Karaelmas Fen ve Mühendislik Dergisi
Dergi web sayfası: http://fbd.beun.edu.tr

Araştırma Makalesi
Geliş tarihi / Received : 15.12.2016
Kabul tarihi / Accepted : 20.01.2017

SIM Kartların Dijital Delil Olarak İncelenmesi ve Analizi

Analysis and Investigation of SIM Cards as Digital Evidence

Erhan Akbal, Şengül Doğan

Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği, Elazığ, Türkiye

Öz

Günümüz mobil cihaz teknolojisinin kullanılabilmesi için sim kartlar vazgeçilmez öğelerin başında gelir. Kullanıcının kimliğinin belirlenmesi ve iletişim ağına dâhil olabilmesi için sim kart kullanılmak zorundadır. Mobil iletişimin hızlı artışı sim kartların Adli Bilişim açısından da önemini arttırmıştır. Adli bilişim, delillerin belirli yöntem ve metotlarla incelenmesini tanımlamaktadır. Bu nedenle sim kartların nasıl incelenmesi gerektiği ve yapısının anlaşılması gerekmektedir. Sim kartlar belirli üreticiler tarafından üretilmekte ve mobil servis sağlayıcılar tarafından kullanılmaktadır. Bir sim kartın belirli bir mimari yapısı, dosya sistemi, fiziksel özellikleri ve bileşenleri bulunmaktadır. Sim kartların incelenmesinde belirli donanım ve yazılım araçlarından faydalanılmaktadır. Bu araçlar kullanılırken sim kartlardan elde edilebilecek verilerin bilinmesi gerekir. Bu çalışmada, Sim kartların yapısal özellikleri ortaya konularak Adli bilişim inceleme metodolojisi gösterilmiştir. Ayrıca kullanılan araçlar ile elde edilebilecek veriler karşılaştırmalı olarak ortaya konmuştur. Örnek bir uygulama ile doğrudan sim kart üzerinden analiz ile mobil cihaza takılı sim kartın mobil cihaz üzerinden elde edilen verileri gösterilmiştir. Eski nesil mobil cihazlar genellikle işlemleri sim kart bellekleri üzerinden gerçekleştirirken yeni nesi mobil cihazlar telefon hafızalarını kullanmaktadır. Bu nedenle eski nesil cihazlarda kullanılan sim kartlardan mesaj, telefon defteri, arama kaydı gibi kişisel bilgilerle birlikte servis bilgileri elde edilebilirken, yeni nesil mobil cihazlardan sadece servis bilgileri elde edilebilmektedir. Diğer bilgiler telefon belleğinde tutulduğundan sim kart inceleme araçlarıyla bu verilere erişilememektedir. Bu tip verilere erişebilmek için mobil adli bilişim araçlarının kullanılması gerekmektedir. Fakat kullanıcı kimliğini belirleyen temel servis verilerine erişmek mümkündür.

Anahtar Kelimeler: Adli bilişim, Dijital delil, Sim kart, Sim kart incelemesi

Abstract

Sim card is one of the indispensable items that today's mobile device technology can be used. Sim cards must be used in order to determine the identity of the user and to be included in the communication network. The rapid rise of mobile communication has increased its importance of Sim Card in terms of digital forensics. Digital forensic is defined as the examination of evidence with specific methods and techniques. Therefore, it is necessary to understand the structures and examination techniques of the sim cards. Sim cards which has a specific architectural structure, file system, physical properties and components are produced by specific manufacturers and are used by mobile service providers. Specific hardware and software tools are used for the examination of sim cards. When these tools are used, the data that can be obtained from sim cards must be known. In this study, the structural features of sim cards are presented and forensic examination methodology is shown. At the same time, data that can be obtained from mobile devices with digital forensics tools are presented comparatively. With a sample application, data obtained directly from sim card and sim card mounted mobile device are demonstrated. A new-generation mobile device uses phone memories while an old-generation mobile device utilizes usually memories of sim card. Therefore, personal information such as messages, phone book, call logs etc. and service information can be obtained from sim card used in old-generation mobile devices while service information can be provided from sim card used in new-generation mobile devices. This data cannot be accessed with sim card investigation tools since other information are stored in the phone memory. Mobile digital forensics tools should be used to access such data. But it is possible to access the basic services data that determine the user identity.

