablosunda ise konum bilgisi enlem boylam olarak saklıdır.

“group_participants” tablosunda “group_jid” sütununda grup bilgisi tutarken, “user_jid” ise gruba dahil olan kullanıcıların bilgileri tutulur.

“groups” tablosunda Şekil 4.23’de görüldüğü üzere “group_name” sütunu grup ismini, “avatar” sütunu gruba ait fotoğrafın resim adres yolunu, “creation_date” grubun oluşturulma tarihini ve “group_owner_jid” sütunu ise grubu oluşturan kişinin bilgisini tutmaktadır.


DB Browser for SQLite - D:\tez büyük veri\dosyalar\com.turkcell.bip\databases\tims.db

Dosya Düzenle Görünüm Yardım

Yeni Veritabanı | Veritabanı Aç | Write Changes | Revert Changes

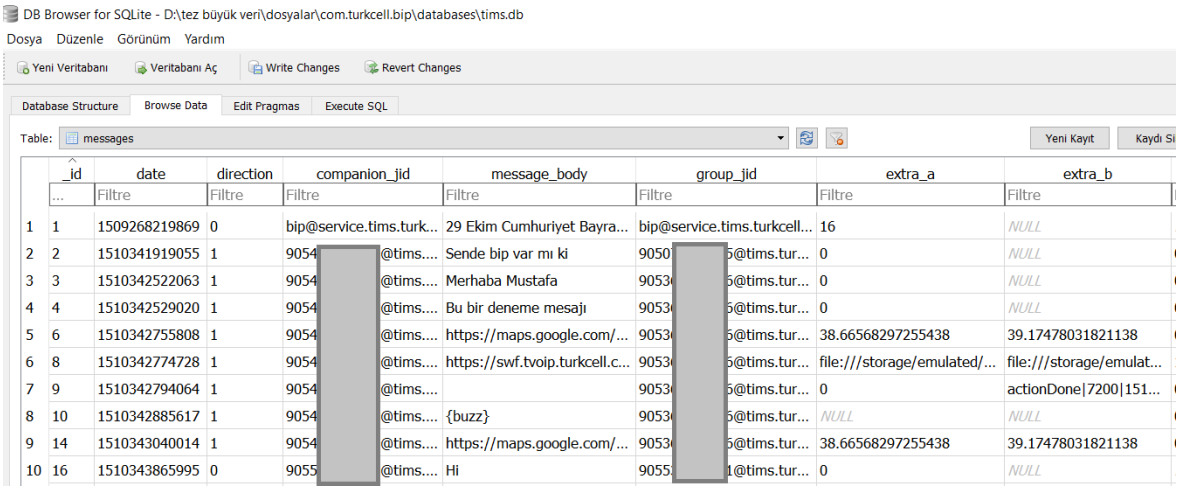
Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: groups

	_id	group_jid	group_name	avatar	creation_date	group_owner_jid
	...	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	905466368466_g_1510347576807@conference.tims.turkcell.com.tr	hey hey	NULL	1510344014633	905466368466@tims.tu...

Şekil 4.23. Bip tims.db veritabanı groups tablosu

“messages” tablosu Şekil 4.24’de verilmiştir, gönderilen ve alınan mesajlar ile ilgili bilgileri barındırır.


DB Browser for SQLite - D:\tez büyük veri\dosyalar\com.turkcell.bip\databases\tims.db

Dosya Düzenle Görünüm Yardım

Yeni Veritabanı | Veritabanı Aç | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages | Yeni Kayıt | Kaydı Si

	_id	date	direction	companion_jid	message_body	group_jid	extra_a	extra_b
	...	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	1	1509268219869	0	bip@service.tims.turk...	29 Ekim Cumhuriyet Bayra...	bip@service.tims.turkcell...	16	NULL
2	2	1510341919055	1	9054[redacted]@tims....	Sende bip var mı ki	9050[redacted]5@tims.tur...	0	NULL
3	3	1510342522063	1	9054[redacted]@tims....	Merhaba Mustafa	9053[redacted]5@tims.tur...	0	NULL
4	4	1510342529020	1	9054[redacted]@tims....	Bu bir deneme mesajı	9053[redacted]5@tims.tur...	0	NULL
5	6	1510342755808	1	9054[redacted]@tims....	https://maps.google.com/...	9053[redacted]5@tims.tur...	38.66568297255438	39.17478031821138
6	8	1510342774728	1	9054[redacted]@tims....	https://swf.tvoip.turkcell.c...	9053[redacted]5@tims.tur...	file:///storage/emulated/...	file:///storage/emulat...
7	9	1510342794064	1	9054[redacted]@tims....		9053[redacted]5@tims.tur...	0	actionDone|7200|151...
8	10	1510342885617	1	9054[redacted]@tims....	{buzz}	9053[redacted]5@tims.tur...	NULL	NULL
9	14	1510343040014	1	9054[redacted]@tims....	https://maps.google.com/...	9053[redacted]5@tims.tur...	38.66568297255438	39.17478031821138
10	16	1510343865995	0	9055[redacted]@tims....	Hi	9055[redacted]1@tims.tur...	0	NULL

Şekil 4.24. Bip tims.db veritabanı messages tablosu

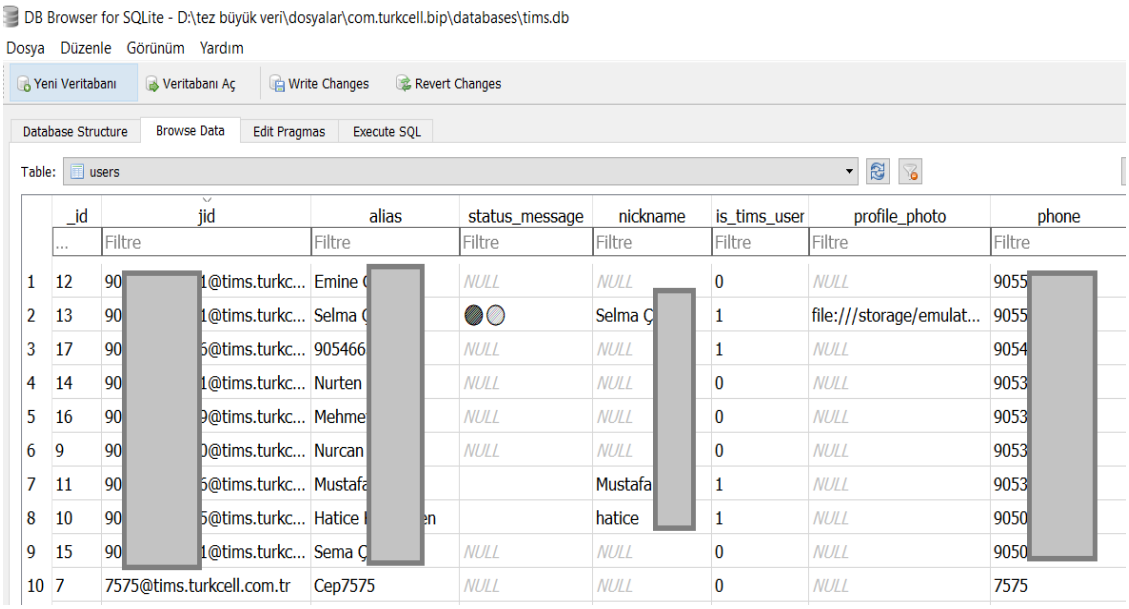
Tablo 4.12 incelendiğinde “date” sütununda mesaj zamanı, “direction” sütununda mesajın yönü (0 ise gelen 1 ise giden mesajdır.), “companion_jid” sütununda kişinin telefonu, “message_body” sütununda mesaj içeriği tutulduğu görülmektedir. Eğer bir ek var ise, “extra_a” ekte gönderilen dosya bir konum ise enlem bilgisini bir resim ise resmin yolunu, “exra_b” ekte gönderilen dosya konum ise boylam bilgisini resim ise resim yolunu tutar.

Tablo 4.12 Bip tims.db veritabanı messages tablosu sütun özellikleri

Sütun adı	Sakladığı değer
date	Mesajın gönderilme zamanı
direction	Mesajın yönünü (0 ise gelen 1 ise giden mesajdır.)
companion_jid	Mesajı gönderen tarafın jid bilgisi
message_body	Mesaj içeriği
extra_a	Ekte gönderilen dosya bilgisi
extra_b	Ekte gönderilen dosya bilgisi

"services" tablosunda BiP üzerinde yer alan sponsorların ve servis hizmetlerinin isimleri, jid bilgileri, servis id'leri, servislere ait görsellerin tutulduğu dizin adresi, servislerin reklam içeriklerini yer aldığı url adresinin adres bilgisi ve servislerin slogan bilgilerini tutulmaktadır.

Şekil 4.25'de verilen "users" tablosunda, kullanıcının telefonunda yer alan rehber numaralarının tümü yer almaktadır.



Şekil 4.25. Bip tims.db veritabanı users tablosu

Bu tablonun sütun özellikleri Tablo 4.13'de verilmiştir. Hangi kullanıcının BIP kullandığını, kullanan kişinin nickname bilgisini ve profil fotoğraflarının adres URL'sini tutmaktadır.

Tablo 4.13. Bip tims.db veritabanı user tablosu sütun özellikleri

Sütun adı	Sakladığı değer
alias	Kişi ismi
status_message	Kişi durum bilgisi
nick_name	Kişi takma ismi
is_tims_user	Bip uygulaması kullanıcısı mı(1 ise kullanıcı 0 ise değil)
profile_photo	Profil resmi dosya yolu
phone	Telefon numarası

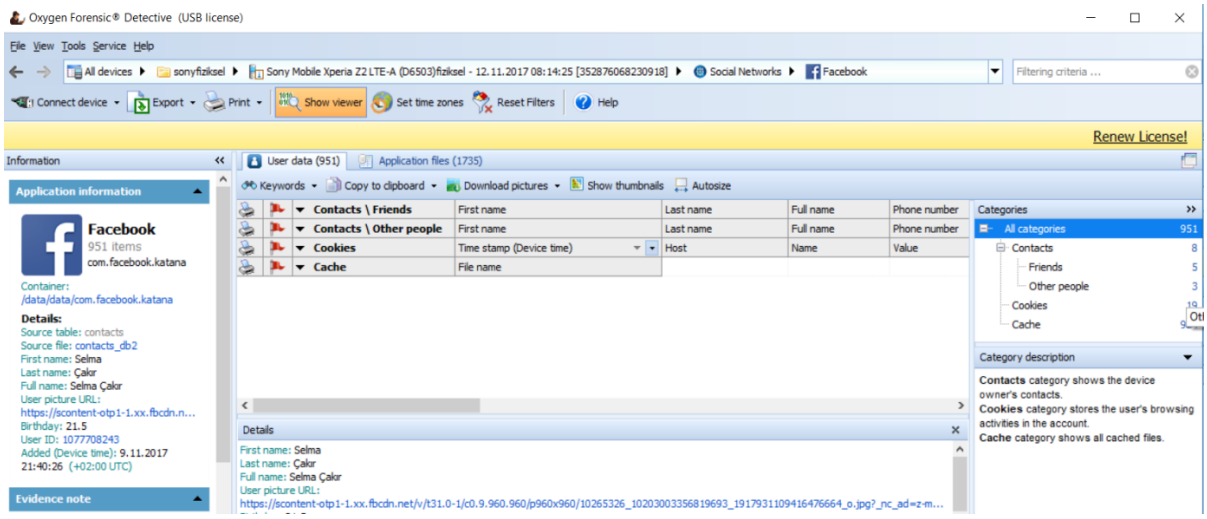
4.2 Adli Araçlar Yardımıyla Elde Etme

4.2.1 Facebook

Oxygen Forensic ile mantıksal imaj incelendiğinde facebook ile ilgili /sdcard/com.facebook.katana ve /sdcard/com.facebook.orca klasörleri mevcuttur. Fakat bu klasörler içerisinde kayda değer veriler bulunmamaktadır.

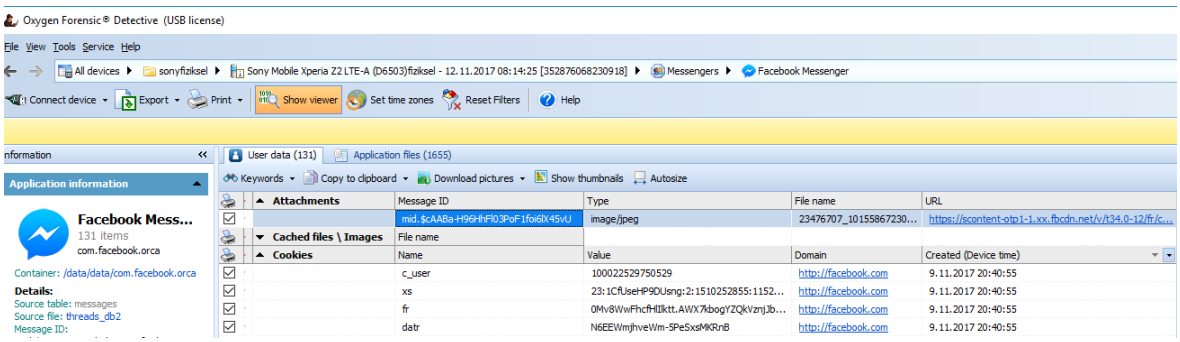
Fiziksel imaj incelendiğinde ise uygulamanın Oxygen Forensic tarafından elde edilen verileri Şekil 4.26'daki gibidir. Bu kısım analiz yapan kişiye önemli derecede kolaylık sağlamaktadır. Yazılım önemli verileri uygun veri tabanlarından ya da dosyalardan çekerek hızlı şekilde kullanıcısına sunmaktadır. "User Data" kısmında kişi bilgileri, çerezler ve önbelleğe alınan resim dosyaları bulunmaktadır. "Application Files" kısmında ise uygulama ile ilgili bütün dosyalar bulunmaktadır.

"User Data" kısmında "Contacs" altında kişiler isim, soyisim, tüm isim ve varsa telefon numarası, profil resmi URL'si, doğum günü, şehir, kullanıcı ID'si ve eklenme zamanı bilgileri ile sunulmaktadır. "cookies" başlığı altında ise çerezler alınma zamanı, alındığı host, ismi, değeri ve yolu şeklinde sunulmaktadır. "cache" başlığı altında ise önbelleğe alınan ".cnt" uzantılı resimler bulunur.



Şekil 4.26. Oxygen Forensic Facebook Çıktısı_1

Facebook Messenger uygulaması mesajlaşma verilerini tutar, Oxygen Forensic aracının bu uygulamadan çıkardığı verilere bakıldığında ise Şekil 4.27 gibidir. "Attachment" kısmında ek dosyaları mesaj ID'si bilgsi, tipi, dosya ismi, URL'si olacak şekilde görüntülenir. "cached files" kısmında önbelleğe yüklenen ".cnt" uzantılı resim dosyaları görüntülenir. "cookies" kısmında ise çerez ismi değeri, geldiği web sitesi ve oluşturulma zamanı şeklinde kullanıcıya sunulur. Bu kısımda beklenenin aksine kullanıcılar ola olan mesajlaşmalar görüntülenmemektedir. Oxygen Forensic de Facebook üzerinden olan mesajlaşma detaylarının görüntülenebilmesi için uygulama manuel olarak incelenmelidir.



Şekil 4.27. Oxygen Forensic Facebook Çıktısı_2

Paraben ile mantıksal imaj incelendiğinde kayda değer herhangi bir veriye ulaşılamamıştır. Fiziksel imaj incelendiğinde ise Şekil 4.28 yazılımın uygulama verilerinden kullanıcıya pratik olarak sunduğu uygulama ayar detayları, kişi listesi, gruplarla ve kişilerle yapılmış görüşmeler şeklindedir. Burada "Raw seetings" altında Facebook uygulama

ayarları bulunur. “Contacts” altında Facebook kişilerinin adı, soyadı, görüntülenen ismi ve kullanıcı kimlik numarası bulunmaktadır. Facebook Messenger başlığı altındaki “Current Info” kısmında kullanıcının ülke kodu telefon numarası gibi bilgiler bulunur. “Conversations” kısmında kişilerle ve gruplarla olan konuşmalar kişi ve grup kimlik numaraları ile listelenmiştir. Burada mesajı gönderen ismi ve kimlik numarası, mesaj içeriği, konuşmanın ikili formatta dökümü, ek dosya var mı yok mu bilgisi bulunur. “Groups Conversations List” kısmında bu zamana kadar açılmış grupların kimlik numaraları ve gruba dahil olan kişilerin bilgileri bulunmaktadır.

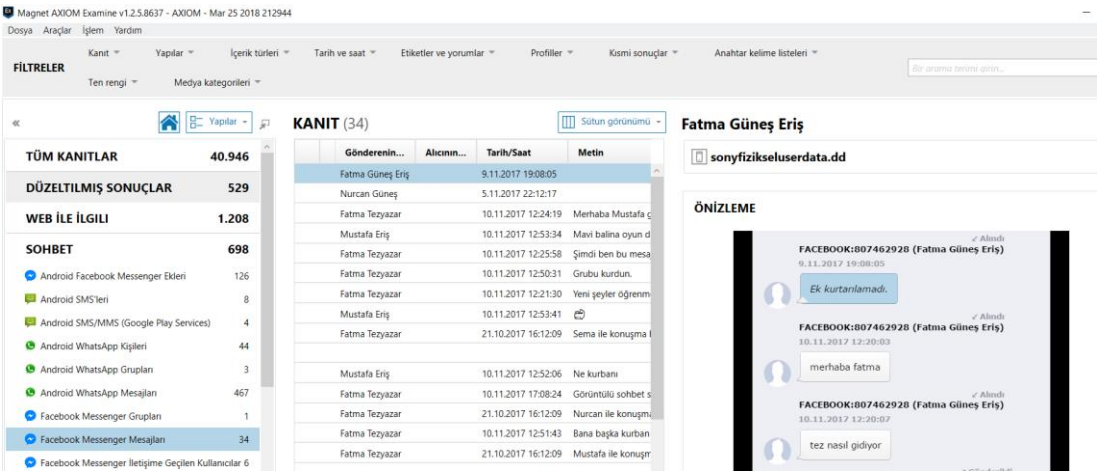
“File browser” kısmında uygulama dosyalarının hepsine erişilmektedir. Uygulamanın hangi verisinin hangi konumda olduğu bilgisi ile kullanıcı tüm detaylı verilere ulaşabilmektedir.

Şekil 4.28. Paraben E3:Ds Facebook Çıktısı

Ddtool ile alınan imaj Magnet Axiom aracı ile incelendiğinde çıkan sonuçlar

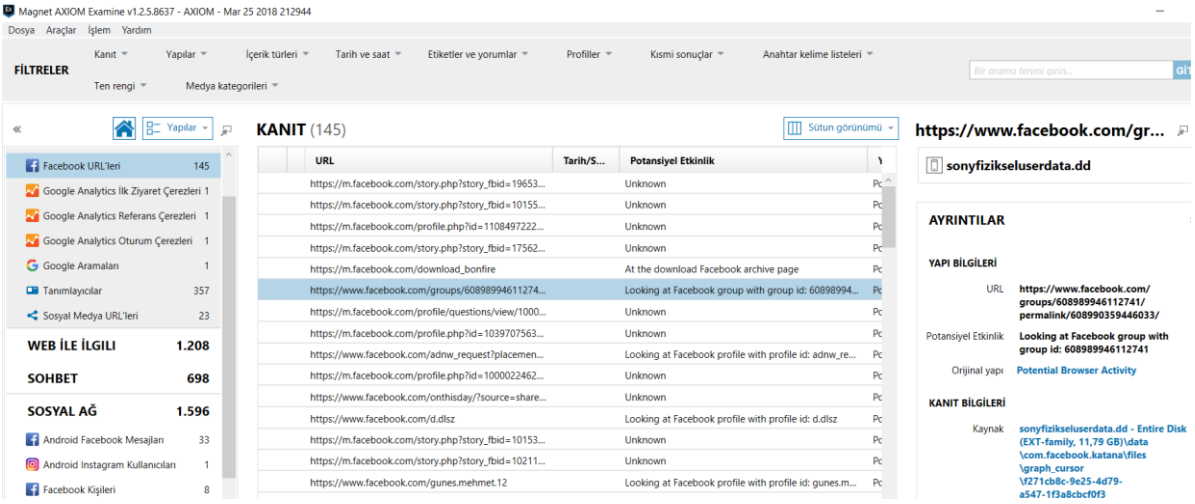
Şekil 4.29 ‘deki gibi kullanıcıya sunulmaktadır. Bu araç ile Facebook Messenger uygulamasında var olan gruplar, kişilerle ve gruplarla olan mesajlar, iletişime geçilen kişiler, aracın sohbet başlığı altında kullanıcıya sunulmaktadır. Araç, mesajları

Şekil 4.29'deki gibi liste halinde detaylı şekilde sunulmakla birlikte sağ taraftaki ön izleme kısmı ile mesajlaşmaları sohbet ekranı gibi görüntülemektedir. "Facebook Messenger Grupları" başlığı altında grup kimlik numarası, katılımcı ID'leri, son mesaj gönderme zamanı, toplam ileti sayısı bilgileri bulunur. "Facebook Messenger Mesajları" kısmında mesaj gönderen kişinin ismi, gönderme zamanı, mesaj içeriği, ek dosya varsa türü, mesaja atanan ID, iletinin geldiği kaynak, iletide konum bilgisi var ise enlem boylam bilgisi bulunur. "Facebook Messenger ile İletişime Geçilen Kullanıcılar" kısmında kullanıcı kimlik numarası, adı, soyadı, görünen ismi, kullanıcı adı, profil resmi URL'si, arkadaş olup olmadığı bilgisi, kişi ile iletişim sıklık oranı bulunur.