Keywords: Digital forensics, Digital evidence, SIM card, Sim card review

*Sorumlu yazarın e-posta adresi: erhanakbal@firat.edu.tr

Erhan Akbal orcid.org/0000-0002-5257-7560
Sengul Dogan orcid.org/0000-0001-9677-5684

1. Giriş

Mobil cihazlar son yıllarda iletişimin vazgeçilmezi haline gelmiştir. Dünya üzerinde gerçekleştirilen telefon görüşmelerinin büyük bir çoğunluğu mobil cihazlar üzerinden gerçekleştirilmektedir. ITU'nun (International Telecommunication Union) 2015 yılında yayınladığı raporda mobil operatör kullanıcılarının son 15 yıl içerisinde büyük bir oranda arttığını göstermektedir (Fact I.C.T 2015).

Sim (Subscriber Identity Module) kartlar mobil cihazlar üzerinden iletişim kurmak için gerekli olan öğelerin temelidir. Kullanıcıların internet erişimi, sms gönderimi ya da sesli görüşme yapabilmeleri sahip oldukları sim kartlarla sağlanmaktadır (Scourias 1995, Kadhiwal ve Zulfiquar 2007). Sim kartlar kullanıcıların mobil servis sağlayıcı üzerindeki kimlik doğrulama ve kullanıcı tanımlamayla ilgili verileri depolar. Bu veriler IMSI (International Mobile Subscriber Identity) uluslararası kimlik numarası, ICCID (Integrated Circuit Card ID) kart numarası, LAI (Local Area Identity) alan kodu, Ki (Authentication Key) doğrulama anahtarı, SMSC (Short Message Service Center) kısa mesaj servis numarası ve SPN (Service Providers Number) servis sağlayıcı isim bilgileridir. Ayrıca kullanıcıların yapmış oldukları arama kayıtları, sms içerikleri ve kullanıcının rehber bilgilerini de sim kartlar tarafından depolanabilmektedir. 16kbyte ile 512 kbyte arasında bir depolama alanına ve işlemleri gerçekleştirecek bir işlemciye sahiptir. Sim kart üzerinde bulunan algoritma sim karttaki tanımlayıcı numara ile servis sağlayıcı tarafında bulunan numaraları eşleştirerek iletişimi kurar (Rongyu vd. 2009, Kadhiwal ve Zulfiquar 2007).

İletişimin sim kartlar üzerinden gerçekleştirilmesi adli suçların aydınlatılmasında önemli bir delil olarak sim kartları karşımıza çıkarmaktadır. Günümüzde suç türüne göre ayırmaksızın adli makamlara yansıyan olayların büyük çoğunluğunda cep telefonları vb. mobil aygıtlar kullanılmaktadır. Bu nedenle cihaz kullanıcısının tespit edilmesi, arama kayıtlarının ortaya çıkarılması, sms geçmişinin incelenmesi bağlandığı servis sağlayıcılardaki tanımlamalar için kullanıcının belirlenmesi gibi birçok verinin elde edilebilmesi için sim kartları incelenmesi gerekmektedir (Walsh ve Brinker 2016, Hiremath vd. 2016).

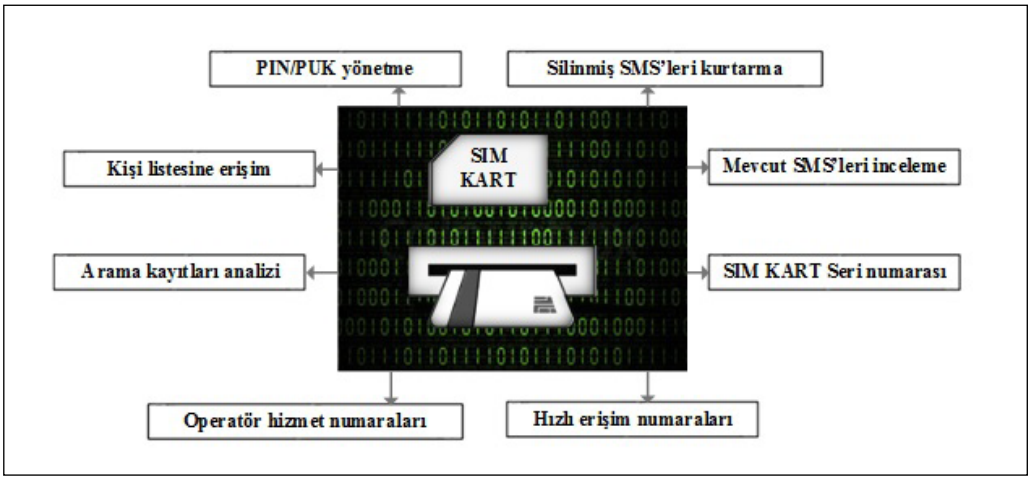
Dijital kaynaklar üzerinden işlenen suçları belirli yöntem ve metotlarla inceleyen bilim dalına Adli Bilişim denilmektedir. Adli bilişim incelemeleri suça konu aygıtın olay yerinden alınıp incelenmesi analizi ve raporlandırma süreçlerinin bütünüyle ilgilenir (Garfinkel 2010, Richard ve Roussev 2006, Gloe ve Böhme 2010, Reith vd. 2002). Mobil cihazlar üzerinden işlenen suç ve suçlunun belirlenmesi için sim kartların incelenmesi adli bilişim açısından büyük önem arz etmektedir (Scourias 1995, Willassen 2003). Bir sim karttan elde edilebilecek bilgiler Şekil 1'de gösterilmiştir (Casadei vd. 2006).

Bu çalışmada sim kartların yapısal özellikleri açıklanmıştır. Ayrıca adli bilişim uzmanlarının sim kartları ne şekilde incelemesi gerektiği ve ne tür bilgiler elde edilebileceği gösterilmiştir. Böylece bu alanda çalışacak uzmanlara yol gösterilmiş olacaktır.

2. Gereç ve Yöntem

2.1. SIM Kartlar

Sim kartlar küçük bir bilgisayar sistemi yapısındadır İşlemci, giriş çıkış birimleri ve bir bellek alanından oluşmaktadır. İçerisinde çeşitli güvenlik mekanizmaları barındıran bir işletim sistemine sahiptir. İletişim fonksiyonlarını gerçekleştirmek için mobil cihaz üzerinde bulunan arabirim



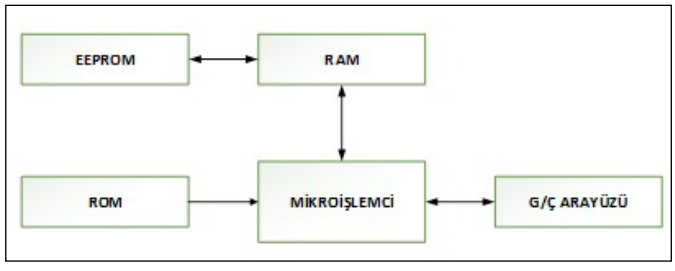
Şekil 1. Sim kart ile elde edilebilecek bilgiler.