Şekil 4.29. Axiom Facebook Messenger Çıktısı

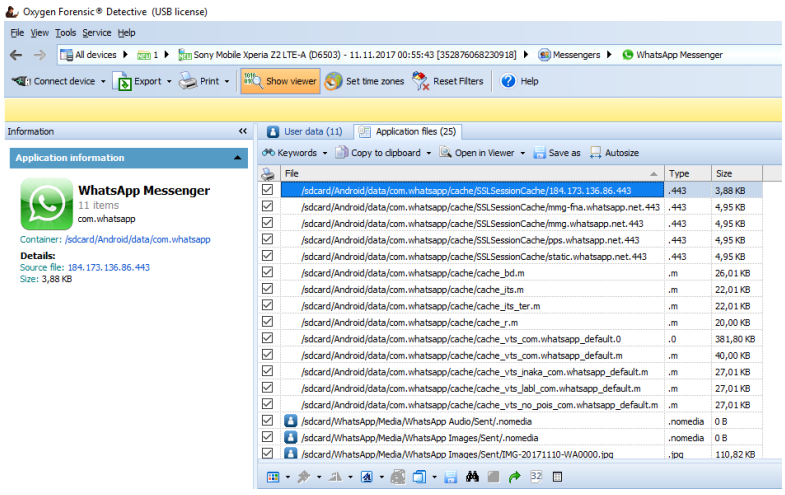
Sosyal ağ kısmında; Facebook kişileri altında kişiler ile ilgili detaylı bilgiler, Facebook mesajları altında ise yapılan mesajlaşmalar detayları ile birlikte bulunur Şekil 4.30. Düzeltilmiş sonuçlar kısmında ise Facebook URL'leri yapılan etkinliği tanımlayacak şekilde bulunmaktadır. "Facebook kişileri" altında ekli olan kişilerin profil kimliği, adı, soyadı, görünen ismi, profil resmi URL'si, telefon numaraları bulunur.



Şekil 4.30. Axiom Facebook Çıktısı

4.2.2 WhatsApp Messenger

Oxygen Forensic ile mantıksal imaj incelendiğinde WhatsApp bulgularının "/sdcard/WhatsApp" klasörü altında bulunduğu gözlenmiştir. Oxygen yazılımı ile uygulama segmesindeki WhatsApp'ı seçtiğimizde Şekil 4.31 görülmüştür. "Userdata" kısmında yalnızca gönderilmiş birkaç resim dosyası görüntülenirken "Application files" kısmında içerisinde veri bulunan ve uygulamanın erişime izin verdiği dosyalar görüntülenmektedir.



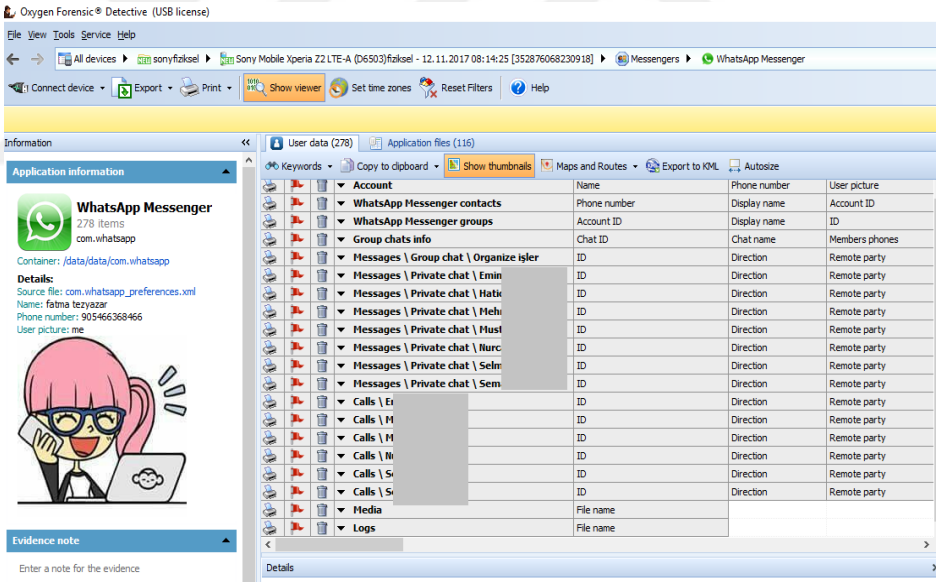
Şekil 4.31. Oxygen Forensic Mantıksal imaj WhatsApp çıktısı

"File browser" sekmesinden açtığımızda ise /sdcard/WhatsApp/ klasörü altında databases klasörü ve media klasörü bulunduğu görülmektedir Media klasörü altında WhatsApp uygulaması ile gönderilen veya alınan medyaların bulunduğu, uygulamanın da her zaman erişime izin verdiği veriler bulunmaktadır. Databases klasörü altında ise bir

kullanıcı ve kişileri arasındaki sohbet görüşmeleri hakkında ayrıntılı bilgi bulunduran msgstore veri tabanının şifrelenmiş hali olan msgstore.db.crypt12dosyası bulunmaktadır [43]. Bu dosya ancak telefonun root edilmesinden sonra ulaşabilecek olan bir anahtar dosyası ile açabilir. Telefon root edildikten sonra bu dosyanın şifresiz haline ve yapılan etkileşimlerle ilgili daha fazla veri tabanına ulaşılabilmektedir. Bu yüzden Whatsapp uygulaması ile ilgili detaylı analiz için fiziksel imajın incelenmesi çok önemlidir.

WhatsApp uygulaması için alınan fiziksel imajının Oxygen ile incelendiğinde aşağıdaki gibi görüntülenmiştir.

"User data" kısmında Şekil 4.32 hesap bilgisi, WhatsApp kişi listesi, grupları, grup bilgileri, kişilerle olan birebir yazışmalar, yapılan aramalar, medya ve log bilgileri bulunmaktadır. Bu kısım analiz yapan kişiye önemli derecede kolaylık sağlamaktadır. Yazılım önemli verileri uygun veri tabanlarından ya da dosyalardan çekerek hızlı şekilde kullanıcısına sunmaktadır.



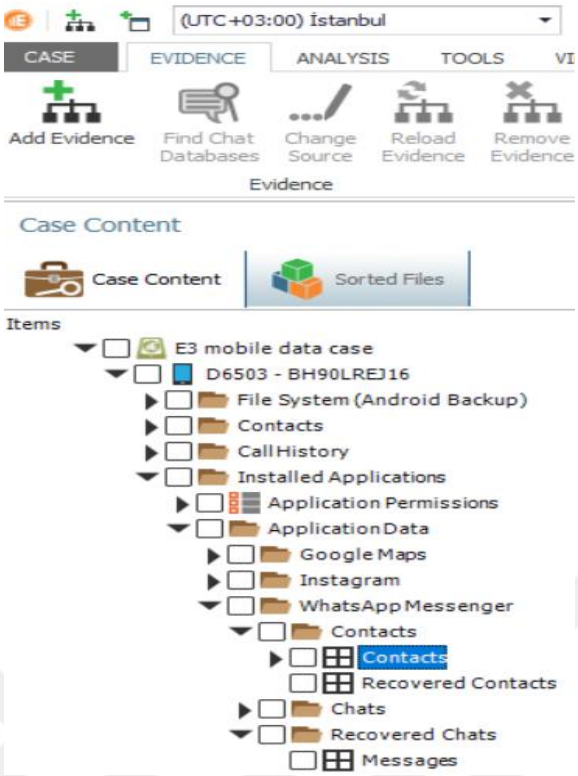
Şekil 4.32. Oxygen Forensic Fiziksel imaj WhatsApp çıktısı

Burada "Account" kısmında hesap sahibinin kişi bilgisi, telefon numarası, profil resmi görüntülenir. "WhatsApp Messenger Contacts" kısmında kişi listesi; ismi, hesap id'si (telefon numarası ile başlayan), telefon numarası, durum bilgisi, profil resimleri ile birlikte görüntülenmektedir. "WhatsApp Messenger groups" kısmında hesap id'si (grubu açan kişinin numarası ile başlayan), grup ismi ve gruba atanan id bilgisi görüntülenmektedir. "Group Chat info" kısımında grup id'si ismi, üyelerinin telefon numaraları ve üyelerin

isimleri görüntülenmektedir. “Messages\Group chat\ grup ismi” kısmında gruptaki mesajlar ona atanan id bilgisi, yönü, kimden geldiği kimlere iletildiği zaman pulu, mesaj içeriği, oluşturulma zamanı, sunucuya iletilme zamanı, kabul edilme zamanı, okunma zamanı bilgisini gönderilen bir medya ise onun boyutu ve dosya konumu bilgileri bulunur. “Messages\Private chat\ kişi” ismi kısmında o kişi olan mesajlar ona atanan id bilgisi, yönü, telefon numarası, kişi ismi, zaman pulu, mesaj içeriği, mesaj tipi, oluşturulma zamanı, sunucuya iletilme zamanı, kabul edilme zamanı, okunma zamanı bilgisi, gönderilen konum ise konum bilgisi, gönderilen bir medya ise onun boyutu ve dosya konumu bilgileri bulunur. “Call\kişi” ismi kısmında yapılan aramaların id’si yönü, arama yapılan telefon numarası, kişi ismi, zaman pulu, görüşmenin ne kadar sürdüğü bilgilerini barındırır. “Media” kısmında gönderilen dosyaların bilgileri bulunmaktadır. “Log” kısmında log dosyalarının isimleri bulunmaktadır.

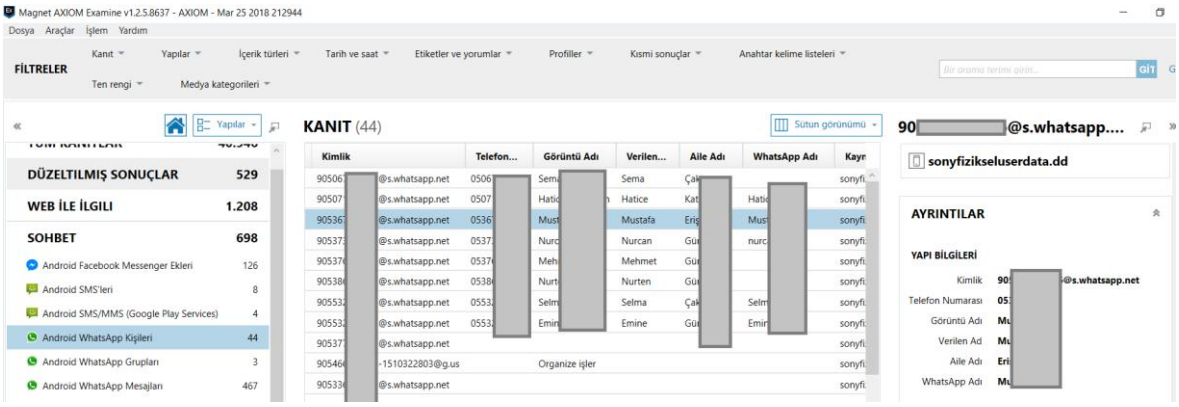
“Application files” kısmında uygulama ilgili tüm dosyaların görüntülenmektedir. File Browser segmesinden açtığımızda ise uygulama ile ilgili analiz yapmamızı sağlayacak dosyaların bulunduğu yerin /data/data/com.whatsapp olduğu görülür.

Paraben E3 ile mantıksal imaj incelendiğinde WhatsApp bulgularına ulaşılamamıştır. Paraben E3 ile root edilen cihazın tam mantıksal imajı incelendiğinde ise Şekil 4.33’deki gibi kişi listesi ve kurtarılmış kişi listesi, konuşmalar ve kurtarılmış konuşmalar görüntülenmektedir. “Contacs” kısmında kişi bilgileri; kişi ismi, soy ismi, WhatsApp’daki ismi, WhatsApp kimliği, durumu, durumu en son güncelleme zamanı, telefon numarası şeklinde bulunur. “Chats” kısmında ise konuşma yapılan kişilerin WhatsApp kimlik bilgilerinin listesi bulunmaktadır bunlar tıklandığında o kişi ile yapılan görüşmeler zamanı, kimlik bilgisi, mesaj içeriği, giden/gelen bilgisi, mesajın ne zaman gönderildiği/alındığı, sunucu tarafından alınma zamanı, kişi tarafından alınma zamanı, mesaj eki ile ilgili bilgilerini kullanıcıya sunmaktadır.



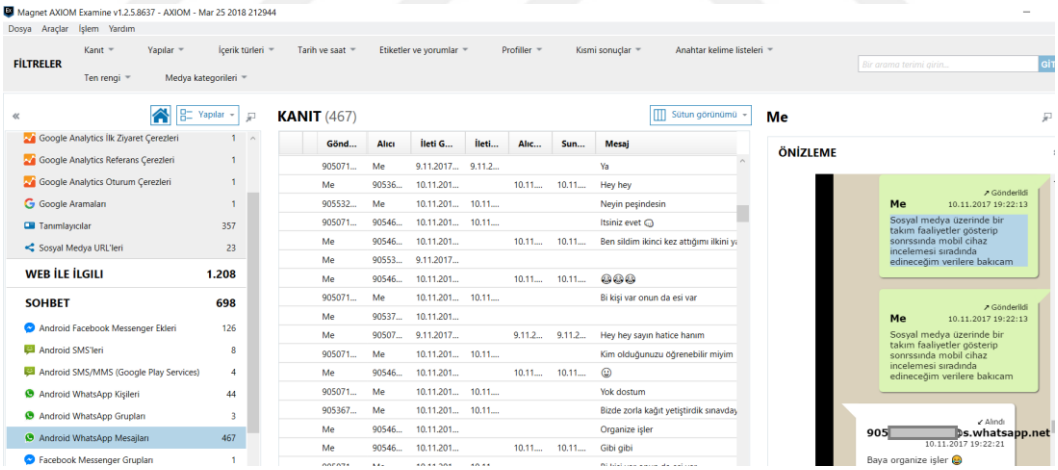
Şekil 4.33. Paraben E3:DS WhatsApp çıktısı

Ddtool ile alınan imaj Magnet Axiom aracı ile incelendiğinde WhatsApp ile ilgili çıkan sonuçlar Şekil 4.34'deki gibi kullanıcıya sunulmaktadır. Araç ile WhatsApp kişiler, gruplar ve mesajlar ayrı başlıklar altında incelenebilmektedir. WhatsApp kişileri başlığı altında kullanıcıların WhatsApp tarafından atanan kimlik bilgileri, telefon numaraları, görünen isim, verilen isim ve WhatsApp uygulaması için belirlenen isimler görüntülenir. Kişi üzerine tıklandığında ise sağ tarafta kişi ile ilgili tüm ayrıntılar görüntülenir. WhatsApp grupları başlığı altında ise grup kimliği, grup ismi, oluşturulduğu zaman ve grup üyeleri bilgileri sunulmaktadır.



Şekil 4.34. Axiom WhatsApp Messenger Çıktısı_1

WhatsApp mesajları başlığı incelendiğinde Şekil 4.35 ise araç kullanıcısına mesajlarla ilgili tüm detayları sunulmaktadır. Mesajın gönderici/alıcı bilgisi, gönderme/alma zamanı bilgisi, alıcının/sunucunun mesajı alma zaman bilgisi, mesaj içeriği, mesajın iletim durumu, ekte konum var ise onun enlem boylam bilgisi, ekte medya varsa türü ve URL'si bilgileri, bu veriyi elde ettiği delil ve veritabanı bilgileri bu kısımda bulunmaktadır. Mesaj üzeri tıklandığında o kişi ile yapılan yazışmalar sohbet formatında kullanıcıya sunulmaktadır.

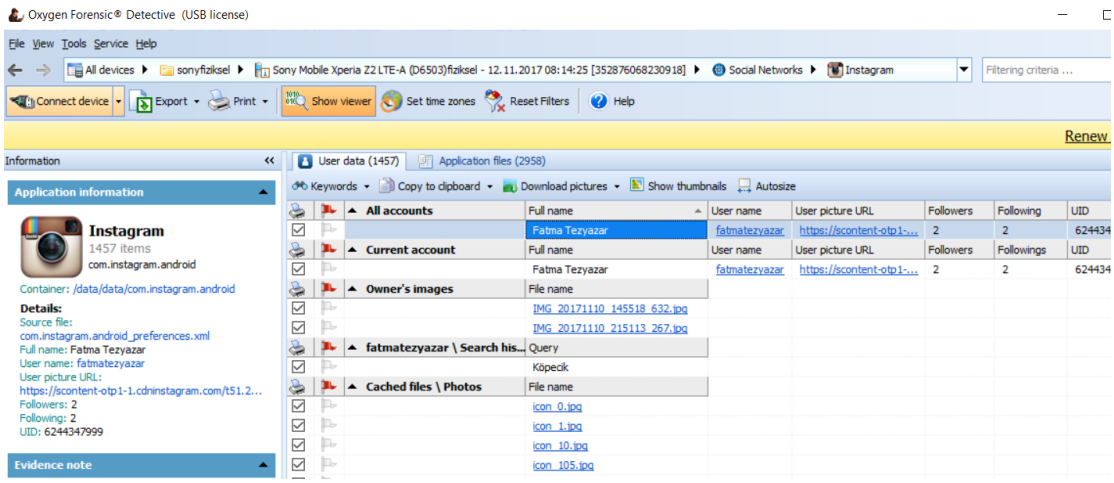


Şekil 4.35. Axiom WhatsApp Messenger Çıktısı_2

Yukarıdaki veriler axiomun sohbet başlığı altındaki WhatsApp bilgileridir. Bunlar haricinde kullanıcıya medya başlığı altında whatsapp profil resimlerinin bulunduğu bir alan sunulmaktadır. Burada profil resmi görüntüsü oluşturulduğu tarih, resmin boyutu gibi bilgiler de yer almaktadır.

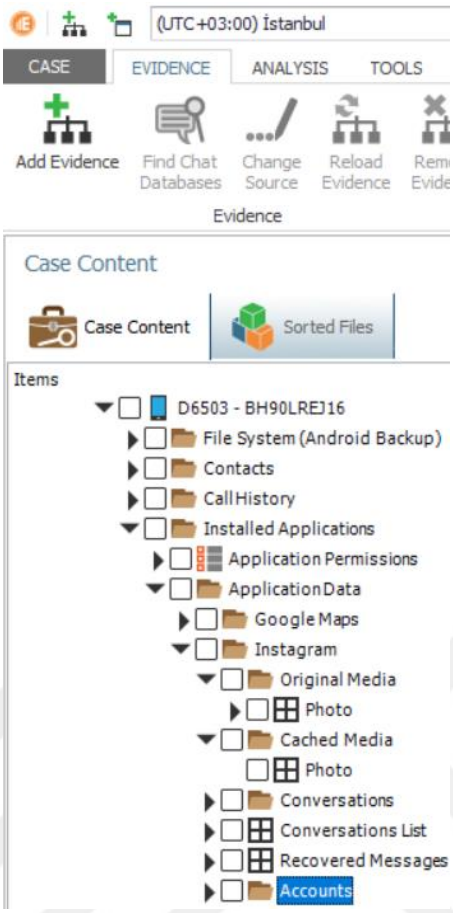
4.2.3 Instagram

Oxygen Forensic aracı ile mantıksal imaj incelendiğinde /sdcard/Android/data/com.instagram.android dosyası içersinde bulunan paylaşılmış resim verileri ile video önbellek dosyaları bulunmaktadır. Oxygen Forensic ile fiziksel imaj incelendiğinde Şekil 4.36 "User data" kısmında telefondaki tüm Instagram hesapları, şu an kullanılan Instagram hesabı, kullanıcının Instagram resimleri, kullanıcının arama geçmişi ve önbellekte duran Instagram' da görüntülenen bütün resimler bulunur. "All accounts" ve "Current account" başlığı altında kullanıcının tüm ismi kullanıcı ismi, profil resmi URL'si takipçi sayısı ve takip ettiği hesap sayısı, kullanıcı kimliği bulunmaktadır.



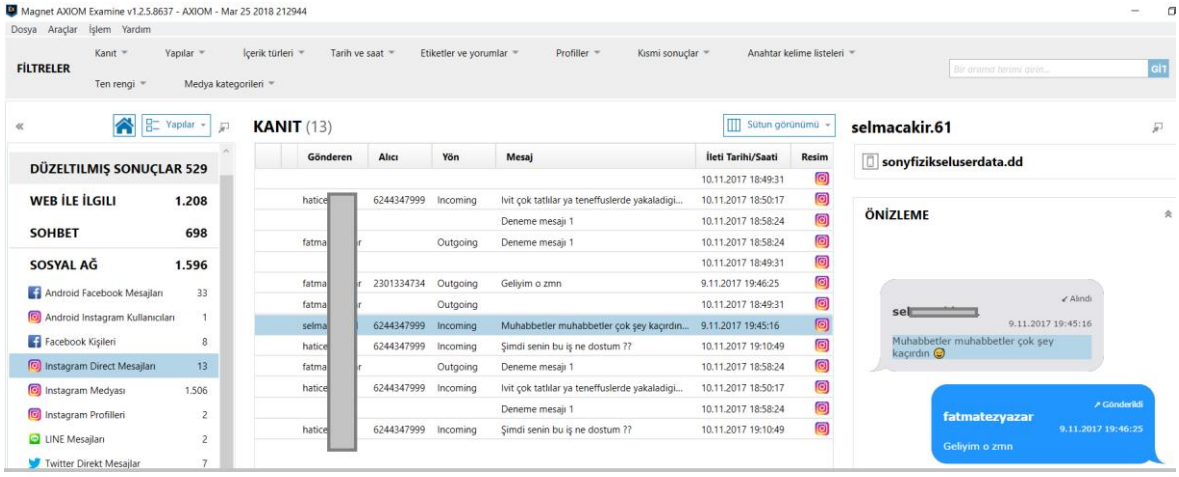
Şekil 4.36. Oxygen Forensic Instagram çıktısı

Paraben ile fiziksel imaj incelendiğinde ise aşağıdaki Şekil 4.37'de görüldüğü gibi resimlerin orijinal hali, Instagram'a düşen tüm resimler, yapılan görüşmeler, kurtarılan mesajlar, bu cihazda girilmiş hesaplar görüntülenmektedir. "Original Media" başlığı altında kullanıcının paylaştığı resimler bulunur, "Cache media" başlığında ise Instagram üzerinde görüntülenen ve önbelleğe atılan ".clean" uzantılı resimler görüntülenir. "conversations" başlığı altında "consevation list" başlığı bulunur. Burada görüşme gerçekleştirilen kişi ile en son ne zaman görüşüldüğü, kişinin Instagram' daki ismi, konuşmaya davet eden, konuşmayı alan ve konuşmaya atanan kimlik bilgileri gösterilmektedir. "Conversation" başlığı altında "recovered messages" kurtarılan mesajlar zamanı, konuşma kimliği, mesaj tipi, yazılı mesaj ise içeriği ve ham formattaki hali bulunmaktadır. Accounts başlığı altında da bu telefondan giriş yapılmış hesapların kullnıcı kimliği, ismi, hala giriş yapıp yapmadığı, profil resmi URL bilgileri bulunmaktadır.



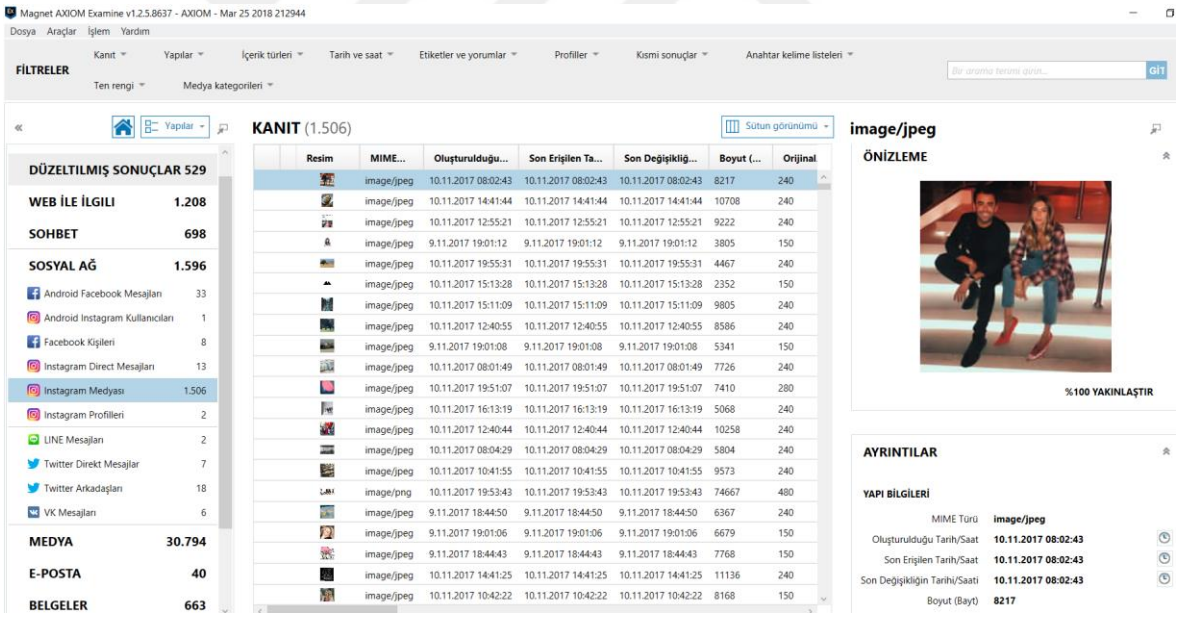
Şekil 4.37. Paraben E3:Ds Instagram çıktısı

Ddtool ile alınan imaj Magnet Axiom aracı ile incelendiğinde Instagram ile ilgili çıkan sonuçlar Şekil 4.38'deki gibi kullanıcıya sunulmaktadır. Instagram kullanıcı bilgileri, direkt mesajları, medyası ve profilleri ayrı başlıklar altında incelenebilmektedir. Instagram kullanıcı bilgilerinde kullanıcının kimliği, Instagram' daki ismi, tam ismi, profil resmi url'si, bulunmaktadır. Direk mesajlar incelendiğinde ise mesajın gönderici/alıcı bilgisi, yönü, içeriği, zamanı ve tipi kullanıcıya sunulur ayrıca sohbet formatında gösterimi de Şekil 4.38 mevcuttur.



Şekil 4.38. Axiom Instagram Çıktısı_1

Instagram medyası başlığı altında Şekil 4.39 kişinin Instagramda görüntülediği önbelleğe alınan resimlerin bilgileri bulunur. Resmin küçük bir görüntüsü, tipi(jpeg,png gibi), oluşturulduğu değiştirildiği zaman bilgileri, boyutu gibi bilgiler görüntülenmektedir.



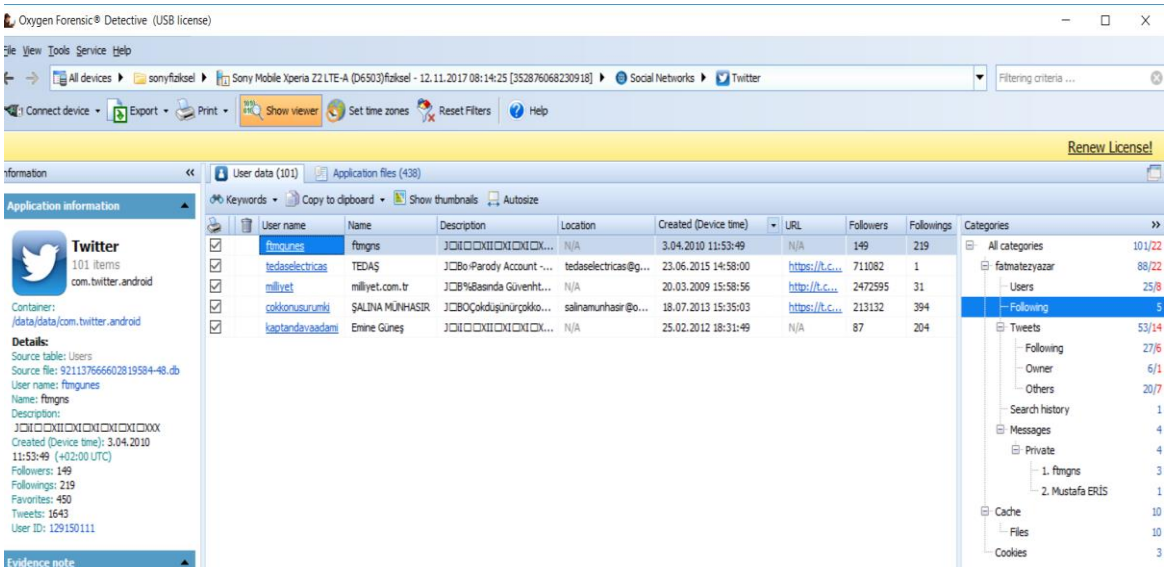
Şekil 4.39. Axiom Instagram Çıktısı_2

Instagram profilleri başlığı altında iletişimde bulunulan kişilerin adı, kimlik bilgileri, profill resmi url'leri, varsa biyografi bilgisi sunulur.

4.2.4 Twitter

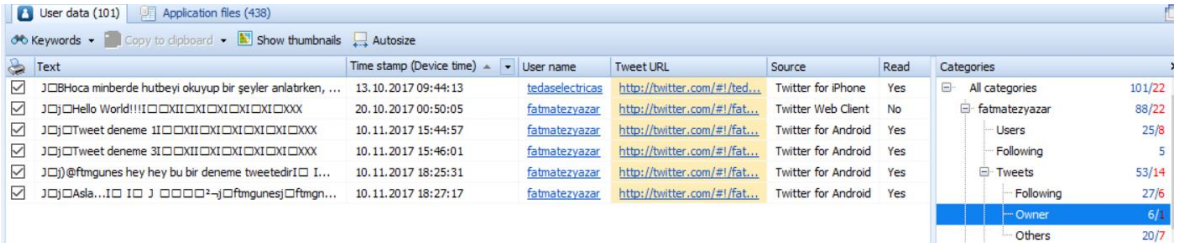
Oxygen Forensic ile alınan mantıksal imaj incelendiğinde yalnızca /sdcard/Android/data/com.twitter.android/cache/ klasörü içerisinde yer alan resimlere ve önbellek dosyalarına erişimin sağlandığı görülmektedir. Uygulamaya ilişkin daha iyi veriler elde edebilmek için fiziksel imaj incelenmelidir.

Oxygen Forensic ile alınan ".ofb" uzantılı fiziksel imaj incelendiğinde sağ kısımdaki kategorilerin bulunduğu görülmüştür. Bu kategorilerde aracın veri tabanlarından çekerek anlamlandırarak kullanıcıya sunduğu veriler Şekil 4.40'deki gibidir.



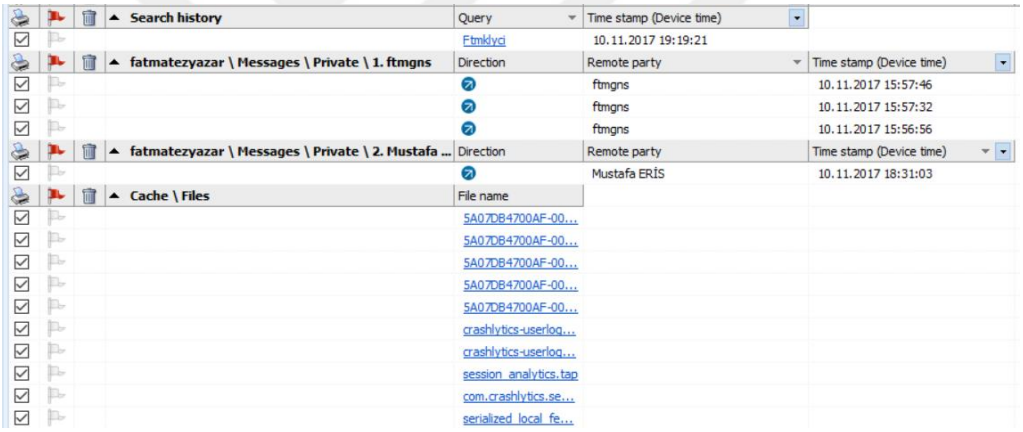
Şekil 4.40. Oxygen Forensic Twitter Çıktısı_1

Bu kısımdaki "fatmatezyazar" hesabı altında "users" başlığı bulunur. Burada kişinin ana sayfasında görüntülenmiş hesapların kullanıcı isimleri, takma isimleri, tanımları, konumları, ne zaman oluşturulduğu, varsa web url'si, toplam takipçi sayısı, toplam takip ettiği kişi sayısı, toplam beğeni sayısı, toplam attığı tweet sayısı ve kullanıcı kimliği bulunmaktadır. "Folowing" başlığı altında ise bu hesaplardan sadece takip edilenlerin bilgileri görüntülenir. "Tweets" başlığı altında atılan tweetler Şekil 4.41 takip ettiği kişiler tarafından atılan, kişinin kendiği attığı ve sayfasına düşmüş diğer tweetler olarak üç başlık altında; tweet içeriği, tweeti atma zamanı, kullanıcı adı, tweet url'si, tweet kaynağı(hangi uygulamadan atıldığı), twettin okunup okunmadığı bilgisi bulunmaktadır.



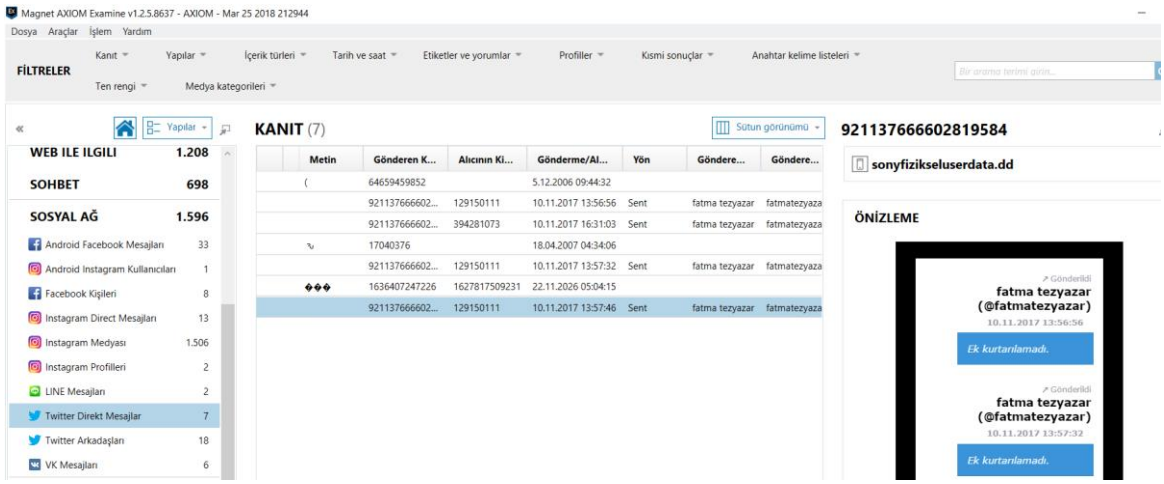
Şekil 4.41. Oxygen Forensic Twitter Çıktısı_2

"Search history" başlığı altında yapılan arama bilgileri arama kelimesi ve arama zamanı şeklinde verilmektedir Şekil 4.42 "Messages" başlığı altında kullanıcının direk mesaj özelliği ile kişilerle birebir olan görüşmelerin bilgileri bulunur Şekil 4.42. Bunlar mesajın yönü kim ile gerçekleştirildiği ve zaman bilgisidir. "Cache" başlığında önbelleğe alınan dosya bilgileri bulunur Şekil 4.42. "Cookies" başlığı altında ise çerez olarak alınan değerler yer almaktadır.



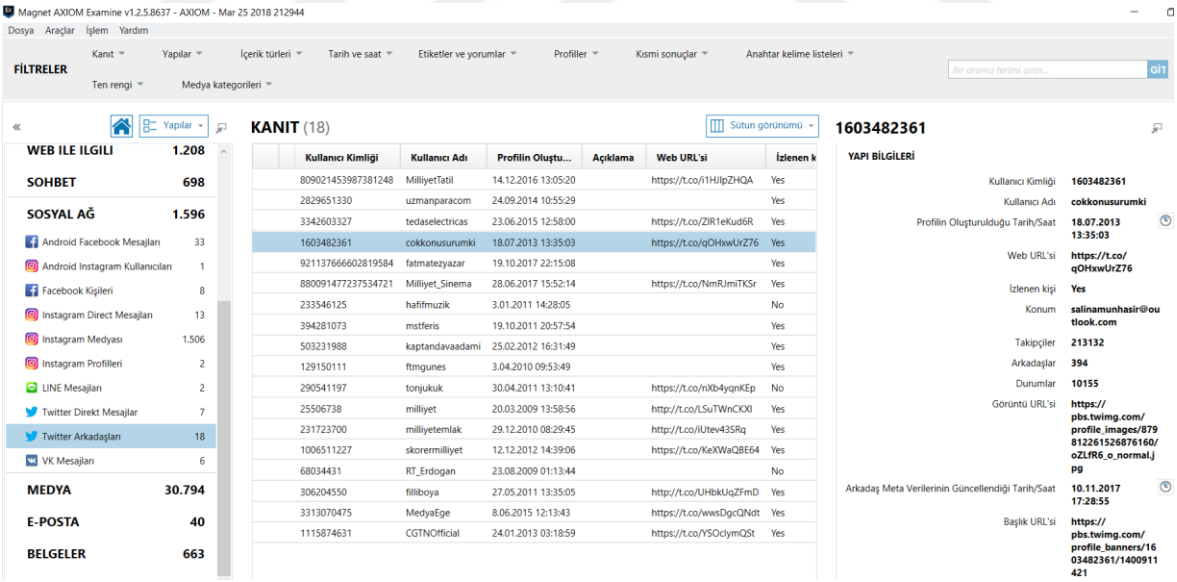
Şekil 4.42. Oxygen Forensic Twitter Çıktısı_3

Ddtool ile alınan imaj Magnet Axiom aracı ile incelendiğinde Twitter ile ilgili çıkan sonuçlar Şekil 4.43'deki gibi kullanıcıya sunulmaktadır. Burada Twitter üzerinden yapılan direk mesajlar ve Twitter arkadaşları, iki başlık altında verilmiştir. Direk mesajlar başlığı incelendiğinde aracın direk mesajların içeriğini görüntüleyemediği görülmektedir. Bunun haricinde mesajı gönderen alan kimliği, mesajın yönü, ismi verilmektedir.



Şekil 4.43. Axiom Twitter Çıktısı_1

Twitter arkadaşları başlığında ise kullanıcının ana sayfasına düşen tweet yazarlarının kullanıcı bilgileri görüntülenmektedir Şekil 4.44. Kullanıcının kimliği, adı, hesabı oluşturma tarihi, var ise açıklaması ve web urlsi, takip edlip edilmediği, konum bilgisi, takipçi ve arkadaş sayıları toplam tweet sayıları gibi bilgileri sunmaktadır. Bu başlıklar atılan veya görüntülenen tweetleri göstermemektedir.



Şekil 4.44. Axiom Twitter Çıktısı_2

Twitter uygulaması verilerini ayıklayarak kullanıcıya sunan Oxygen Forensic ve Axiom araçları arasında Oxygen Forensic ile daha çok veriye ulaşıldığı görülmüştür. Axiom ile tweet içerikleri, arama bilgileri, önbellek dosyaları ve çerez bilgileri gösterilmemektedir. Bu

iki araç Twiter uygulama verilerini ayıklayabilirken Paraben aracı kullanıcıya bu kolaylığı sağlayamamaktadır.

4.2.5 BiP Messenger

BiP uygulaması genel olarak Türk kullanıcısına hitap ettiği için mobil adli bilişim araçları tarafından tanınıp ayıklanamamaktadır. BiP gibi belli bir kesim tarafından kullanılan uygulamaların analizi manuel olarak gerçekleştirilir.

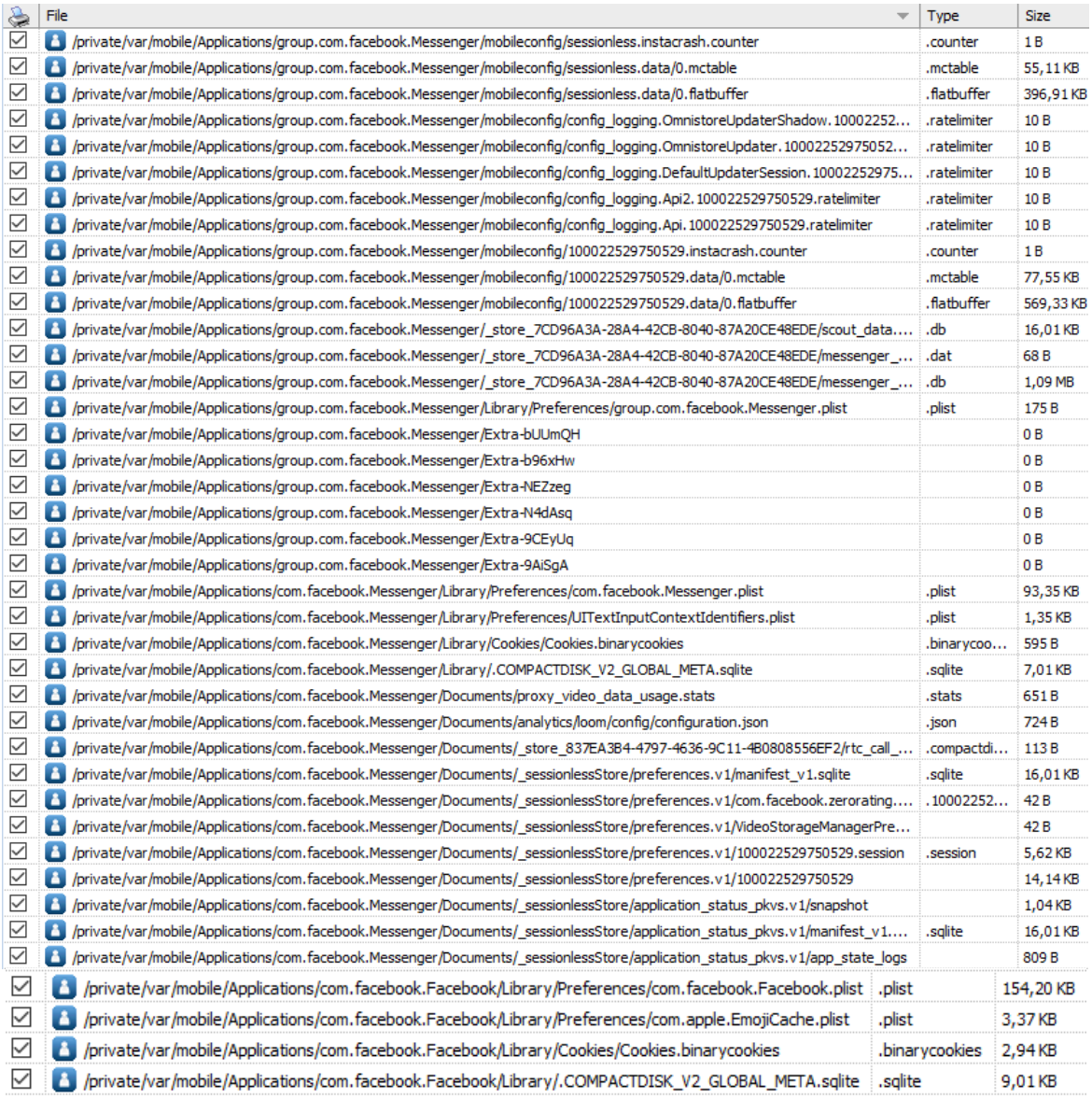
5. iOS İŞLETİM SİSTEMİNDE SOSYAL MEDYA UYGULAMALARININ ADLİ BİLİŞİM ANALİZİ

5.1 Manuel Elde Etme

Manuel elde etme, kullanılan iPhone 6s cihazının dosya sistemindeki uygulama dosyalarını bulup uygun editörler yardımı ile açıp inceleyerek gerçekleştirilmiştir. Bu edinimler, cihaza yüklü olan işletim sisteminin 11.3.1 iOS olması ve henüz bu cihaz üzerinde jailbreak işleminin mümkün olmaması nedeni ile mantıksal imajlardan elde edilen dosyalar üzerinden gerçekleştirilmiştir. Manuel elde etme sırasında Oxygen Forensic aracı ile dışarı aktarılan uygulama dosyaları incelenirken; *DB Browser for SQLite* yazılımı SQLite veri tabanı dosyalarını görüntülemek için, *plistEditor pro* yazılımı plist dosyalarını görüntülemek için, *HXD Hex Editor* yazılımı içeriği hex formatında görüntülenmesi gereken dosyalar için kullanılmıştır.