bağlantı noktalarına bağlanmaları gerekmektedir. GSM 11.11, ISO 7816, 3GPP ve ETSI gibi standartlara uygun çalışması gerekmektedir. Servis sağlayıcılar üzerinden iletişim kurmak isteyen kullanıcıların mobil ağa bağlanmaları için gerekli güvenlik, kimliklendirme ve doğrulama süreçlerini gerçekleştirmede kullanılır (Mohamed vd 2016, Ok vd. 2016). Mobil servis sağlayıcılara kayıtlı kullanıcıların kontrolünü sağlarken kullanılır. İletişim sürecinde verilerin güvenliğini sağlamak için Ki (Authentication Key) gibi bir şifreleme tekniği kullanır. Ayrıca kullanıcıların ihtiyacı olan kişi bilgileri, sms kayıtları, en son aranan numaralar, arama geçmişi bilgileri sim kartın belleği ölçeğinde saklanabilmektedir. Mobil cihazların hafızalarının gelişmesinden sonra sim kartların kapasitelerinin düşük olmasından dolayı fazla bilgi saklanmamaktadır (Ok vd. 2016). Günümüzde sim kartlar 4 farklı biçimde karşımıza çıkabilmektedir. Standart sim kartlar, mini sim kartlar, micro sim kartlar ve nano sim kart boyutunda olabilmektedir. Tüm türlerin mimarisi aynıdır. Sadece boyutları farklılık göstermektedir (Willassen 2005, Swenson 2005).

2.1.1. Sim Kart Mimari Yapısı

Sim kartlar fiziksel yapılarına ve destekledikleri teknolojilere değişmektedir. Fiziksel yapılarına göre Tam boy sim, Mini Sim, Mikro Sim, Nano Sim olmak üzere 4 türü bulunmaktadır. Destekledikleri teknolojilere göre 2g, 3g ve LTE destekli olarak ayrılmaktadır (Mayes ve Markantonakis 2007, Sesia vd. 2011). Tüm sim kartların mimari yapısı içerisinde aynı arabirimler bulunmaktadır. Mimari yapıda ROM, EEPROM, Mikro işlemci, Ram ve Giriş Çıkış arayüzleri bulunmaktadır. Mimari yapısı Şekil 2'de gösterilmiştir.

Sim kartların güvenlik problemi oluşturmaması için iç mimari yapısı sim kart üretici firmalar tarafından koruma altında tutulmaktadır. Fakat sim kart ile takıldığı cihaz arasında iletişimin nasıl kurulacağı ile ilgili standartlar tanımlanmıştır. Sim kartlar içerisinde kullanıcı ile ilgili kalıcı bilgiler EEPROM'da tutulmaktadır. Bu alan sim kartın türüne göre 16kb ile 512 kb boyutunda olabilmektedir.



Şekil 2. Sim kart mimari yapısı.

Sim kartlarda içerisindeki tüm verilere erişmek mümkün değildir. Pin, puk kodları, kimlik doğrulama anahtarı gibi veriler yazılımsal ya da donanımsal olarak erişilip okunamaz bilgilerdir. Belirli alanlardaki verilere erişim sağlamak için Pin kodu bilgisine ihtiyaç vardır. Pin kodu girişi sim kart üzerinde yönetici yetkileri tanımlanmasını sağlamaktadır. Bu görevleri mikroişlemci gerçekleştirmektedir. Sim kartın takıldığı cihaz ile bağlantı sağlayabilmesini ve çeşitli giriş çıkış işlemlerini yapabilmesi için giriş/çıkış arayüzü bulunmaktadır. Sim kartlar genellikle 6 ya da 8 pinlidir ve sadece bir pini giriş/çıkış için kullanmaktadır. Bu bağlantıda seri bir G/Ç işlemi gerçekleştirebilmektedir. Takıldığı cihaz üzerindeki tanımlı bir komut kümesi ile sim kart ile iletişim kurabilmektedir. Sim kart ile takıldığı cihaz arasındaki maksimum veri aktarım hızı 20 Kb/sn geçmemektedir. Sim kartta bulunan bağlantı arayüzleri Çizelge 1'de verilmiştir (Srivastava ve Vatsal 2016, Casadei vd. 2006).

Çizelge 1. Sim kart bağlantı arayüzleri.