5.1.1 Facebook

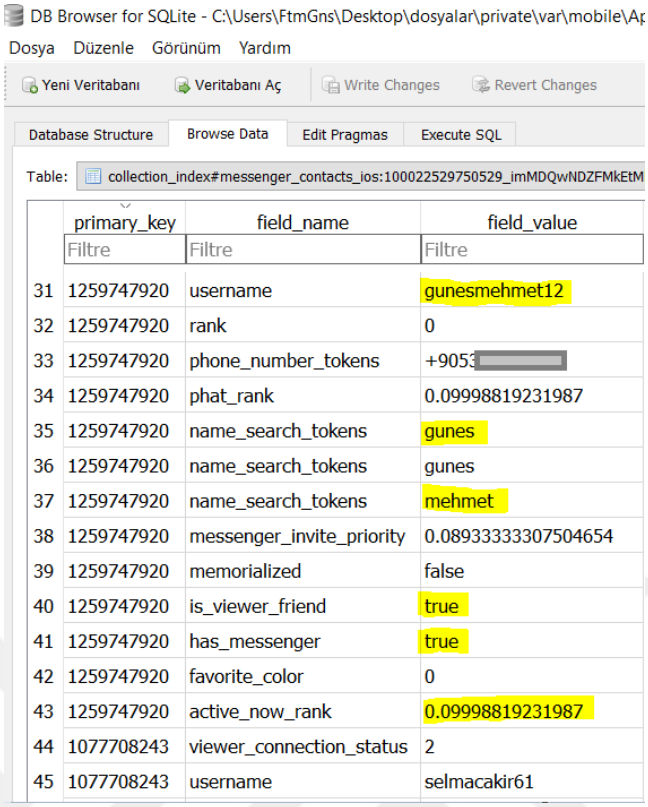
Dosya sistemi incelendiğinde önemli Facebook kalıntılarının "/private/var/mobile/Applications/com.facebook.Messenger" , "/private/var/mobile/Applications/group.com.facebook.Messenger" ve /private/var/mobile/Applications/com.facebook.Facebook klasörleri altında bulunduğu gözlenmiştir. Uygulamalara ilişkin verilerin bulunduğu dosyalar Şekil 5.1 'de verilmiştir. Bu veriler Oxygen Forensic aracından alınmıştır.



File	Type	Size
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/sessionless.instacrash.counter	.counter	1 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/sessionless.data/0.mctable	.mctable	55,11 KB
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/sessionless.data/0.flatbuffer	.flatbuffer	396,91 KB
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/config_logging.OmnistoreUpdaterShadow.10002252...	.ratelimiter	10 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/config_logging.OmnistoreUpdater.10002252975052...	.ratelimiter	10 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/config_logging.DefaultUpdaterSession.10002252975...	.ratelimiter	10 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/config_logging.Api2.100022529750529.ratelimiter	.ratelimiter	10 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/config_logging.Api.100022529750529.ratelimiter	.ratelimiter	10 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/100022529750529.instacrash.counter	.counter	1 B
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/100022529750529.data/0.mctable	.mctable	77,55 KB
/private/var/mobile/Applications/group.com.facebook.Messenger/mobileconfig/100022529750529.data/0.flatbuffer	.flatbuffer	569,33 KB
/private/var/mobile/Applications/group.com.facebook.Messenger/_store_7CD96A3A-28A4-42CB-8040-87A20CE48EDE/scout_data....	.db	16,01 KB
/private/var/mobile/Applications/group.com.facebook.Messenger/_store_7CD96A3A-28A4-42CB-8040-87A20CE48EDE/messenger_...	.dat	68 B
/private/var/mobile/Applications/group.com.facebook.Messenger/_store_7CD96A3A-28A4-42CB-8040-87A20CE48EDE/messenger_...	.db	1,09 MB
/private/var/mobile/Applications/group.com.facebook.Messenger/Library/Preferences/group.com.facebook.Messenger.plist	.plist	175 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-bUUmQH		0 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-b96xHw		0 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-NEZzeg		0 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-N4dAsq		0 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-9CEyUq		0 B
/private/var/mobile/Applications/group.com.facebook.Messenger/Extra-9AiSgA		0 B
/private/var/mobile/Applications/com.facebook.Messenger/Library/Preferences/com.facebook.Messenger.plist	.plist	93,35 KB
/private/var/mobile/Applications/com.facebook.Messenger/Library/Preferences/UITextInputContextIdentifiers.plist	.plist	1,35 KB
/private/var/mobile/Applications/com.facebook.Messenger/Library/Cookies/Cookies.binarycookies	.binarycoo...	595 B
/private/var/mobile/Applications/com.facebook.Messenger/Library/.COMPACTDISK_V2_GLOBAL_META.sqlite	.sqlite	7,01 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/proxy_video_data_usage.stats	.stats	651 B
/private/var/mobile/Applications/com.facebook.Messenger/Documents/analytics/loom/config/configuration.json	.json	724 B
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_store_837EA3B4-4797-4636-9C11-4B0808556EF2/rtc_call_...	.compactdi...	113 B
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/preferences.v1/manifest_v1.sqlite	.sqlite	16,01 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/preferences.v1/com.facebook.zerorating....	.10002252...	42 B
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/preferences.v1/VideoStorageManagerPre...		42 B
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/preferences.v1/100022529750529.session	.session	5,62 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/preferences.v1/100022529750529		14,14 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/application_status_pkvs.v1/snapshot		1,04 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/application_status_pkvs.v1/manifest_v1....	.sqlite	16,01 KB
/private/var/mobile/Applications/com.facebook.Messenger/Documents/_sessionlessStore/application_status_pkvs.v1/app_state_logs		809 B
/private/var/mobile/Applications/com.facebook.Facebook/Library/Preferences/com.facebook.Facebook.plist	.plist	154,20 KB
/private/var/mobile/Applications/com.facebook.Facebook/Library/Preferences/com.apple.EmojiCache.plist	.plist	3,37 KB
/private/var/mobile/Applications/com.facebook.Facebook/Library/Cookies/Cookies.binarycookies	.binarycookies	2,94 KB
/private/var/mobile/Applications/com.facebook.Facebook/Library/.COMPACTDISK_V2_GLOBAL_META.sqlite	.sqlite	9,01 KB

Şekil 5.1. iOS'da Facebook ve Facebook Messenger uygulama verilerinin saklandığı dosyalar

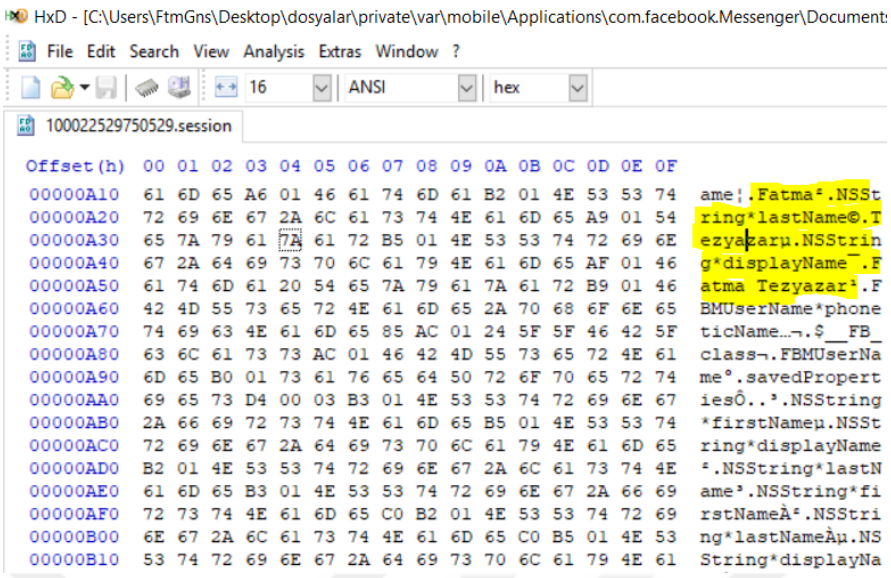
Bu klasörlerin altında bulunan *fbomnistore.db, 100022529750529.session, Cookies.binarycookies* dosyalarının uygulama hakkında önemli veriler içerdiği tespit edilmiştir. *fbomnistore.db* veritabanının *collection_index#messenger_contacts_ios:* tablosu incelendiğimde kişinin Facebook arkadaşları ile ilgili bilgiler indeks şeklinde tutulmuştur. Kişinin Facebook tarafından kişilere atanan benzersiz kimlikler bu tabloda *primary_key* sütunu olarak verilmiştir. Kişinin Facebook arkadaşlarına ait kullanıcı adı, isimler, telefon numarası, Messenger uygulamasına sahip olup olmadığı, aktiflik oranı gibi bilgiler Şekil 5.2'deki gibi bu tabloda tutulmaktadır.



Şekil 5.2. Facebook fbomnistore.db veritabanı

Cookies.binarycookies dosyası uygulamanın tuttuğu çerez bilgilerinin detaylarını içermektedir. Buradaki veriler sayesinde uygulama üzerinden ziyaret edilen sitelerin bilgilerine ulaşılabilmektedir.

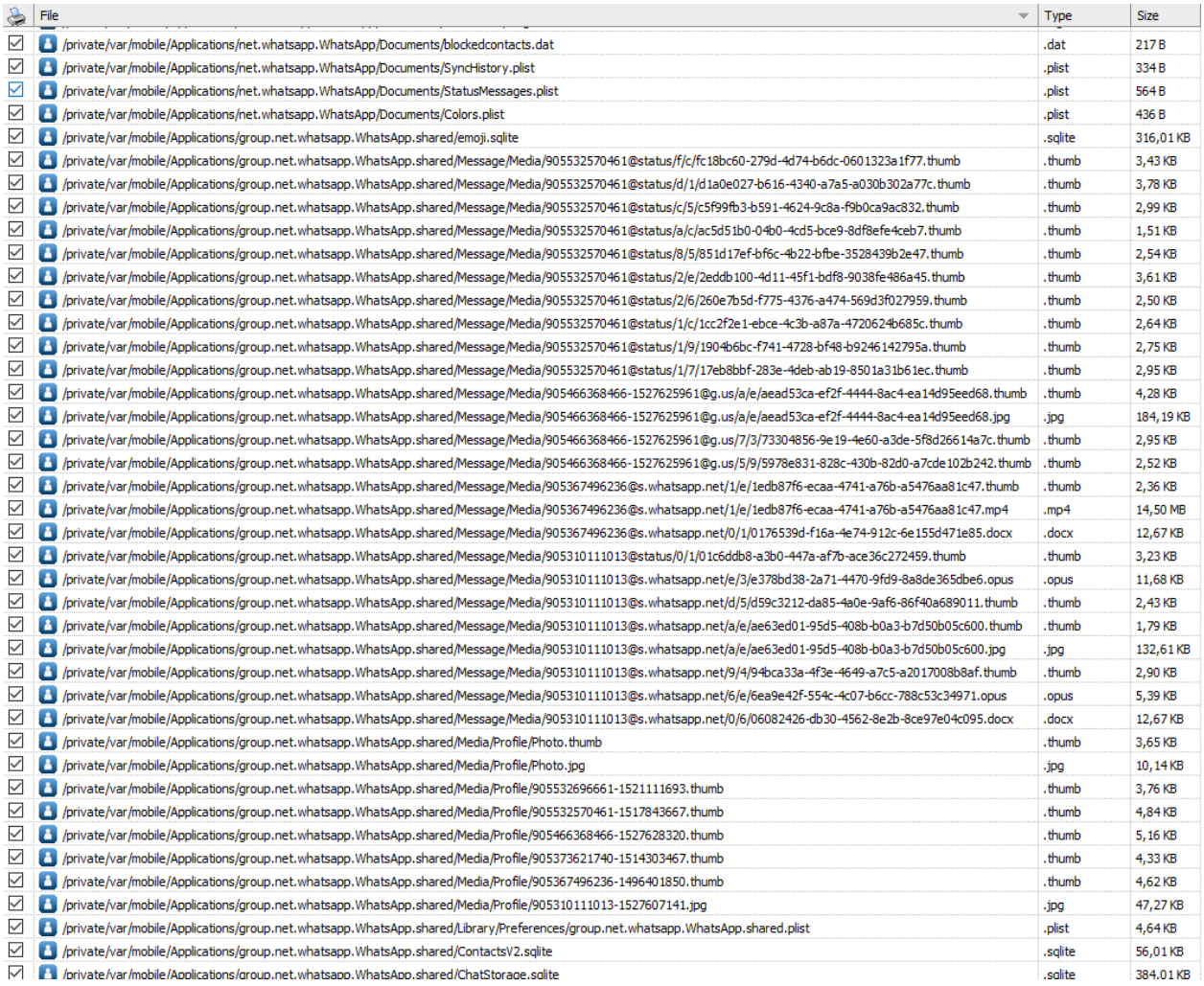
com.facebook.facebook.plist dosyası uygulamadaki yapılandırılmış hesabın e-posta adresi ve Facebook kimliği bu dosyadan çıkarılabilmektedir. *100022529750529.session* dosyası Şekil 5.3'deki gibi kullanıcı hesabı ile ilgili; adı, soyadı ve kullanıcı adı gibi bilgileri barındırmaktadır.



Şekil 5.3. Facebook 100022529750529.session dosyası

5.1.2 WhatsApp Messenger

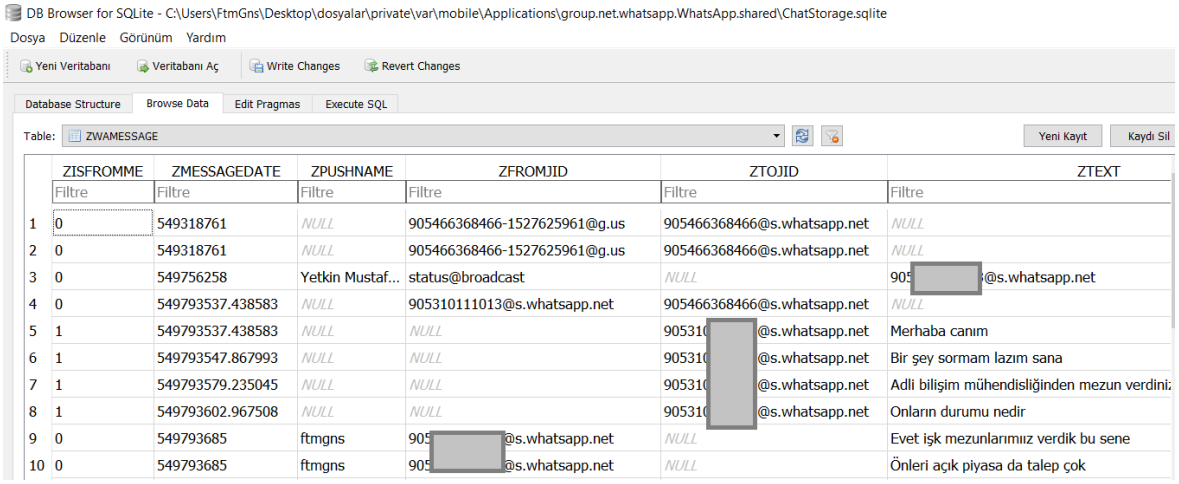
Dosya sistemi incelendiğinde WhatsApp kalıntılarının "/private/var/mobile/Applications/net.whatsapp.WhatsApp" ve "/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared" klasörleri altında bulunduğu gözlenmiştir. Uygulamaya ilişkin verilerin bulunduğu dosyalar Şekil 5.4 'de verilmiştir. Bu veriler Oxygen Forensic aracından alınmıştır.



File	Type	Size
/private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/blockedcontacts.dat	.dat	217 B
/private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/SyncHistory.plist	.plist	334 B
/private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/StatusMessages.plist	.plist	564 B
/private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/Colors.plist	.plist	436 B
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/emoji.sqlite	.sqlite	316,01 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/f/c/fc18bc60-279d-4d74-b6dc-0601323a1f77.thumb	.thumb	3,43 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/d/1/d1a0e027-b616-4340-a7a5-a030b302a77c.thumb	.thumb	3,78 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/c/5/c5f99fb3-b591-4624-9c8a-f9b0ca9ac832.thumb	.thumb	2,99 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/a/c/ac5d51b0-04b0-4cd5-bce9-8df8efe4ceb7.thumb	.thumb	1,51 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/8/5/851d17ef-bf6c-4b22-bfbe-3528439b2e47.thumb	.thumb	2,54 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/2/e/2eddb100-4d11-45f1-bdf8-9038fe486a45.thumb	.thumb	3,61 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/2/6/260e7b5d-f775-4376-a474-569d3f027959.thumb	.thumb	2,50 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/1/c/1cc2f2e1-ebce-4c3b-a87a-4720624b685c.thumb	.thumb	2,64 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/1/9/1904b6bc-f741-4728-bf48-b9246142795a.thumb	.thumb	2,75 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905532570461@status/1/7/17eb8bbf-283e-4deb-ab19-8501a31b61ec.thumb	.thumb	2,95 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905466368466-1527625961@g.us/a/e/aead53ca-ef2f-4444-8ac4-ea14d95eed68.thumb	.thumb	4,28 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905466368466-1527625961@g.us/a/e/aead53ca-ef2f-4444-8ac4-ea14d95eed68.jpg	.jpg	184,19 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905466368466-1527625961@g.us/7/3/73304856-9e19-4e60-a3de-5f8d26614a7c.thumb	.thumb	2,95 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905466368466-1527625961@g.us/5/9/5978e831-828c-430b-82d0-a7cde102b242.thumb	.thumb	2,52 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905367496236@s.whatsapp.net/1/e/1edb87f6-ecaa-4741-a76b-a5476aa81c47.thumb	.thumb	2,36 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905367496236@s.whatsapp.net/1/e/1edb87f6-ecaa-4741-a76b-a5476aa81c47.mp4	.mp4	14,50 MB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905367496236@s.whatsapp.net/0/1/0176539d-f16a-4e74-912c-6e155d471e85.docx	.docx	12,67 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@status/0/1/01c6ddb8-a3b0-447a-af7b-ace36c272459.thumb	.thumb	3,23 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/e/3/e378bd38-2a71-4470-9fd9-8a8de365dbe6.opus	.opus	11,68 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/d/5/d59c3212-da85-4a0e-9af6-86f40a689011.thumb	.thumb	2,43 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/a/e/ae63ed01-95d5-408b-b0a3-b7d50b05c600.thumb	.thumb	1,79 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/a/e/ae63ed01-95d5-408b-b0a3-b7d50b05c600.jpg	.jpg	132,61 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/9/4/94bca33a-4f3e-4649-a7c5-a2017008b8af.thumb	.thumb	2,90 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/6/e/6ea9e42f-554c-4c07-b6cc-788c53c34971.opus	.opus	5,39 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media/905310111013@s.whatsapp.net/0/6/06082426-db30-4562-8e2b-8ce97e04c095.docx	.docx	12,67 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/Photo.thumb	.thumb	3,65 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/Photo.jpg	.jpg	10,14 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905532696661-1521111693.thumb	.thumb	3,76 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905532570461-1517843667.thumb	.thumb	4,84 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905466368466-1527628320.thumb	.thumb	5,16 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905373621740-1514303467.thumb	.thumb	4,33 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905367496236-1496401850.thumb	.thumb	4,62 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Media/Profile/905310111013-1527607141.jpg	.jpg	47,27 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist	.plist	4,64 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ContactsV2.sqlite	.sqlite	56,01 KB
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite	.sqlite	384,01 KB

Şekil 5.4. iOS'da WhatsApp Messenger uygulama verilerinin saklandığı dosyalar

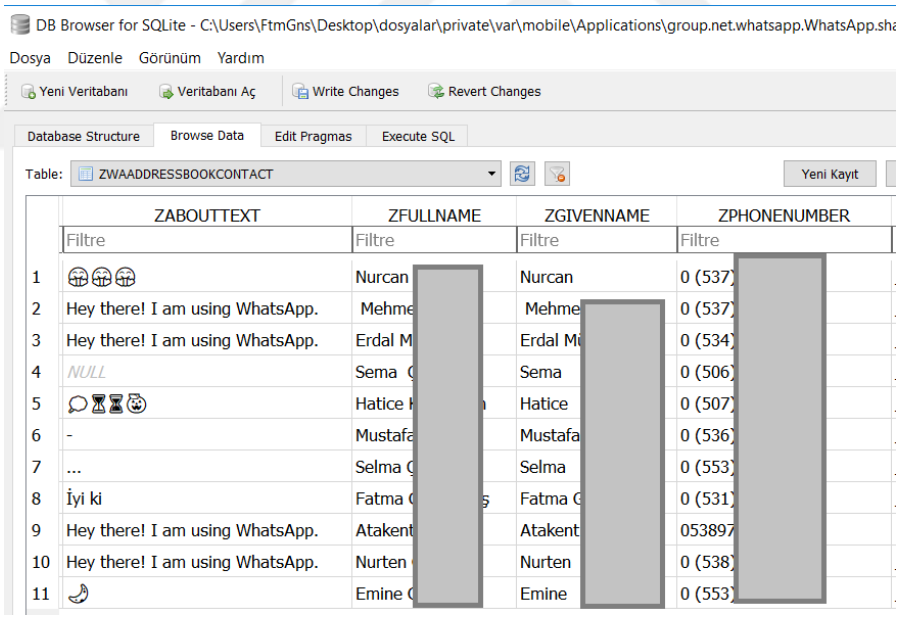
Veri tabanı dosyalarına bakıldığında ChatStorage, ContactsV2, ChatSearchV3 dosyaları önemli bilgileri barındırmaktadır. ChatStorage veri tabanı Zwmessage tablosu Şekil 5.5'de gösterildiği gibi; mesaj yönü, mesaj zaman bilgisi, gönderen ismi, WhatsApp tarafından atanan ID'ler, mesaj içeriği bilgileri barındırmaktadır. Bu veri tabanındaki diğer tablolardan grup bilgilerine, kullanıcı profil resimlerine, dosya ekleri ile ilgili verilere de erişilebilmektedir. *JID* WhatsApp tarafından kullanıcı, grup ve kişi durumlarına atılan benzersiz kimliği ifade etmektedir. Kişiler için "telefon numarası @ s.whatsapp.net", gruplar için "grubu kuran kişinin telefon numarası- ne zaman kurduğu damga pulu @g.us" , durum paylaşımı için "kişinin telefon numarası @status" şeklinde belirlenir.



	ZISFROMME	ZMESSAGEDATE	ZPUSHNAME	ZFROMJID	ZTOJID	ZTEXT
	Filtre	Filtre	Filtre	Filtre	Filtre	Filtre
1	0	549318761	NULL	905466368466-1527625961@g.us	905466368466@s.whatsapp.net	NULL
2	0	549318761	NULL	905466368466-1527625961@g.us	905466368466@s.whatsapp.net	NULL
3	0	549756258	Yetkin Mustaf...	status@broadcast	NULL	905 [redacted] @s.whatsapp.net
4	0	549793537.438583	NULL	905310111013@s.whatsapp.net	905466368466@s.whatsapp.net	NULL
5	1	549793537.438583	NULL	NULL	90531 [redacted] @s.whatsapp.net	Merhaba canım
6	1	549793547.867993	NULL	NULL	90531 [redacted] @s.whatsapp.net	Bir şey sormam lazım sana
7	1	549793579.235045	NULL	NULL	90531 [redacted] @s.whatsapp.net	Adli bilişim mühendisliğinden mezun verdini
8	1	549793602.967508	NULL	NULL	90531 [redacted] @s.whatsapp.net	Onların durumu nedir
9	0	549793685	ftmgns	905 [redacted] @s.whatsapp.net	NULL	Evet ışk mezunlarımız verdik bu sene
10	0	549793685	ftmgns	905 [redacted] @s.whatsapp.net	NULL	Önleri açık piyasa da talep çok

Şekil 5.5. WhatsApp ChatStorage veritabanı Zwmessage tablosu

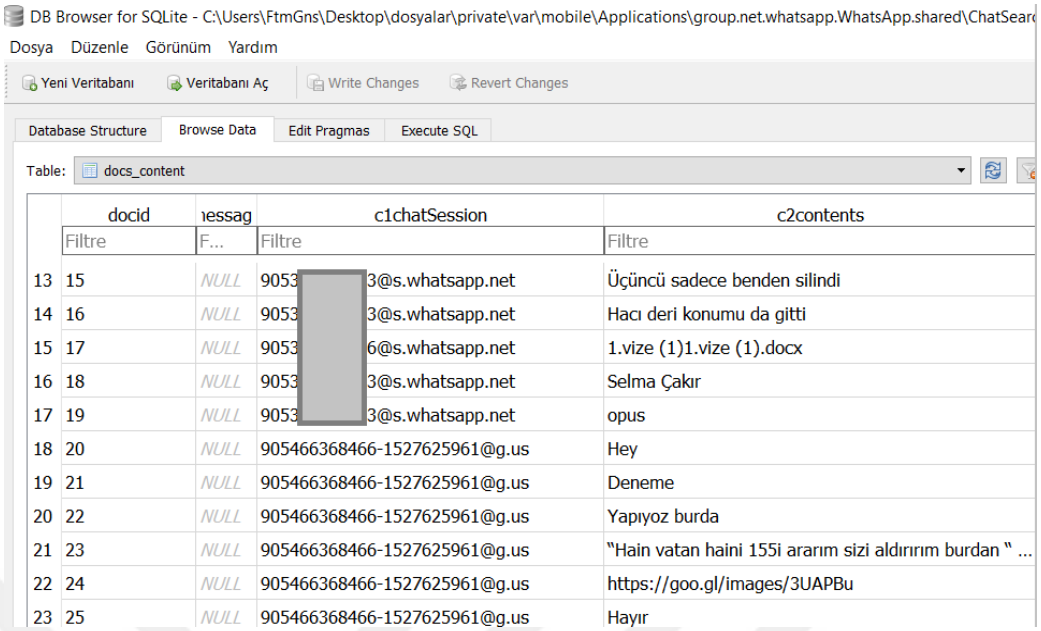
ContactsV2 veritabanı incelendiğinde ise Şekil 5.6'daki gibi WhatsApp kişi listesindeki kişilerin durumlarını, isimlerini, takma isimlerini, telefon numaralarını saklamakta olduğu görülmüştür.



	ZABOUTTEXT	ZFULLNAME	ZGIVENNAME	ZPHONENUMBER
	Filtre	Filtre	Filtre	Filtre
1	😂😂😂	Nurcan [redacted]	Nurcan	0 (537) [redacted]
2	Hey there! I am using WhatsApp.	Mehme [redacted]	Mehme [redacted]	0 (537) [redacted]
3	Hey there! I am using WhatsApp.	Erdal M [redacted]	Erdal M [redacted]	0 (534) [redacted]
4	NULL	Sema [redacted]	Sema	0 (506) [redacted]
5	💬⌛⌛🐻	Hatice [redacted]	Hatice	0 (507) [redacted]
6	-	Mustafa [redacted]	Mustafa	0 (536) [redacted]
7	...	Selma [redacted]	Selma	0 (553) [redacted]
8	İyi ki	Fatma [redacted]	Fatma [redacted]	0 (531) [redacted]
9	Hey there! I am using WhatsApp.	Atakent [redacted]	Atakent [redacted]	053897 [redacted]
10	Hey there! I am using WhatsApp.	Nurten [redacted]	Nurten	0 (538) [redacted]
11	🤳	Emine [redacted]	Emine	0 (553) [redacted]

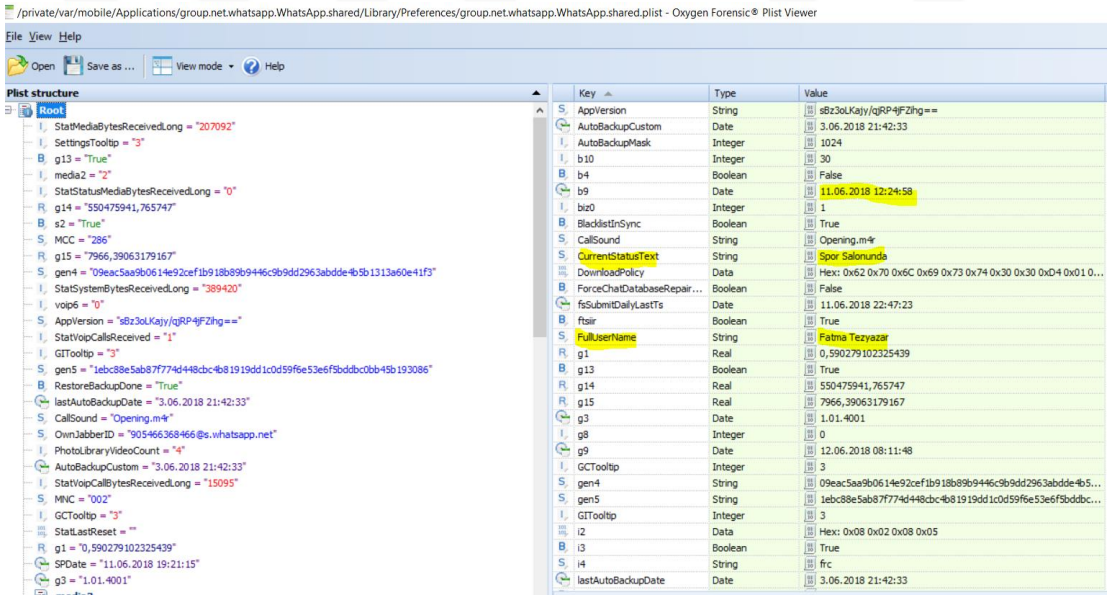
Şekil 5.6. WhatsApp ContactsV2 veritabanı Zwaddressbookcontact tablosu

ChatSearchV3 veri tabanı incelendiğinde Şekil 5.7'de görüldüğü gibi mesaj içerikleri, zamanları, mesajın atıldığı kişinin ya da grubun JID bilgilerini içerdiği görülmektedir.



Şekil 5.7 WhatsApp ChatSearch veritabanı Docs_content tablosu

/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist dosyası Şekil 5.8'deki gibi kullanıcı hesaba ilişkin bilgileri bulundurur.



Şekil 5.8. WhatsApp.shared.plist dosyası

/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ dosyası içerisinde WhatsApp üzerinden paylaşılan medyalar, durum medyaları, profil resimleri bulunmaktadır.

/private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/calls.log dosyasında arama günlüklerini tutmaktadır.

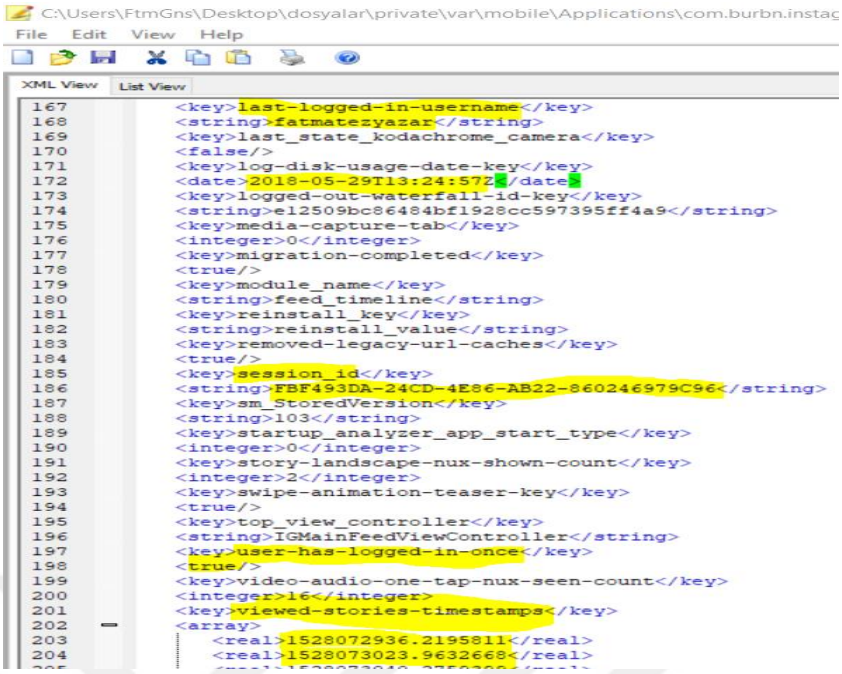
5.1.3 Instagram

Dosya sistemi incelendiğinde Instagram kalıntılarının "/private/var/mobile/Applications/com.burbn.instagram" ve "/private/var/mobile/Applications/group.com.burbn.instagram" klasörleri altında bulunduğu tespit edilmiştir. Uygulamaya ilişkin verilerin bulunduğu dosyalar Şekil 5.9'de verilmiştir. Bu veriler Oxygen Forensic aracından alınmıştır. Bu klasörler içerisindeki *group.com.burbn.instagram.plist*, *com.burbn.instagram.plist* ve *bootstrap-6244347999* dosyaları adli bilişim açısından önem arz eden veriler içermektedir.

File	Type	Size
/private/var/mobile/Applications/com.burbn.instagram/Documents/version_history.plist	.plist	218 B
/private/var/mobile/Applications/com.burbn.instagram/Library/Application Support/DirectSQLiteDatabase/6244347999.db	.db	112,01 KB
/private/var/mobile/Applications/com.burbn.instagram/Library/Cookies/Cookies.binarycookies	.binarycookies	348 B
/private/var/mobile/Applications/com.burbn.instagram/Library/Preferences/com.burbn.instagram.plist	.plist	6,55 KB
/private/var/mobile/Applications/com.burbn.instagram/Library/com-facebook-sdk-AppEventsTimeSpent.json	.json	135 B
/private/var/mobile/Applications/com.burbn.instagram/Library/com-facebook-sdk-PersistedAnonymousID.json	.json	52 B
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-DS7doh		38,19 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-KOvkZd		38,19 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-LNIKIw		38,16 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-NgHEYm		2,69 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-ONl6x4		38,12 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-Xn3da5		38,18 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-dORykF		38,21 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-esQ0OR		38,21 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-mGeznt		38,15 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-tHmuU1		38,18 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-xJ2anF		38,15 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Breakpad/Extra-xKmNJl		38,15 KB
/private/var/mobile/Applications/group.com.burbn.instagram/Library/Preferences/group.com.burbn.instagram.plist	.plist	7,84 KB
/private/var/mobile/Applications/group.com.burbn.instagram/shared_bootstraps/bootstrap-6244347999		10,94 KB

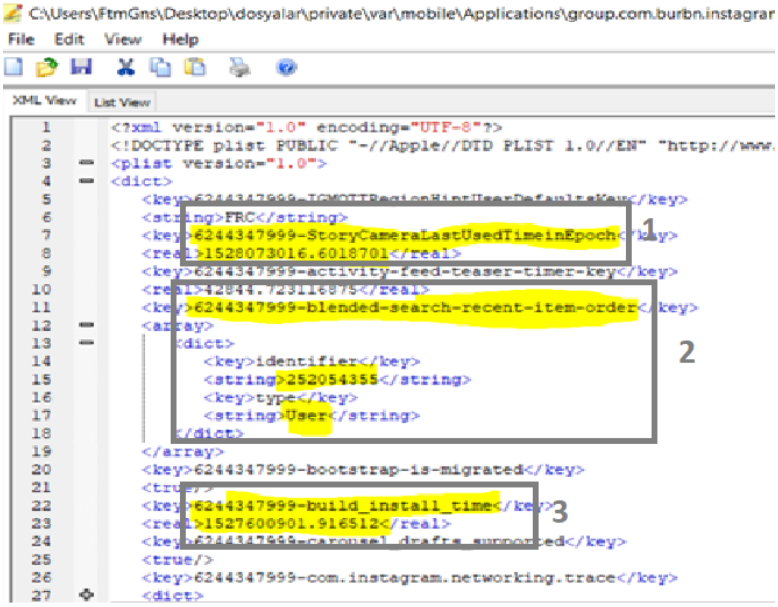
Şekil 5.9. iOS'da Instagram uygulama verilerinin saklandığı dosyalar

com.burbn.instagram.plist dosyası Şekil 5.10'de uygulama hakkında en son giriş yapan kullanıcı adı, kullanıcının daha önce giriş yapıp yapmadığı, oturum ID' si, hikâye görülme zamanları gibi bilgileri içerir.



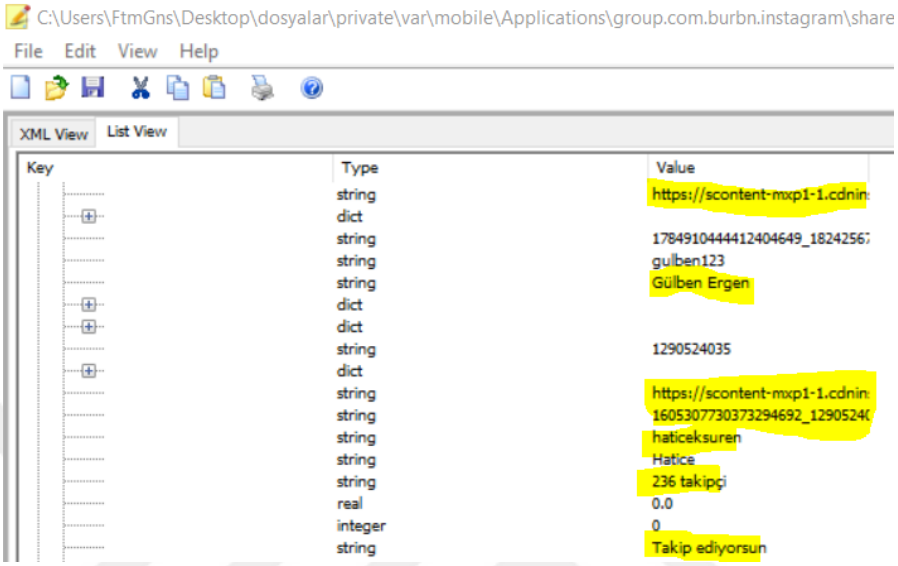
Şekil 5.10. Instagram com.burbn.instagram.plist

group.com.burbn.instagram.plist dosyası incelendiğinde Şekil 5.11'deki gibi kullanıcı ile ilgili kullanıcıya Instagram tarafından atanan ID, çerçeve 1'de kullanıcının en son kamera açma zamanı (Linux epoch formatında), çerçeve 2'de en son yapılan arama, çerçeve 3'de uygulamayı indirme zamanı bilgilerini barındırmaktadır.



Şekil 5.11. Instagram group.com.burbn.instagram.plist

*bootstrap-6244347999 d*osyası incelendiğinde, Şekil 5.12'deki gibi etkileşime geçilen çeşitli profil bilgilerini, kişi ismi, profil resmi URL'si toplam takipçi sayısı, kullanıcı tarafından takip edilme bilgisi gibi bilgileri barındırmaktadır. Gülben ergen hesabı takibe alınmış sonrasında bırakılmıştı. Burada o hesaba dair verilerin bulunduğu görülmektedir.



Şekil 5.12. Instagram bootstrap-6244347999

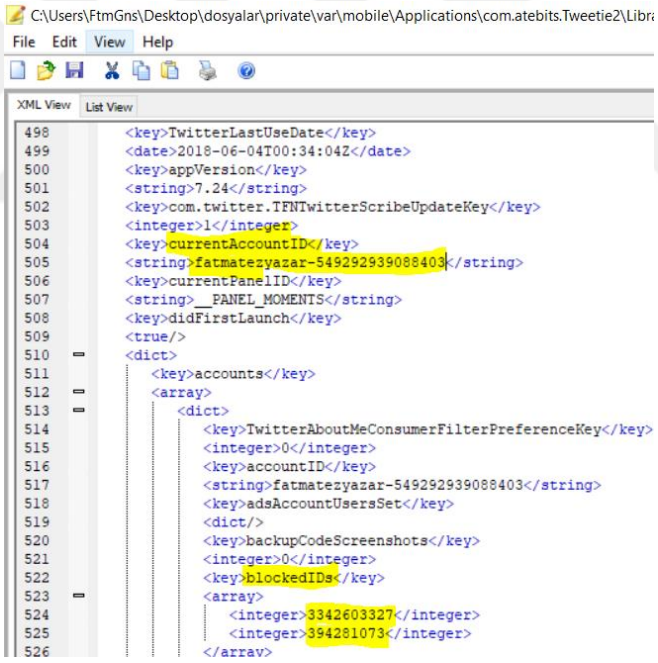
5.1.4 Twitter

Dosya sistemi incelendiğinde Twitter kalıntılarının "/private/var/mobile/Applications/com.atebits.Tweetie2" ve "/private/var/mobile/Applications/group.com.atebits.Tweetie2" klasörü altında olduğu tespit edilmiştir. Uygulamaya ilişkin verilerin bulunduğu dosyalar Şekil 5.13'de verilmiştir. Bu veriler Oxygen Forensic aracından alınmıştır. Bu klasörler altında bulunan com.atebits.Tweetie2.plist app.acct.fatmatezyazar-549292939088403.detail.11 dosyaları önemli verileri barındırmaktadır.

File	Type	Size
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.application-state/app.acct.fatmatezyaz...	.10	1,55 KB
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.application-state/app.acct.fatmatezyaz...	.11	32,41 KB
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.authorizationmanagerTFNAuthorization...	.data	598 B
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.authorizationmanagerTFNAuthorization...	.data	273 B
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.configuration/fs_metrics_state		389 B
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.direct-message.attachments/ADF2948D...		372,35 KB
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.twitter.TFSFeatureSwitches.config/app.featureswitche...	.- guest -	128,59 KB
/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.twitter.TFSFeatureSwitches.config/app.featureswitche...	.fatmatezya...	133,05 KB
/private/var/mobile/Applications/com.atebits.Tweetie2/Library/Application Support/com.crashlytics/CLSUserDefaults.plist	.plist	277 B
/private/var/mobile/Applications/com.atebits.Tweetie2/Library/Cookies/Cookies.binarycookies	.binarycookies	343 B
/private/var/mobile/Applications/com.atebits.Tweetie2/Library/Preferences/com.atebits.Tweetie2.plist	.plist	10,98 KB
/private/var/mobile/Applications/group.com.atebits.Tweetie2/Library/Preferences/group.com.atebits.Tweetie2.plist	.plist	4,13 KB
/private/var/mobile/Applications/group.com.atebits.Tweetie2/com.atebits.tweetie.scribe/scribe.2.sqlite	.sqlite	60,00 KB

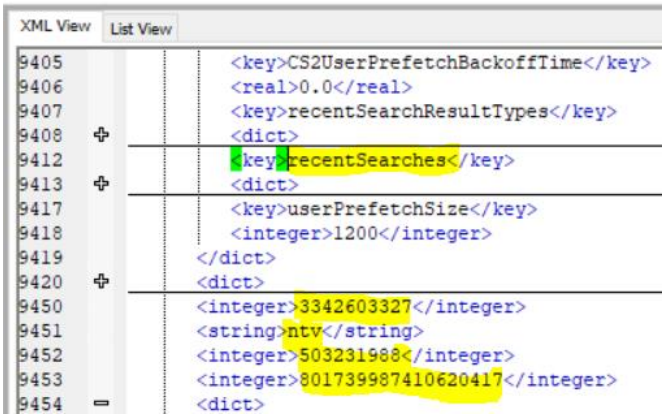
Şekil 5.13. iOS'da Twitter uygulama verilerinin saklandığı dosyalar

Detaylı şekilde incelendiğinde com.atebits.Tweetie2.plist dosyasının kullanıcı hesabı ile ilgili verileri tuttuğu görülmüştür. Şekil 5.14'deki gibi kullanıcıya Twitter tarafından atanan ID ve kullanıcının engellediği hesapların ID bilgileri bu dosya içerisinde yer almaktadır.