Bağlantı ismi	Bağlantı Görevi
VCC	Besleme Gerilimi
RST	Kartın Reset
CLK	Kartının Frekans Çevrimi
NC	Bağlantısızlık
GND	Güç/Sinyal
VPP	Programlama Gerilimi
IO	Giriş/Çıkış
NC	Bağlantısızlık

2.1.2. Sim Kart Veri Yapısı

Sim kartlar içerisinde çeşitli bilgileri saklayabilecek yapıdadır. Mesaj verileri, kişi listesi, en son arama yapılan numaralar ve telefon numaraları gibi kişisel verileri depolar. Sim kartlar depolama alanlarının büyük bir kısmını mesaj saklamak için kullanır. 256 adet SMS'e kadar metin mesajı saklanabilmektedir. Saklama alanı dolmadığı sürece veriler birbirinin üzerine yazılmaz ve buda mesajların kurtarılabileceği anlamına gelmektedir. Diğer büyük saklama alanı kişi listelerini saklamak için kullanılır. Maksimum 255 adet kişi bilgisi saklanabilir. Kişi bilgileri silindiğinde o bilginin bulunduğu bellek ofset değerini sıfırlayacağından kurtarma ile kişi bilgisi elde etmek mümkün değildir. Kişi listesi için sadece isim ve telefon numarası alanı bulunmaktadır. Bir kişi için en fazla bir numara saklayabilmektedir. En son aranan maksimum 20 adet numara ile ilgili veri sim kartta saklanabilmektedir. Sim kart aranan yada cevapsız arama ile ilgili herhangi bir kayıt saklayacak alana sahip değildir. Bu nedenle sadece arama

yapılan kayıtlara ulaşılabilmektedir (Mayes ve Markantonakis 2007, Casadei vd. 2006). Kişisel kullanım ile ilgili verileri saklamanın yanında, iletişimin sağlanması için gerekli bilgiler de sim kart içinde saklanmaktadır. Adli bilişim açısından sim kart üzerinden elde edilebilecek tüm bilgiler büyük önem taşımaktadır. Günümüzde kullanılan sim kartlarda veri depolama işlemi çok fazla yapılmamaktadır. Akıllı cihazların gelişmesiyle birlikte kullanıcılar arama, kişi listesi, mesaj gibi verilerini telefon hafızlarında saklamaktadır. Bu nedenle yeni nesil sim kartlardan bununla ilgili pek fazla veri elde etmek mümkün olmamaktadır Fakat iletişim için kullanılan verilerin elde edilmesi suçun aydınlatılması için önemlidir. Sim kartlar iletişimle ilgili Çizelge 2'de verilen temel bilgileri saklamaktadır (Jansen, ve Ayers 2006).

2.1.3. Sim Kart Dosya Yapısı

Sim kartlar içerisinde bir hiyerarşik dosya yapısı kullanmaktadır. Tüm verileri temel 3 dosya yapısı ile saklamaktadır. Bunlar Master File (MF), Dedicated File (DF) ve Elementary File (EF) dır. MF dosya sisteminin ana dizinidir ve içerisinde DF ve EF alt alanlarını bulundurur. DF, MF altında bulunur ve içerisinde temel (EF)-özel (DF) dosya dizinleri bulundurur. Temel klasör hizmetlerini sağlar. EF ise içerisinde çeşitli dosya türlerini, verinin bayt dizisini ve sabit boyutlu kayıt seti gibi verilerin tutulduğu öğelerdir. Dosya yapısı Şekil 3'de gösterilmiştir.

MF'nin altında GSM, DCS1800, Telecom gibi alt DF dizinleri bulunmaktadır. MF ve bu DF'ler için farklı EF yapıları tanımlanmıştır. GSM ve DCS1800 gibi dizinlerin altında temel ağ ile ilgili bilgileri 900,1800 Mhz GSM iletişimi ya da dijital hücresel sistemle ilgili tanımların olduğu EF dosyaları bulunmaktadır. Her ülkede kullanılan frekans bantlarına uygun yapıda EF'ler ilgili DF dizinlerinin altında bulunmaktadır. Böylece sim kartın iletişimle ilgili tüm standartları dosya sistemi içerisinde entegre edilmiş olmaktadır. Ayrıca sim kartların dosya yapılarının anlaşılması adli bilişim incelemeleri açısından da önem göstermektedir (Jansen ve Ayers 2006, Casadei vd. 2006).