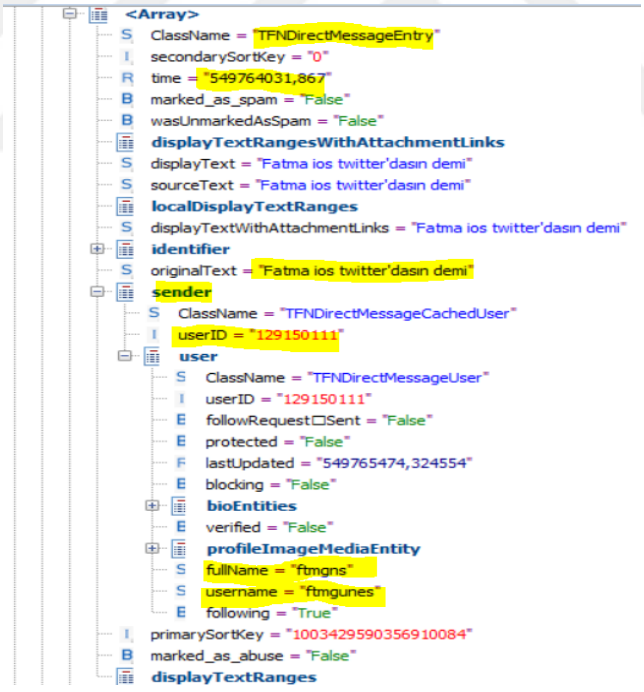
Şekil 5.14. Twitter com.atebits.Tweetie2.plist dosyası

"app.acct.fatmatezyazar-549292939088403.detail.11" dosyasında Şekil 5.15'deki gibi kullanıcının yaptığı aramaların listesinin XML formatında tutulduğu görülmüştür.



Şekil 5.15. Twitter app.acct.fatmatezyazar-549292939088403.detail.11 dosyası

Bu dosyada ayrıca kullanıcının aldığı veya attığı direk mesajların içeriği zaman bilgisi ile birlikte bu dosyada yer aldığı tespit edilmiştir. Şekil 5.16'da tez çalışması için gerçekleştirilen davranışlardan olan mesajın zamanı ve içeriği, mesajı gönderenin ID'si, ismi ve kullanıcı adı bilgileri görüntülenmektedir.



Şekil 5.16. Twitter app.acct.fatmatezyazar-549292939088403.detail.11 dosyası

Detaylı olarak bakıldığında iOS üzerinden atılan mesajların yanı sıra önceden var olan direk mesajların da görüntülendiği tespit edilmiştir. Silinen mesaj verisine dosyada erişilememiştir.

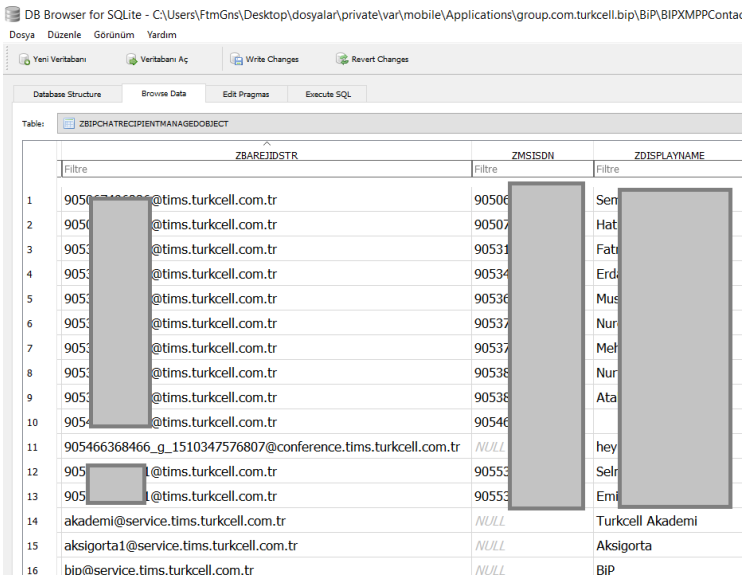
"/private/var/mobile/Applications/com.atebits.Tweetie2/Documents/com.atebits.tweetie.dir

ect-message.attachments" klasöründe direk mesaj ile atılan mesaj eklerinin yer aldığı klasördür.

5.1.5 BiP Messenger

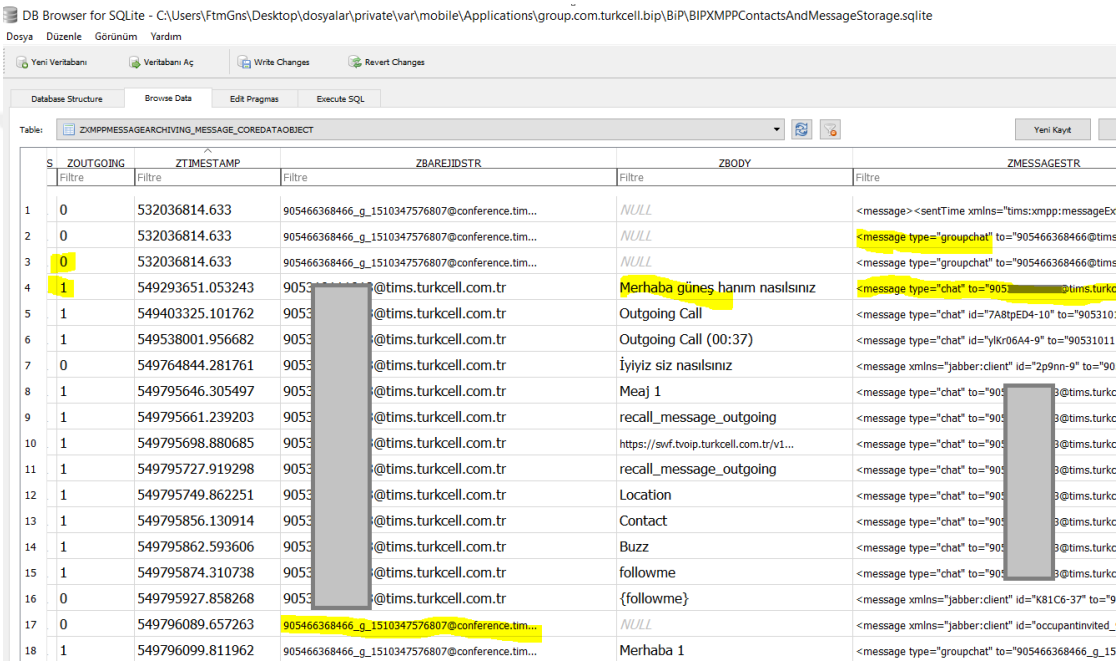
Dosya sistemi incelendiğinde BiP Messenger kalıntılarının "/private/var/mobile/Applications/group.com.turkcell.bip" ve "/private/var/mobile/Applications/com.turkcell.bip" klasörü altında olduğu tespit edilmiştir. Bu klasörlerin altında bulunan "BIPXMPPContactsAndMessageStorage.sqlite", "BIPXMPPMessagesInfoStorage.sqlite", "FollowMeCoreDataStorage.sqlite" dosyalarının önemli veriler içerdiği tespit edilmiştir.

"BIPXMPPContactsAndMessageStorage.sqlite" veritabanı incelendiğinde ZBIPCHATRECIPIENTMANAGEDOBJECT tablosundaki veriler Şekil 5.17 'deki gibidir. Burada ZBAREJIDSTR sütunu kullanıcılara, gruplara ve servislere atanan ID bilgisini tutmaktadır. Bu ID bilgisi, kişi ise "KişininNumarası@tims.turkcell.com.tr", grup ise "GrubuKuranKişiJidBilgisi_g_Grubun KurulduğuZaman@conference.tims.turkcell.com.tr "@conference.tims.turkcell.com.tr" , servis ise sonu "@service.tims.turkcell.com.tr" şeklinde tutulmaktadır. Bu tabloda ZMSISDN sütununda kişi telefon numarası, ZDISPLAYNAME sütununda kullanıcı ismi tutulmaktadır.



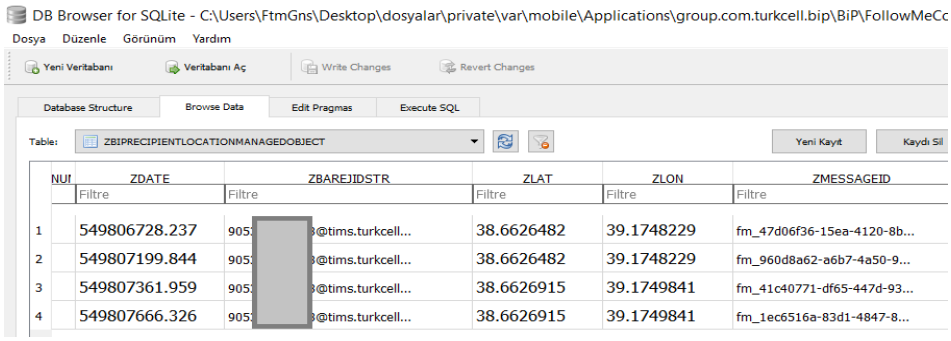
Şekil 5.17. BiP BIPXMPPContactsAndMessageStorage veritabanı

Bu veritabanının ZXMPPMESSAGEARCHIVING_MESSAGE_COREDATA OBJECT tablosu mesajları tutan tablodur. Bu tablonun ZOUTGOING sütunu mesajın yönünü, ZTIMESTAMP sütunu zamanını, ZBAREJIDSTR sütunu mesajın geldiği/gittiği kişinin/grubun/servisin ID'sini, ZBODY sütunu içeriğini, ZMESSAGESTR sütunu mesaj ile ilgili detaylı bilgileri Şekil 5.18'deki gibi tutmaktadır. Bu veritabanının ZBIPSERVICECATEGORYMANAGEDOBJECT tablosu servislerin kategorilerini tutan tablodur.



Şekil 5.18. BiP BIPXMPPContactsAndMessageStorage veritabanı

BIPXMPPMessagesInfoStorage.sqlite tablosu mesajın iletilme ve görüntülenme gibi bilgileri detaylarını barındırmaktadır. FollowMeCoreDataStorage.sqlite veritabanı ise uygulamadaki takip etme özelliği ile ilgili detaylı bilgileri bulunduran veritabanıdır. Şekil 5.19'de görüldüğü üzere takip etme mesajının zamanı, kime atıldığı, enlem, boylam, ve mesaja ait ID bilgileri bu veritabanının ZBIPRECIPENTLOCATIONMANAGEOBJECT tablosunda tutulduğu tespit edilmiştir.

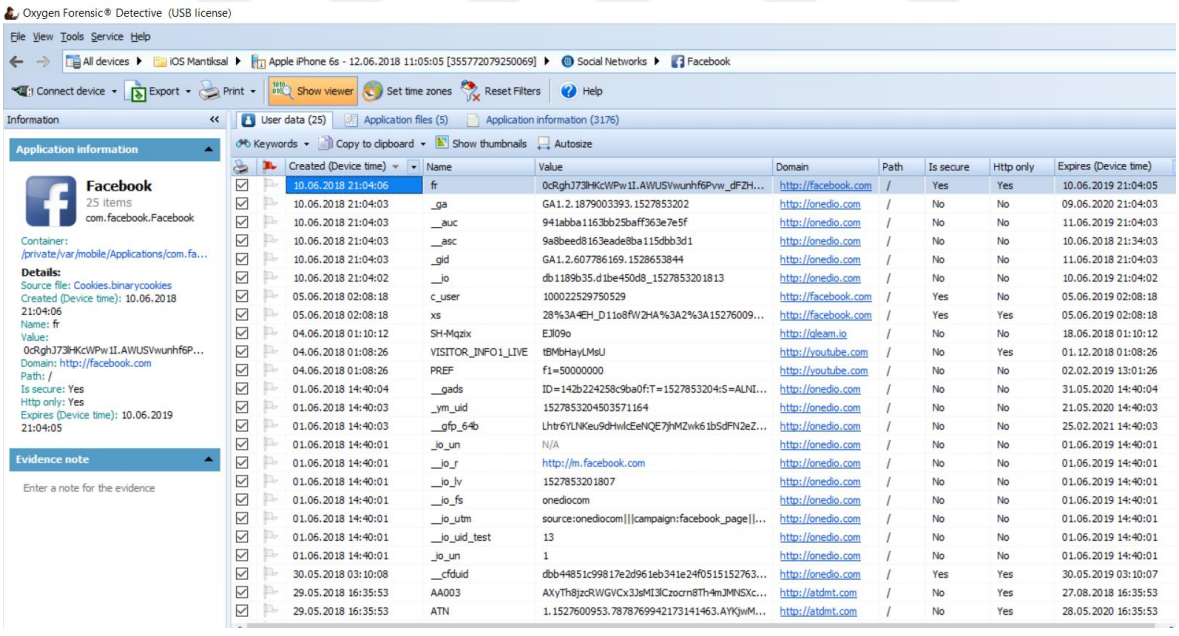


Şekil 5.19. BiP FollowMeCoreDataStorage veritabanı

5.2 Adli Araçlar Yardımıyla Elde Etme

5.2.1 Facebook

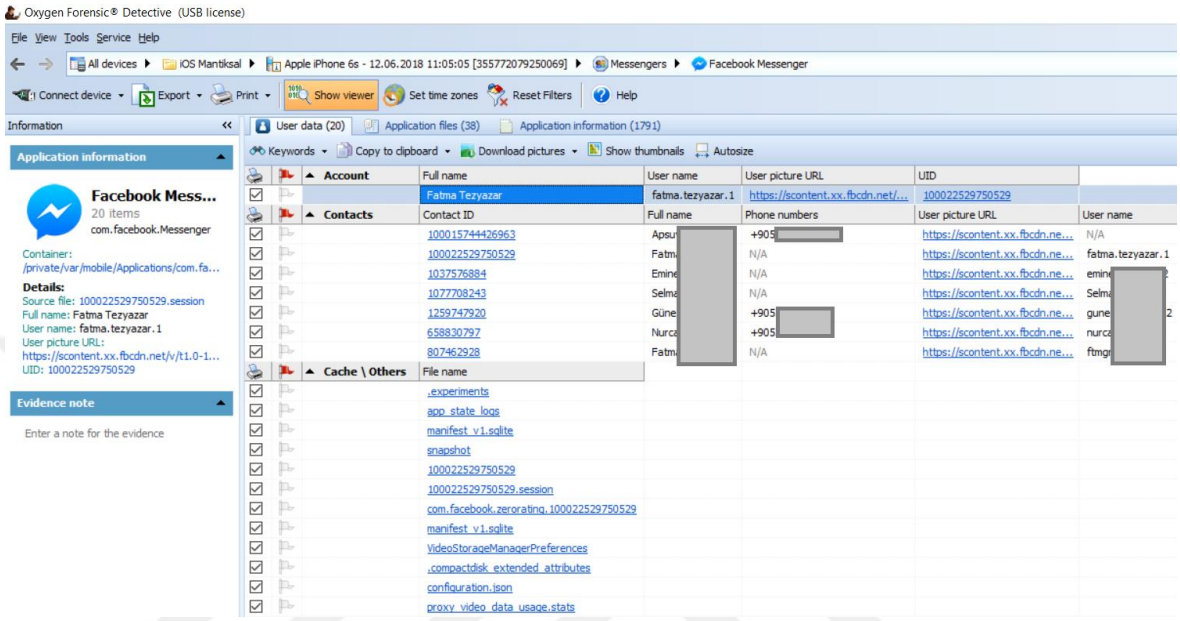
Oxygen Forensic aracı ile alınan mantıksal imaj incelendiğinde Facebook uygulamaları ile ilgili ayıklanarak kullanıcıya sunulan veriler Şekil 5.20 verilmiştir. Detaylı şekilde bakıldığında Facebook uygulamasına ilişkin yalnızca çerez bilgilerinin getirildiği gözlemlenmiştir.



Şekil 5.20. Oxygen Forensic Facebook ekranı

Facebook Messenger uygulamaları ile ilgili ayıklanarak kullanıcıya sunulan veriler Şekil 5.21'de verilmiştir. Facebook Messenger uygulaması ile ilgili ise kullanıcı hesap bilgileri *Account* başlığı altında, kişinin ismi, kullanıcı adı, profil resmi URL'si ve kişiye

Facebook tarafından atanan benzersiz ID ile sunulmaktadır. *Contacts* başlığı altında ise iletişime geçilen kişilerin ID'leri, isimleri, telefon numaraları, profil resmi URL'leri ve kullanıcı isim bilgileri bulunmaktadır. *Cache/others* başlığı altında ise uygulamanın bazı ayarlar dosyalar, önbelleğe alınan bazı dosyalar görüntülenmektedir.



Şekil 5.21. Oxygen Forensic Facebook Messenger ekranı

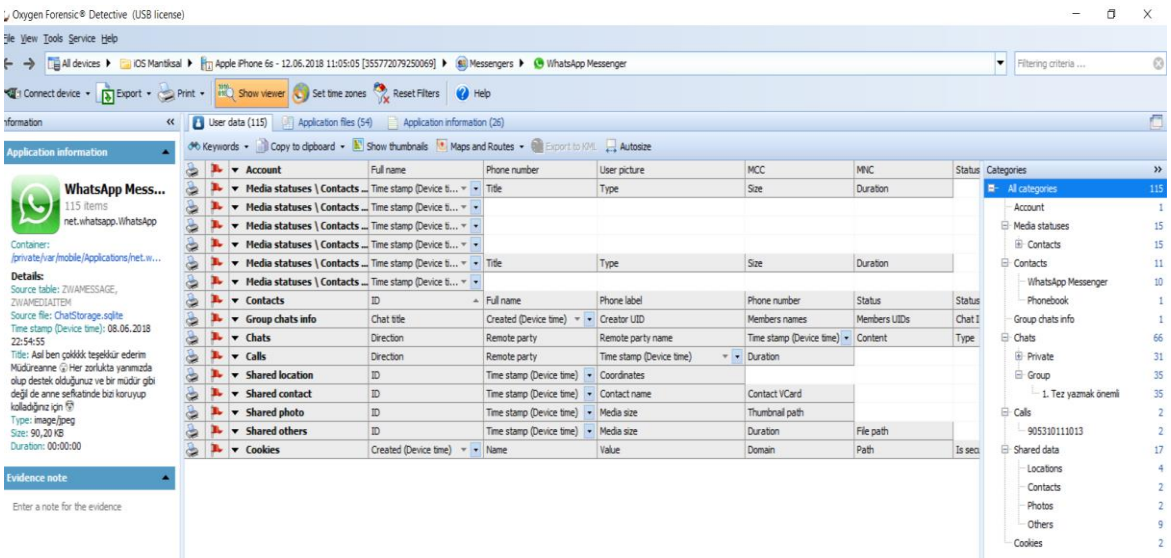
Paraben aracı ile alınan mantıksal imaj incelendiğinde Facebook ve Facebook Messenger uygulamalarına ait verilerin ayıklanarak kullanıcıya sunulmadığı görülmüştür. Uygulama ile ilgili verileri incelemek için verilerin saklandığı yerleri bulup dosya yoluna gidip incelenmelidir. Bu da manuel olarak incelemede anlatılmıştır.

Axiom aracı ile alınan mantıksal imaj incelendiğinde Facebook uygulamasına ait ayıklanmış veriler deki gibi görüntülenmektedir. Düzeltilmiş sonuçlar altında ziyaret edilmiş Facebook URL'leri bulunmaktadır. Bu URL'lere ait potansiyel etkinlikler, URL kimliği, verinin elde edildiği kaynak ve konum belirtilmiştir. Uygulama ile ilgili diğer verileri incelemek için verilerin saklandığı yerleri bulup dosya yoluna gidip incelenmelidir.

5.2.2 WhatsApp Messenger

Oxygen Forensic ile alınan mantıksal imaj incelendiğinde WhatsApp kalıntılarının "/private/var/mobile/Applications/net.whatsapp.WhatsApp" ve "/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared" klasörleri altında

bulunduğu gözlenmiştir. Oxygen yazılımı ile uygulama sekmesindeki WhatsApp'ı seçtiğimizde kullanıcıya veriler Şekil 5.22' deki gibi sunulmaktadır. Burada "Userdata" kısmında hesap bilgisi, medya durumu bulunan kişiler, kişi listesi, grup mesaj bilgisi, mesajlar, aramalar, paylaşılan veriler (konum, kişi, resim ve diğerleri) ve çerez bilgileri bulunmaktadır. Bu kısım analiz yapan kişiye kolaylık sağlamaktadır. Yazılım önemli verileri çekerek hızlı şekilde kullanıcıya sunmaktadır.