2.2. SIM Kartların Adli Bilişim İncelemesi

Bilişim suçlarının incelenmesinde Sim kartlar birçok suçun aydınlatılması için kullanılmaktadır. Soygun, yaralama, gasp, cinsel istismar, cinayet, internet dolandırıcılığı, uyuşturucu satışı ve kullanımı, sosyal mühendislik gibi birçok suçta cep telefonları yoğun bir şekilde kullanılmaktadır. Suçlunun

Çizelge 2. Sim kart iletişim kodları.

Kısaltmalar	İngilizce Karşılıkları	Türkçe Karşılıkları
IMSI No	International Mobile Subscriber Identity	Uluslararası Abone Kimlik Numarası
ICCID No	Integrated Circuit Card Identifier	Entegre Devre Kart Tanımlayıcı Numarası
MNC	Mobil Network Code	Servis Sağlayıcının Ülke İçindeki Kodu
MCC	Mobil Calling Code	Mobil Arama Ülke Kodu
MSIN	Mobil Subscriber Identification Number	10 haneli Mobil Ağ Tanımlayıcı Numarası
MSISDN	Mobil Subscriber International ISDN Number	Mobil Cihazda kullanılacak telefon numarası, Ülke Kodu, Lokasyon kodu ve tanımlayıcı numaradan oluşur.
ADN	Abbreviated Dialling Numbers	Kısaltılmış Arama Numaraları
LND	Last Numbers Dialled	Son Aranan Numaralar
SDNs	Service Dialling Number	Servis Arama Numaraları
SPN	Service Provider Name	Servis Sağlayıcı İsmi
PIN	Personal Identification Number	Kişisel Tanımlama Numarası
PUK	PIN Unblocking Key	PIN bloke kaldırma anahtarı
LP	Language Preference	Dil Özellikleri
SST	Sim Service Table	Sim karttaki kullanılan servis tablosu
ECC	Emergency Call Code	Acil Durum Arama numarası
RAI	Routing Area Identifier	Yönlendirme ile ilgili Ağ kodu
LOCI, LOCIGPRS	Location Information	Lokasyon bilgileri
RAC	Routing Area Code	Yönlendirme Alan Kodu
LAC	Location Area Code	Konum Alan Kodu

mobil cihazının kimliğinin belirlenmesi, telefon üzerinde yapılan en son görüşme bilgisi, görüşme zamanı, sms bilgileri gibi birçok veri sim kartların incelenmesinden elde edilebilmektedir. Bu nedenle dijital delil olarak gelen sim kartların doğru metot ve yöntemlerle incelenmesi gerekmektedir. İnceleme için lisanlı ya da açık kaynak kodlu yazılımlar kullanılmaktadır. Ayrıca sim kart ile bağlantı sağlanabilmesi için Sim kart okuyucu donanımlara ihtiyaç duyulmaktadır (Casadei vd. 2006, Anwar vd. 2016).

2.2.1. Sim Karttan Adli İnceleme Metodu

Sim kartlar incelenirken inceleme metodunun belirlenmesi gereklidir. Adli sim kart incelenmesinde genel 2 yöntem kullanılmaktadır. İlki doğrudan sim kart takılı olan mobil cihaz üzerinden inceleme, ikincisi ise mobil cihazdan sim kartı çıkarıp bir sim kart okuyucu aygıta sim kartı takarak incelemedir. İki yöntemde de bilgisayar üzerinden inceleme yazılımları kullanılması gerekmektedir. İnceleme süreci iki aşamadan oluşmaktadır. İlki hazırlık, ikinci ise veri edinme aşamasıdır. Hazırlık aşamasında sim kartın telefon üzerinden mi yoksa sim kart okuyucu üzerinde mi analiz edileceğine karar verilir. Sonrasında iki durum içinde uyulması gereken prosedürler bulunmaktadır. Uygulanacak adımlar Şekil 4'de gösterilmiştir (Jansen, ve Ayers 2006, Casadei vd. 2006).