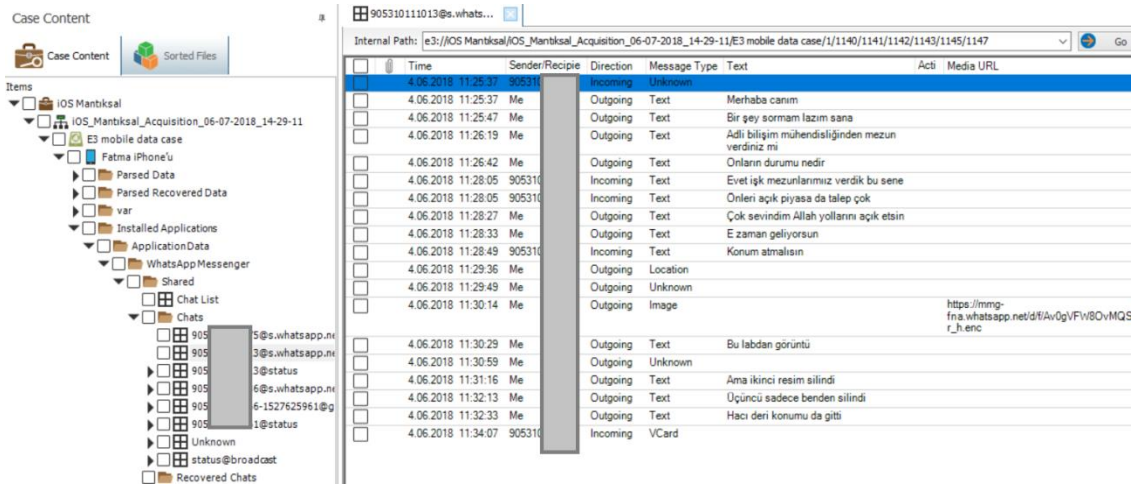
Şekil 5.22. iOS Oxygen Forensic WhatsApp Çıktısı

Burada "Account" kısmında hesap sahibinin kişi bilgisi, telefon numarası, profil resmi, durum bilgisi, en son yedekleme zamanı görüntülenir. "Media statuses/ contacts/ kişi ismi" kısmında medya durumu görüntülenen kişinin durum bilgisini paylaşma zamanı, varsa başlığı, dosya tipi, boyutu, video ise süresi bilgisi görüntülenir. "Contacts" kısmında kişi listesi; ismi, telefon etiketi, telefon numarası, durum bilgisi, durum ekleme bilgisi, profil resimleri ile birlikte görüntülenmektedir. "Group Chat info" kısımında grup konu başlığı, grup oluşturulma zamanı, grubu oluşturan kişinin telefon numarası, üyelerinin telefon numaraları görüntülenmektedir. "Chats" kısmında mesajlar mesaj yönü, mesajlaşmadaki karşı tarafın telefon numarası, WhatsApp ismi, zaman bilgisi, içeriği, mesaj tipi, paylaşılan bir dosya ise boyutu, video veya ses dosyası ise süresi, varsa ismi görüntülenir. "Calls" kısmında yapılan konuşmaların yönü, karşı tarafın telefon numarası, yapıldığı zaman ve ne kadar sürdüğü bilgileri bulunur. "Shared location" kısmında paylaşılan konum bilgisinin zamanı, ve koordinat bilgileri görüntülenir. "Shared contact" kısmında paylaşılan kişi bilgilerinin paylaşılma zamanı, ismi, kişiye ait tüm bilgilerin bulunduğu Vcard bilgileri

bulunur. “Shared photo” paylaşılan fotoğrafın paylaşılma zamanı, boyutu, tırnak resminin dosya yolu bilgileri bulunur. “Cookies” kısmında ise çerezlerin oluşturma zamanı değeri gibi bilgileri barındırmaktadır.

“Application files” kısmında içerisinde veri bulunan ve uygulamanın erişime izin verdiği bütün dosyalar görüntülenmektedir.

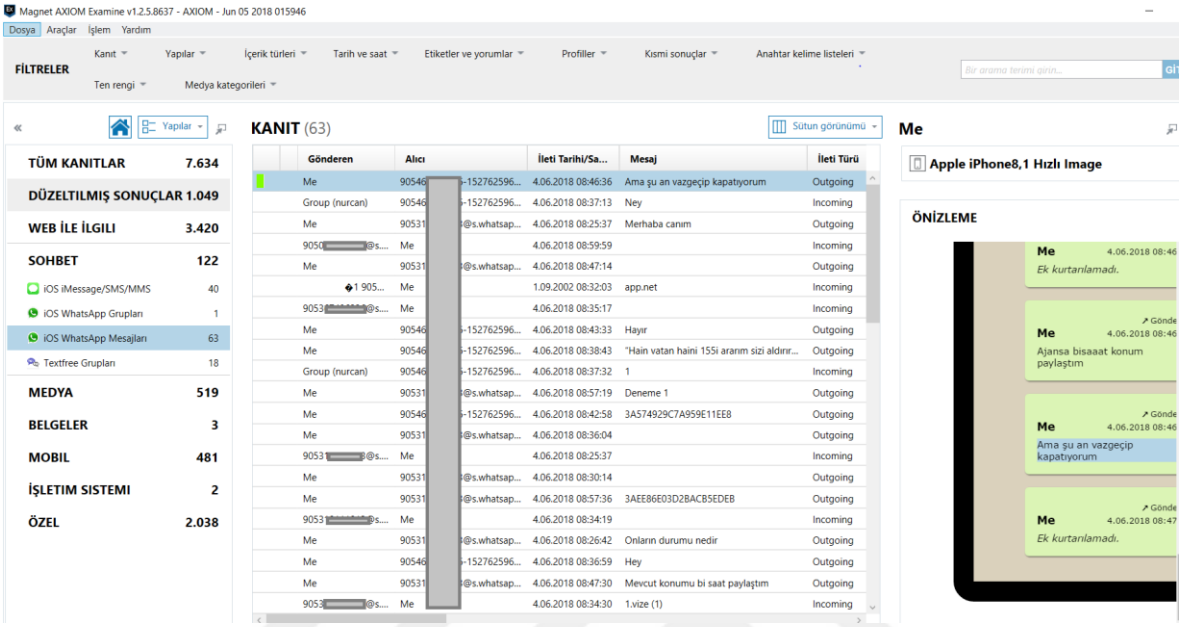
Paraben aracı ile alınan mantıksal imaj incelendiğinde Uygulama verileri olarak WhatsApp Messenger verileri kullanıcıya Şekil 5.23’deki gibi sunulduğu görülmüştür. Veriler incelendiğinde genel olarak görüşme yapılan kişilerin listesi, mesajlaşmalar, kişilerin durumları bilgileri verilmektedir. *Chat List* başlığı altında iletişime geçilen grup veya kişinin ismi, grupsa üyelerin telefon numaraları, chat ID olarak adlandırılan kişiler için “telefon numarası @ s.whatsapp.net”, gruplar için “grubu kuran kişinin telefon numarası- ne zaman kurduğu damga pulu @g.us” , durum paylaşımı için “kişinin telefon numarası @status” şeklinde kimlikler bulunur. *Chats* başlığı altında Chat ID’lerin başlıkları altında yapılan mesajlaşmalar görüntülenir. Bu mesajlaşmalar incelendiğinde ise mesajın gönderilme zamanı, gönderen veya alıcı numarası, mesaj yönü, mesaj tipi, mesaj içeriği, paylaşılan dosya varsa URL’si, dosya yolu, boyutu, paylaşılan bir konum ise koordinatları, VCard bilgilerine erişilir. *Recoverd Chats* başlığı altında ise hiçbir veriye ulaşılamamıştır.



Şekil 5.23. Paraben WhatsApp çıktısı

Axiom aracı ile alınan mantıksal imaj incelendiğinde uygulama verileri olarak WhatsApp Messenger verileri kullanıcıya Şekil 5.24 gibi sunulduğu görülmüştür. *iOS WhatsApp Grupları* başlığı altında gruba atanan ID, grup adı, oluşturulduğu tarih, grup üyelerinin isimleri ve ID’leri, bilgileri aldığı kaynağı ve veri tabanının konumu görüntülenir.

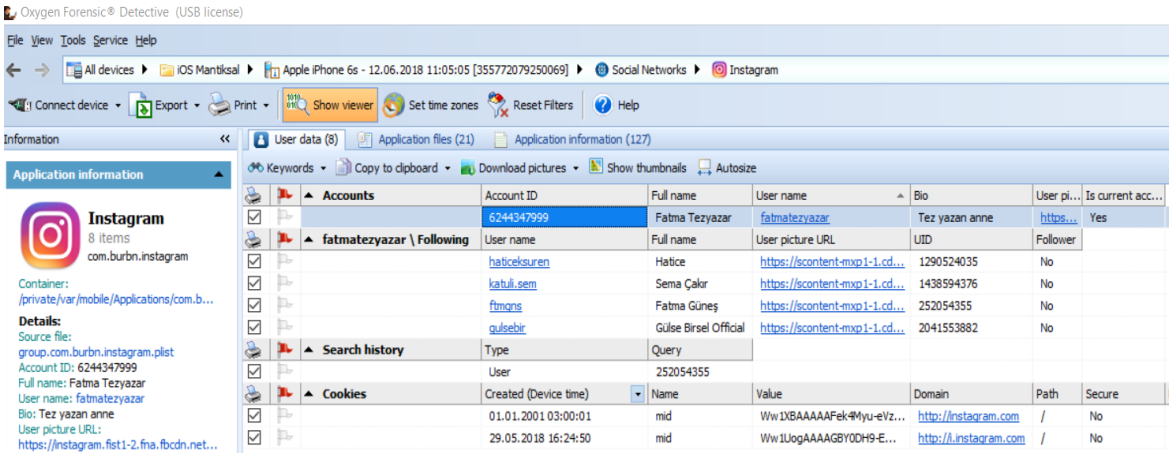
iOS WhatsApp Mesajları başlığı altında ise mesajın göndereni, alıcı ID'leri, gönderilme zamanı, içeriği, yönü, ekte dosya varsa URL'si dosya konumu verilerin kaynağını ve veritabanı görüntülenmektedir.



Şekil 5.24. Axiom WhatsApp Çıktısı

5.2.3 Instagram

Oxygen Forensic aracı ile alınan mantıksal imaj incelendiğinde Instagram uygulamasına ait verilerin ayıklanarak kullanıcıya Şekil 5.25'deki gibi sunulduğu görülmektedir. Burada *Accounts* başlığı altında uygulama üzerinden giriş yapan hesaplara ait, ID, isim, kullanıcı adı, biyografi, kullanıcı profil resmi URL'si, o sırada aktif olan hesap olup olmadığı bilgisi bulunur. *Fatmatezyazar\following* başlığı altında ise kullanıcının takip ettiği hesapların kullanıcı adı, ad_soyad, kullanıcı profil resmi URL'si, Instagram tarafından atanan ID, kişinin kullanıcının hesabını takip bilgisi bulunur. Search history başlığı altında arama yapılan kullanıcı, kelime yada etiket bulunur. Cookies başlığı altına ise çerez bilgileri bulunmaktadır. *Aplication Files* kısmında ise uygulama ile ilgili kullanıcı erişimine açılmış tüm dosyalar bulunmaktadır.

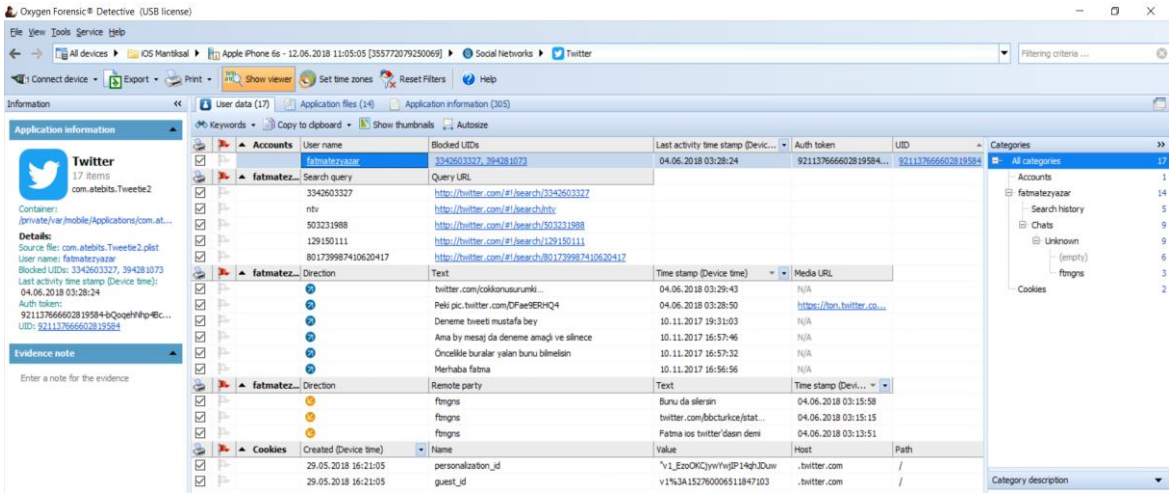


Şekil 5.25. Oxygen Forensic Instagram çıktısı

Paraben aracı ve Axiom aracı ile alınan mantıksal imajlar incelendiğinde Instagram'a ait verilerin ayıklanarak kullanıcıya sunulmadığı görülmüştür. Uygulama ile ilgili verileri incelemek için verilerin saklandığı yerleri bulup dosya yoluna gidip incelenmelidir. Bu da manuel olarak incelemede anlatılmıştır.

5.2.4 Twitter

Oxygen Forensic aracı ile alınan mantıksal imaj incelendiğinde Instagram uygulamasına ait verilerin ayıklanarak kullanıcıya Şekil 5.26'deki gibi sunulduğu görülmektedir. Burada *Accounts* başlığı altında kullanıcı ismi, kullanıcı tarafından engellenen hesap ID'leri, en son eylem zamanı, kullanıcıya Twitter tarafından atanan ID bilgileri bulunur. *Search history* kısmında aranan kelime ya da ID ve bu aramaların URL'leri bulunur. *Chats* başlığı altında mesajlaşmaların yönü, karşı tarafın kullanıcı ismi, içeriği, zamanı, ekte bir medya URL'si bulunur. *Cookies* başlığı altında çerez bilgi detayları bulunmaktadır.



Şekil 5.26. Oxygen Forensic Twitter çıktısı

Paraben aracı ile alınan mantıksal imaj incelendiğinde Instagram'a ait verilerin ayıklanarak kullanıcıya sunulmadığı görülmüştür. Uygulama ile ilgili verileri incelemek için verilerin saklandığı yerleri bulup dosya yoluna gidip incelenmelidir. Bu da manuel olarak incelemede anlatılmıştır.

Axiom aracı ile alınan mantıksal imaj incelendiğinde Twitter uygulamasına ait verilerin ayıklanarak kullanıcıya özel bir başlık altında sunulmadığı görülmektedir. Sosyal medya URL'leri altında şekildeki biçimde Twitter'da ziyaret edilmiş bazı URL'lere rastlanmıştır. Uygulama ile ilgili detaylı verileri incelemek için verilerin saklandığı yerleri bulup dosya yoluna gidip incelenmelidir. Bu da manuel olarak incelemede anlatılmıştır.

5.2.5 BiP Messenger

BiP uygulaması genel olarak Türk kullanıcısına hitap ettiği için mobil adli bilişim araçları tarafından tanınıp ayıklanamamaktadır. BiP gibi belli bir kesim tarafından kullanılan uygulamaların analizi manuel olarak gerçekleştirilir.

6. TESPİT EDİLEBİLEN KULLANICI DAVRANIŞLARI VE SONUÇLAR

Bu bölümde Bölüm 3.2'de bahsedilen gerçekleştirilmiş kullanıcı davranışlarının sosyal medya uygulamaları üzerinde analizi yapılmıştır. Tablo 3.3, Tablo 3.4, Tablo 3.5, Tablo 3.6 ve Tablo 3.7'de gerçekleştirilen kullanıcı davranışlarının analizi sırasında bulunabilen ve bulunamayan kanıtlar tablolar halinde sunulmuştur.

6.1 Android İşletim Sisteminden Elde Edilen Sonuçlar

Bu bölümde Android cihaz üzerinde manuel ve araçlarla yapılan analizlerden elde edilen sonuçlar uygulamaya ait veriler ve kullanıcı davranışları olarak sınıflandırılarak tablo haline getirilmiştir. Tablolarda uygulamalara ait verilerin ve üzerlerinde gerçekleştirilen kullanıcı davranışlarının, imajlardan araçlarla veya manuel olarak editörlerle tespit edilip edilmediği bilgilerine yer verilmiştir.

6.1.1 Facebook

Facebook uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.1'da verilmiştir. Tablo incelendiğinde Android cihazın Paraben ve Oxygen araçları ile alınan mantıksal imajlarından veri edinilemediği görülmektedir. Kullanıcı davranışlarından olan paylaşım, yorum, beğeni hareketleri analiz sırasında tespit edilememiştir. Fiziksel imajlardan hem araçlarla hem de manuel olarak kişi bilgileri, medya dosyaları, önbellek dosyaları, mesajlar, grup mesajları edinilebilmekte iken silinmiş mesajlara yalnızca manuel olarak erişilebildiği görülmüştür.

Tablo 6.1. Android Facebook uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Oxygen Fiziksel	Paraben Mantıksal	Paraben Fiziksel	Axiom Fiziksel	Manuel
Uygulamaya Ait Veriler						
Hesap bilgileri	-	+	-	-	-	+
Kişi Bilgileri	-	+	-	+	+	+
Medya	-	+	-	+	+	+
Önbellek dosyaları	-	+	-	+	+	+
Mesaj	-	+	-	+	+	+
Grup mesajı	-	+	-	+	+	+
Aramalar	-	+	-	+	+	+
Dosya eki	-	+	-	-	-	+

Tablo 6.2. Android Facebook uygulama verileri ve kullanıcı davranışları (Devamı)

Kullanıcı Davranışları						
Paylaşım	-	-	-	-	-	-
Yorum	-	-	-	-	-	-
Beğeni	-	-	-	-	-	-
Eklenmiş Arkadaş	-	+	-	+	+	+
Grup paylaşımı	-	-	-	-	-	-
Hikâye	-	-	-	-	-	-
Mesaj	-	+	-	+	+	+
Silinmiş mesaj	-	-	-	-	-	+
Grup mesajı	-	+	-	+	+	+
Silinmiş grup mesajı	-	-	-	-	-	+

6.1.2 WhatsApp Messenger

WhatsApp Messenger uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.3'da verilmiştir. Tablo incelendiğinde Android cihazın Paraben ile alınan mantıksal imajından kişi bilgilerine, Oxygen aracı ile alınan mantıksal imajdan ise paylaşılan medyalara erişildiği görülmektedir. Fiziksel imajlar incelendiğinde Paraben aracının hesap bilgilerini kullanıcıya direk sunmadığı, diğerleri ile erişilebildiği, silinmiş mesajlara yalnızca manuel olarak erişilebildiği tespit edilmiştir.

Tablo 6.3. Android WhatsApp Messenger uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Oxygen Fiziksel	Paraben Mantıksal	Paraben Fiziksel	Axiom Fiziksel	Manuel
Uygulamaya Ait Veriler						
Hesap bilgileri	-	+	-	-	+	+
Profil resimleri	-	+	-	+	+	+
Kişi Bilgileri	-	+	+	+	+	+
Grup Bilgileri	-	+	-	+	+	+
Grup Mesajları	-	+	-	+	+	+
Kişi mesajları	-	+	-	+	+	+
Aramalar	-	+	-	+	+	+
Medya	+	+	-	+	+	+
Kullanıcı Davranışları						
Text Mesaj	-	+	-	+	+	+
Silinen mesaj	-	-	-	-	-	+
Fotoğraf paylaşımı	+	+	-	+	+	+
Konum paylaşımı	-	+	-	+	+	+
Grup text mesajı	-	+	-	+	+	+
Silinen grup text mesajı	-	-	-	-	-	+
Grup fotoğraf paylaşımı	+	+	-	+	+	+
Arkadaş engelleme	-	-	-	-	-	-
Görüntülü konuşma	-	+	-	+	+	+
Sesli Konuşma	-	+	-	+	+	+
Durum paylaşımı	-	-	-	+	-	-

6.1.3 Instagram

Instagram uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.4'da verilmiştir. Tablo incelendiğinde Android cihazın Paraben ve Oxygen araçları ile alınan mantıksal imajlarından yalnızca paylaşılan medyalara erişilebildiği görülmektedir. Kullanıcı davranışlarından olan durum paylaşımına ve paylaşım kaydetme hareketleri analiz sırasında tespit edilememiştir. Fiziksel imajlardan hem araçlarla hem de manuel olarak iletişime geçilen kişi bilgileri, medya dosyaları, önbellek resimleri, mesajlar edinilebilmekte iken iptal edilen mesajlara yalnızca manuel olarak erişilebildiği görülmüştür. Anasayfadaki paylaşımları görüntüleyebilme bunların kullanıcı tarafından beğenilip beğenilmediği, etiket arama özelliklerin Oxygen Forensic aracı ile ve manuel arama ile fiziksel imajlardan tespit edilebildiği görülmüştür.

Tablo 6.4. Android Instagram uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Oxygen Fiziksel	Paraben Mantıksal	Paraben Fiziksel	Axiom Fiziksel	Manuel
Uygulamaya Ait Veriler						
Hesap bilgileri	-	+	-	+	+	+
İletişime geçilen kişiler	-	+	-	+	+	+
Mesajlar	-	+	-	+	+	+
Ana sayfa	-	+	-	-	-	+
Arama geçmişi	-	+	-	-	-	+
Medya	+	+	+	+	+	+
Önbellek resimleri	-	+	-	+	+	+
Kullanıcı Davranışları						
Paylaşım	+	+	+	+	+	+
Durum	-	-	-	-	-	-
Beğeni	-	+	-	-	-	+
Yorum	-	-	-	-	-	+
Mesaj	-	-	-	+	+	+
İptal edilen mesaj	-	-	-	-	-	+
Takip	-	-	-	-	-	+
Paylaşım kaydetme	-	-	-	-	-	-
Etiket	-	+	-	-	-	+

6.1.4 Twitter

Twitter uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.5'da verilmiştir. Tablo incelendiğinde Android cihazın alınan mantıksal imajlarından Paraben ile veri edinilemediği Oxygen aracında ise önbelleğe alınan resim dosyalarının bulunduğu görülmektedir. Paraben aracı gerek mantıksal gerekse fiziksel imajlarında, Twitter uygulaması ile ilgili verileri ayıklayarak kullanıcıya sunmadığı görülmektedir. Axiom aracı fiziksel imajdan yalnızca kişi bilgilerini, hesap bilgilerini, direk mesajları ve önbellek dosyalarını ayıklayarak kullanıcıya sunmaktadır. Tabloda verilen diğer tüm özelliklere hem Oxygen Forensic aracı ile hem de manuel olarak erişilebilmektedir.