Hazırlık aşaması tamamlandıktan sonra Veri Edinme aşamasına geçilir. Veri edinme aşamasında uygulanacak işlem adımları sırasıyla uygulanması gerekmektedir. Veri edinme işlem adımları da Şekil 4'de gösterilmiştir. Telefon ya da sim kart okuyucu üzerinden inceleme yapılırken en kritik durum sim kartın PIN kodunun bilinmesidir. PIN kodu bilinmeyen sim kartlardan kullanıcının verilerini elde etmek mümkün olmamaktadır. Sadece sim kartın temel bilgileri elde edilir. PIN kodu bulunamayan sim kartın operatörleriyle adli yollarla iletişime geçilerek PIN bilgisini öğrenmekte kullanılacak PUK bilgileri öğrenilebilmektedir (Scourias 1995, Jansen, ve Ayers 2006).

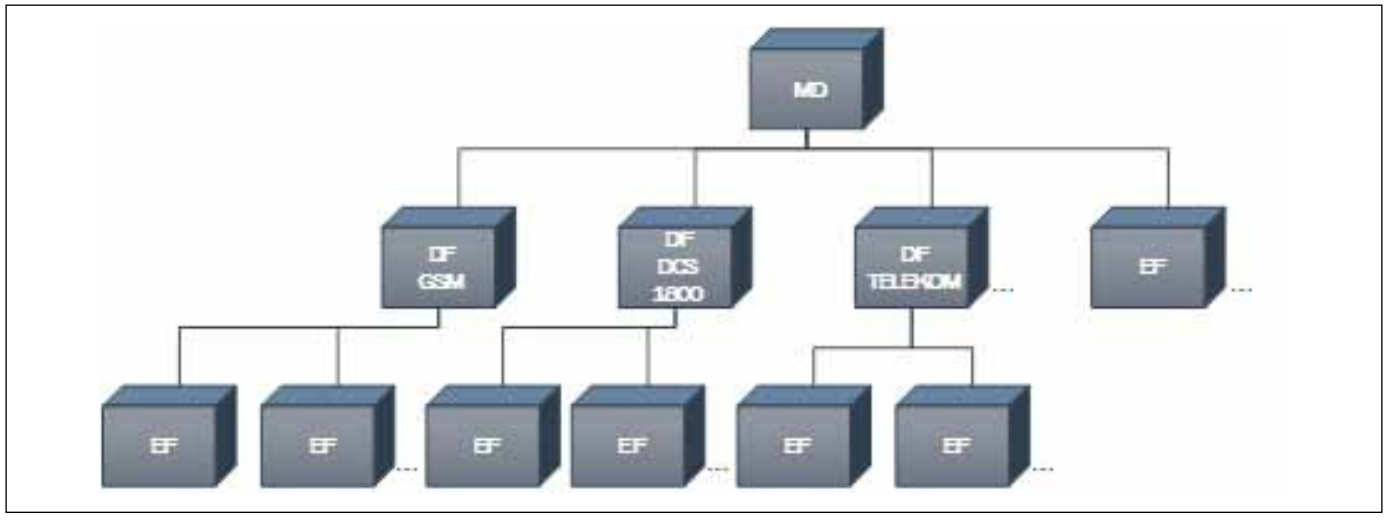
2.2.2. İnceleme Araçları

Sim kartlar incelenirken donanımsal ve yazılımsal araçlara ihtiyaç duyulur. Mobil aygıt üzerinden ya da sim kart okuyucu ile inceleme yapılacaksa her ikisi içinde inceleme yazılımlarına ihtiyaç duyulur. Bu amaçla geliştirilmiş birçok inceleme yazılımı bulunmaktadır. Bunlar Simcon, Oxygen, Mobiledit, Paraben gibi yazılımlardır. Donanımsal olarak sim kart okuyucu aygıtlara, farklı sim kart türlerinin dönüşümleri için kullanılacak dönüştürücülere ve mobil cihaz üzerinden inceleme yapılacaksa bağlantı kablosuna ihtiyaç duyulmaktadır. Bunlar Şekil 5'de gösterilmiştir.