Tablo 6.5. Android Twitter uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Oxygen Fiziksel	Paraben Mantıksal	Paraben Fiziksel	Axiom Fiziksel	Manuel
Uygulamaya Ait Veriler						
Hesap bilgileri	-	+	-	-	+	+
Twitter arkadaşları	-	+	-	-	+	+
Takip edilenler	-	+	-	-	-	+
Takipçiler	-	+	-	-	-	+
Tweetler	-	+	-	-	-	+
Arama geçmişi	-	+	-	-	-	+
Direk mesaj	-	+	-	-	+	+
Önbellek dosyaları	+	+	-	+	+	+
Kullanıcı Davranışları						
Tweet	-	+	-	-	-	+
Silinmiş tweet	-	+	-	-	-	+
Yanıt	-	+	-	-	-	+
Retweet	-	+	-	-	-	+
Mesaj(DM)	-	+	-	-	+	+
Silinen mesaj	-		-	-	-	+
Hesap Takip	-	+	-	-	+	+
Takipten çıkarılan	-	+	-	-	+	+

6.1.5 BiP Messenger

BiP Messenger uygulaması yerel kullanıma hitap ettiği ve mobil adli bilişim aracı üreticileri tarafınca ayıklanmadığı için araçlarla analiz kısmında herhangi bir kullanıcı davranışına ulaşılamamıştır. Alınan dd imajdan elde edilen uygulama dosyaları manuel olarak analiz edilerek bulunan kullanıcı davranışları tespit edilebilmiştir. Tablo 6.6'de elde edilebilen kullanıcı davranışları verilmiştir. Bu davranışlardan engellenen arkadaşların tespit edilemediği görülmüştür.

Tablo 6.6. Android BiP Messenger uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Oxygen Fiziksel	Paraben Mantıksal	Paraben Fiziksel	Axiom Fiziksel	Manuel
Kullanıcı Davranışları						
Mesajlaşma	-	-	-	-	-	+
Silinmiş mesaj	-	-	-	-	-	+
Fotoğraf paylaşımı	-	-	-	-	-	+
Konum paylaşımı	-	-	-	-	-	+
Grup mesajı	-	-	-	-	-	+
Silinmiş grup mesajı	-	-	-	-	-	+
Arkadaş engelleme	-	-	-	-	-	-
Zamanlı mesaj paylaşımı	-	-	-	-	-	+
Zamanlı konum paylaşımı	-	-	-	-	-	+

6.2 iOS İşletim Sisteminden Elde Edilen Sonuçlar

Bu bölümde iOS cihazın alınan mantıksal imajı üzerinde manuel ve araçlarla yapılan analizlerden elde edilen sonuçlar uygulamaya ait veriler ve kullanıcı davranışları olarak sınıflandırılarak tablo haline getirilmiştir. Tablolarda uygulamalara ait verilerin ve üzerlerinde gerçekleştirilen kullanıcı davranışlarının, imajlardan araçlarla veya manuel olarak editörlerle tespit edilip edilmediği bilgilerine yer verilmiştir.

6.2.1 Facebook

Facebook uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.7'da verilmiştir. Tablo incelendiğinde iOS cihazın Paraben, Oxygen, Axiom araçları ile alınan mantıksal imajlarından Paraben ve Axiom araçları ile hiç veri edinilemediği görülmektedir. Oxygen aracı ile ve manuel olarak yapılan analizde ise uygulamaya ait verilerden medya, mesaj, grup mesajı, aramalara kullanıcı davranışlarından paylaşım, yorum, beğeni, hikaye paylaşımı verilerinin hiç birine erişilemediği görülmüştür. Hesap bilgileri, kişi bilgileri, önbellek dosyaları, çerez bilgilerine ise erişilebilmektedir.

Tablo 6.7. iOS Facebook uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Paraben Mantıksal	Axiom Mantıksal	Manuel
Uygulamaya Ait Veriler				
Hesap bilgileri	+	-	-	+
Kişi Bilgileri	+	-	-	+
Medya	-	-	-	-
Önbellek dosyaları	+	-	-	+
Mesaj	-	-	-	-
Grup mesajı	-	-	-	-
Aramalar	-	-	-	-
Çerez bilgileri	+	-	-	+
Kullanıcı Davranışları				
Paylaşım	-	-	-	-
Yorum	-	-	-	-
Beğeni	-	-	-	-
Kişi listesi	+	-	-	+
Grup paylaşımları	-	-	-	-
Hikaye	-	-	-	-
Mesaj	-	-	-	-
Grup mesajı	-	-	-	-

6.2.2 WhatsApp Messenger

WhatsApp Messenger uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.7'de verilmiştir. Tablo incelendiğinde iOS cihazın Paraben, Oxygen, Axiom araçları ile alınan mantıksal imajlarından silinen mesaj ve grup mesajlarına erişilemediği görülmektedir. Tablo genel olarak incelendiğinde araçlardan ve manuel analizden; durum bilgileri, grup bilgileri, mesajlar, grup mesajları, fotoğraf ve konum paylaşımlarının çıkarılabildiği belirlenmiştir. Axiom aracının diğer araçlardan hesap bilgileri, kişi bilgilerini, yapılan sesli ve görüntülü aramaları bulamada yetersiz kaldığı gözlemlenmiştir.

Tablo 6.8. iOS WhatsApp Messenger uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Paraben Mantıksal	Axiom Mantıksal	Manuel
Uygulamaya Ait Veriler				
Hesap bilgileri	+	-	-	+
Durum bilgileri	+	+	+	+
Kişi Bilgileri	+	+	-	+
Grup Bilgileri	+	+	+	+
Grup Mesajları	+	+	+	+
Kişi mesajları	+	+	+	+
Aramalar	+	+	-	+
Medya	+	+	+	+

Tablo 6.9. iOS WhatsApp Messenger uygulama verileri ve kullanıcı davranışları (Devamı)

Kullanıcı Davranışları				
Text Mesaj	+	+	+	+
Silinen mesaj	-	-	-	-
Fotoğraf paylaşımı	+	+	+	+
Konum paylaşımı	+	+	+	+
Grup text mesajı	+	+	+	+
Silinen grup text mesajı	-	-	-	-
Grup fotoğraf paylaşımı	+	+	+	+
Görüntülü konuşma	+	+	-	+
Sesli Konuşma	+	+	-	+
Durum paylaşımı	+	+	+	+

6.2.3 Instagram

Instagram uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.8'de verilmiştir. Tablo incelendiğinde iOS cihazın Paraben, Oxygen, Axiom araçları ile alınan mantıksal imajlarından ve manuel analizden kullanıcı davranışlarından olan fotoğraf, video ve paylaşımlarına, yapılan yorum ve beğenilere, atılan mesajlara erişilememiştir. Paraben ve Axiom araçları iOS cihazın mantıksal imajından Instagram verilerine erişemediği gözlemlenmiştir. Oxygen aracı hesap bilgilerine, takip edilen kişi bilgilerine, arama geçmişine, etiket bilgilerine erişim sağlamıştır. Bu bilgilere manuel analizde de erişilebilmiştir.

Tablo 6.10. iOS Instagram uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Paraben Mantıksal	Axiom Mantıksal	Manuel
Uygulamaya Ait Veriler				
Hesap bilgileri	+	-	-	+
Takip edilen kişi bilgileri	+	-	-	+
Mesajlar	-	-	-	-
Arama geçmişi	+	-	-	+
Kullanıcı Davranışları				
Paylaşım	-	-	-	-
Durum	-	-	-	-
Beğeni	-	-	-	-
Yorum	-	-	-	-
Mesaj	-	-	-	-
Takip	+	-	-	-
Etiket	+	-	-	+

6.2.4 Twitter

Twitter uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.11'da verilmiştir. Tablo incelendiğinde iOS cihazın Paraben, Oxygen, Axiom araçları ile alınan mantıksal imajlarından Paraben ve Axiom araçları uygulama verilerine erişememiştir. Hesap bilgileri, arama geçmişi, direk mesaj bilgilerine hem Oxygen aracı hem de manuel analiz ile erişilirken, Twitter arkadaşları silinen mesajlar ve engellenen arkadaşlara yalnızca manuel analiz ile erişilebilmektedir.

Tablo 6.11. iOS Twitter uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Paraben Mantıksal	Axiom Mantıksal	Manuel
Uygulamaya Ait Veriler				
Hesap bilgileri	+	-	-	+
Twitter arkadaşları	-	-	-	+
Takip edilenler	-	-	-	-
Takipçiler	-	-	-	-
Tweetler	-	-	-	-
Arama geçmişi	+	-	-	+
Direk mesaj	+	-	-	+
Kullanıcı Davranışları				
Tweet	-	-	-	-
Yanıt	-	-	-	-
Retweet	-	-	-	-
Beğenmek	-	-	-	-
Mesaj(DM)	+	-	-	+
Silinen mesaj	-	-	-	+
Hesap Takip	-	-	-	-
Takipten çıkarılan	-	-	-	-
Engellenen	-	-	-	+

6.2.5 BiP Messenger

BiP Messenger uygulamasına ait uygulama verileri ve tespit edilebilen kullanıcı davranışları Tablo 6.10'da verilmiştir. Tablo incelendiğinde iOS cihazın Paraben, Oxygen, Axiom araçları ile alınan mantıksal imajlarından hiçbirinin uygulama verilerini ayıklamadığı görülmüştür. Uygulamaya ilişkin kullanıcı davranışlarına yalnızca manuel analiz sırasında erişilebilmiştir. Uygulamanın mesaj bilgilerine, paylaşılan fotoğraf ve konum bilgilerine, grup mesajlarına sesli ve görüntülü aramalarına erişilebilmiştir.

Tablo 6.12. iOS BiP Messenger uygulama verileri ve kullanıcı davranışları

	Oxygen Mantıksal	Paraben Mantıksal	Axiom Mantıksal	Manuel
Kullanıcı Davranışları				
Mesajlaşma	-	-	-	+
Silinmiş mesaj	-	-	-	*
Fotoğraf paylaşımı	-	-	-	+
Konum paylaşımı	-	-	-	+
Grup mesajı	-	-	-	+
Silinmiş grup mesajı	-	-	-	-
Arkadaş engelleme	-	-	-	-
Zamanlı mesaj paylaşımı	-	-	-	-
Zamanlı konum paylaşımı	-	-	-	-
Sesli arama	-	-	-	+
Görüntülü arama	-	-	-	+

7. SONUÇLAR

Bu tez çalışmasında mobil cihazlarda sosyal medya uygulamalarının analizi gerçekleştirilmiştir. Mobil işletim sistemi olarak günümüzde en fazla kullanılan ilk iki işletim sistemi iOS ve Android seçilmiştir. Sosyal medya uygulamalarının analizi sırasında mobil cihazların adli incelenmesinde izlenen yollar gösterilmiştir. İncelenmek üzere biri Android 6.0.1 işletim sistemine sahip Sony Xperia Z2 model ve diğeri iOS 11.3.1 işletim sistemine sahip iPhone 6s model iki mobil cihaz seçilmiştir. Bu cihazların seçilmesinin nedeni günümüzde yaygın olarak kullanılan çok eski olmamakla birlikte en son sürüm de olmayan modeller olmasıdır. Bu sayede çok yeni ve çok eski modellerde ortaya çıkabilen uyumsuzluk sorunlarından kaçınılmıştır. Mobil cihazlar ne kadar özellik olarak birbirine benzese de işletim sistemi ve veri kayıt tipi olarak büyük farklılıklara sahiptir. Bu yüzden her iki cihazın incelemesi de ayrı ayrı ve dikkatle gerçekleştirilmiştir.

Yapılan çalışmalarda hem Android hem de iOS cihaz için Oxygen Forensic, Paraben ve Magnet AXIOM adli bilişim yazılımları ve manuel veri çıkarım yöntemleri ile ayrı ayrı analiz gerçekleştirilmiştir. Cihazların incelenmesi sonucu kullanıcıların sosyal medya programlarından gerçekleştirdiği davranışlara ulaşılması amaçlanmıştır. Elde edilen sonuçlar hem işletim sistemleri açısından hem de yazılımların verileri yorumlaması açısından karşılaştırmalı olarak incelenmiştir. Yazılımlar tarafından yorumlanamayan verilerin ise elle çıkarılması amaçlanmıştır.

Yapılan incelemelerde Android işletim sistemine sahip cihazın mantıksal imajlarından uygulamalar hakkında çıkarılabilen verilerin uygulamanın tuttuğu medya dosyalarından öteye geçmediği bazen onların bile kullanıcı erişimine sunulmadığı yani verilerin çok yetersiz olduğu gözlemlenmiştir. iOS cihazın mantıksal imajından ise mesajlaşma içerikleri, kişi listeleri, uygulama bilgileri gibi değerli verilerin bir kısmına ulaşılabildiği görülmüştür. Fiziksel imajın alınmasının mümkün olduğu Android cihazın fiziksel imajlarından uygulama ile ilgili tüm dosyalara erişilebilmektedir. Fiziksel imaj incelendiğinde uygulamaların silinmiş verilerin kurtarılabilir durumda olanları da görüntülenebilir. Bu imajların analizleri, araçlar ile gerçekleştirildiğinde çıkarılabilen verilerin araçlar arasında değişken olduğu görülmüştür. Dosya sisteminden çıkarılan uygulama dosyalarının içeriği manuel olarak incelendiğinde ise araçların çıkarabildiği verilerden daha çok veriye ulaşılabildiği, kullanıcı davranışı olarak silinmiş olan verilerin de bir kısmına erişilebildiği görülmüştür.

İncelemede kullanılan yöntemler karşılaştırıldığında uygulamadan çıkarımı yapılan veri çeşidine göre birbirine olan üstünlükleri değişmektedir.

Android cihazın mantıksal imajından çıkarılan dosyalar Oxygen aracında kullanıcısına uygulama başlığı altında sunmaktayken Paraben bunu kullanıcının kendi çabasına bırakmıştır. Android cihazının fiziksel imajları incelendiğinde üç aracın da uygulama verilerine erişebildiği görülmüştür. Aracın bu verileri ayıklayarak uygulama başlığı altında kullanıcıya sunma yeteneğine bakılırsa, Facebook, WhatsApp, Instagram, Twitter uygulamalarının verilerini Oxygen ve Axiom sunabilmekte iken Paraben aracı bunlardan Twitter verilerini ayıklayamamaktadır.

iOS cihazının mantıksal imajı araçlar tarafından incelendiğinde ise, Oxygen yazılımı Facebook, WhatsApp, Instagram ve Twitter verilerinin bir kısmını ayıklarken, Axiom Facebook, WhatsApp verilerini ayıklamakta, Paraben sadece WhatsApp Messenger'ın verilerini ayıklayarak kullanıcıya sunmaktadır. Android ve iOS imajlarının tümünde BiP Messenger uygulamasının hiç bir araç tarafından ayıklanarak uygulama kategorisinden kullanıcıya sunulmamıştır.

KAYNAKLAR

[1] **Nelson, B., Phillips, A., & Steuart, C.** (2014). Guide to computer forensics and investigations: Cengage Learning.

[2] **Bommisetty, S., Tamma, R., & Mahalik, H.** (2014). Practical mobile forensics: Packt Publishing Ltd.

[3] **Ayers, R., Jansen, W., & Brothers, S.** (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, 1(1), 85.

[4] https://wearesocial.com/blog/2018/01/global-digital-report-2018 (Son Erişim Tarihi: 22.04.2018)

[5] **Casey, E.** (2011). Digital evidence and computer crime: Forensic science, computers, and the internet: Academic press.

[6] **Lohiya, R., John, P., & Shah, P.** (2015). Survey on mobile forensics. International Journal of Computer Applications, 118(16).

[7] **Reith, M., Carr, C., & Gunsch, G.** 2002. An examination of digital forensic models International Journal of Digital Evidence: Fall.

[8] **Çakmak, Y.** (2015). Social media forensics on mobile devices. İstanbul Bilgi Üniversitesi.

[9] **Quick, D., & Choo, K.-K. R.** (2017). Pervasive social networking forensics: intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications, 86, 24-33.

[10] **EMEKCİ, A., KUĞU, E., & TEMİZTÜRK, M.** (2016). Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim. ULUSLARARASI BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ DERGİSİ, 2(1).

[11] **Palmer, G.** (2001). A road map for digital forensic research. Paper presented at the First Digital Forensic Research Workshop, Utica, New York.

[12] **Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V.** (2013). A critical review of 7 years of Mobile Device Forensics. Digital Investigation, 10(4), 323-349.

[13] **Murphy, C. A.** (2009). Developing process for mobile device forensics. SANS Digital Forensics and Incident Response.

[14] https://digital-forensics.sans.org/media/DFIR-Smartphone-Forensics-Poster.pdf, 13 Nisan 2018.

[15] **Jansen, W., & Ayers, R.** (2007). Guidelines on cell phone forensics. NIST Special Publication, 800(101), 800-101.

[16] **Lin, I.-L., Chao, H.-C., & Peng, S.-H.** (2011). Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. Paper presented at the Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on.

[17] **Sadiq, M., Iqbal, M. S., Sajad, M., Naveed, K., & Malip, A.** (2016). Mobile devices forensics investigation: process models and comparison. Theoretical & Applied Science(1), 164-168.

[18] **Ali, A., Razak, S. A., Othman, S. H., Mohammed, A., & Saeed, F.** (2017). A metamodel for mobile forensics investigation domain. PloS one, 12(4), e0176223.

[19] **Hassan, M., & Pantaleon, L.** (2017). An investigation into the impact of rooting android device on user data integrity. Paper presented at the Emerging Security Technologies (EST), 2017 Seventh International Conference on.

[20] **Wu, S., Zhang, Y., Wang, X., Xiong, X., & Du, L.** (2017). Forensic analysis of WeChat on Android smartphones. Digital Investigation, 21, 3-10.

[21] **Ovens, K. M., & Morison, G.** (2016). Forensic analysis of kik messenger on ios devices. Digital Investigation, 17, 40-52.
[22] **Gregorio, J., Gardel, A., & Alarcos, B.** (2017). Forensic analysis of telegram messenger for windows phone. Digital Investigation, 22, 88-106.
[23] **Anglano, C.** (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201-213.
[24] **Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R.** (2016). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Australian journal of forensic sciences, 48(4), 469-488.
[25] **Martini, B., & Choo, K.-K. R.** (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80.
[26] **Yusoff, M. N., Dehghantanha, A., & Mahmod, R.** (2017). Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 41-62): Elsevier.
[27] **Cahyani, N. D. W., Ab Rahman, N. H., Glisson, W. B., & Choo, K.-K. R.** (2017). The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. Mobile Networks and Applications, 22(2), 240-254.
[28] **Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R.** (2016). Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Australian journal of forensic sciences, 48(6), 615-642.
[29] **Azfar, A., Choo, K. K. R., & Liu, L.** (2017). Forensic taxonomy of Android social apps. Journal of forensic sciences, 62(2), 435-456.
[30] **Ogazi-Onyemaechi, B. C., Dehghantanha, A., & Choo, K.-K.** (2017). Performance of android forensics data recovery tools Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 91-110): Elsevier.
[31] **Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F.** (2015). Network and device forensic analysis of android social-messaging applications. Digital Investigation, 14, S77-S84.
[32] **Aquila, I., Sacco, M., Gratteri, S., Sirianni, M., De Fazio, P., & Ricci, P.** (2017). The "Social-Mobile Autopsy": The Evolution of Psychological Autopsy with New Technologies in Forensic Investigations on Suicide. Legal Medicine.
[33] https://www.alexa.com/topsites, The top 500 sites on the web, 22 Nisan 2018.
[34] https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ , Most popular mobile messaging apps worldwide, 25 Nisan 2018.
[35] https://www.whatsapp.com/, 25 Nisan 2018.
[36] **Rosen A.**, Tweeting Made Easier, http://instagram.tumblr.com/post/8755963247/introducing-hashtags-on-instagram, 25 Nisan 2018.
[37] https://blog.twitter.com/official/en_us/topics/product/2017/tweetingmadeeasier.html, 26 Nisan 2018.
[38] https://www.turkcell.com.tr/servisler/BiP, 26.Nisan 2018.
[39] **Al Mutawa, N., Baggili, I., & Marrington, A.** (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24-S33.

[40] **Cohen, M., Garfinkel, S., & Schatz, B.** (2009). Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Digital Investigation, 6, S57-S68.

[41] **Kausar, F., & Alyahya, T. N.** (2016). Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones. International Journal of Computer Science and Network Security (IJCSNS), 16(11), 38.

[42] **Chang, Y.-T., Teng, K.-C., Tso, Y.-C., & Wang, S.-J.** (2015). Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence. Journal of Computers, 26(2).

[43] **AKBAL, E., DOĞAN, Ş., & BALOĞLU, İ.** Android İşletim Sisteminde WhatsApp Uygulamasının Adli Bilişim Açısından İncelenmesi. Bilişim Teknolojileri Dergisi, 11(2), 147-156.

ÖZGEÇMİŞ

Fatma GÜNEŞ ERİŞ

Teknoloji Fakültesi

Adli Bilişim Mühendisliği Bölümü

GSM: +90 531 0111013

E- mail: f.gunes@firat.edu.tr

Eğitim

YÜKSEK LİSANS **(2015–) Fırat Üniversitesi** /Elazığ, Türkiye

Fırat Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı.

LİSANS **(2008–2013) Kocaeli Üniversitesi** /Kocaeli, Türkiye

Kocaeli Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü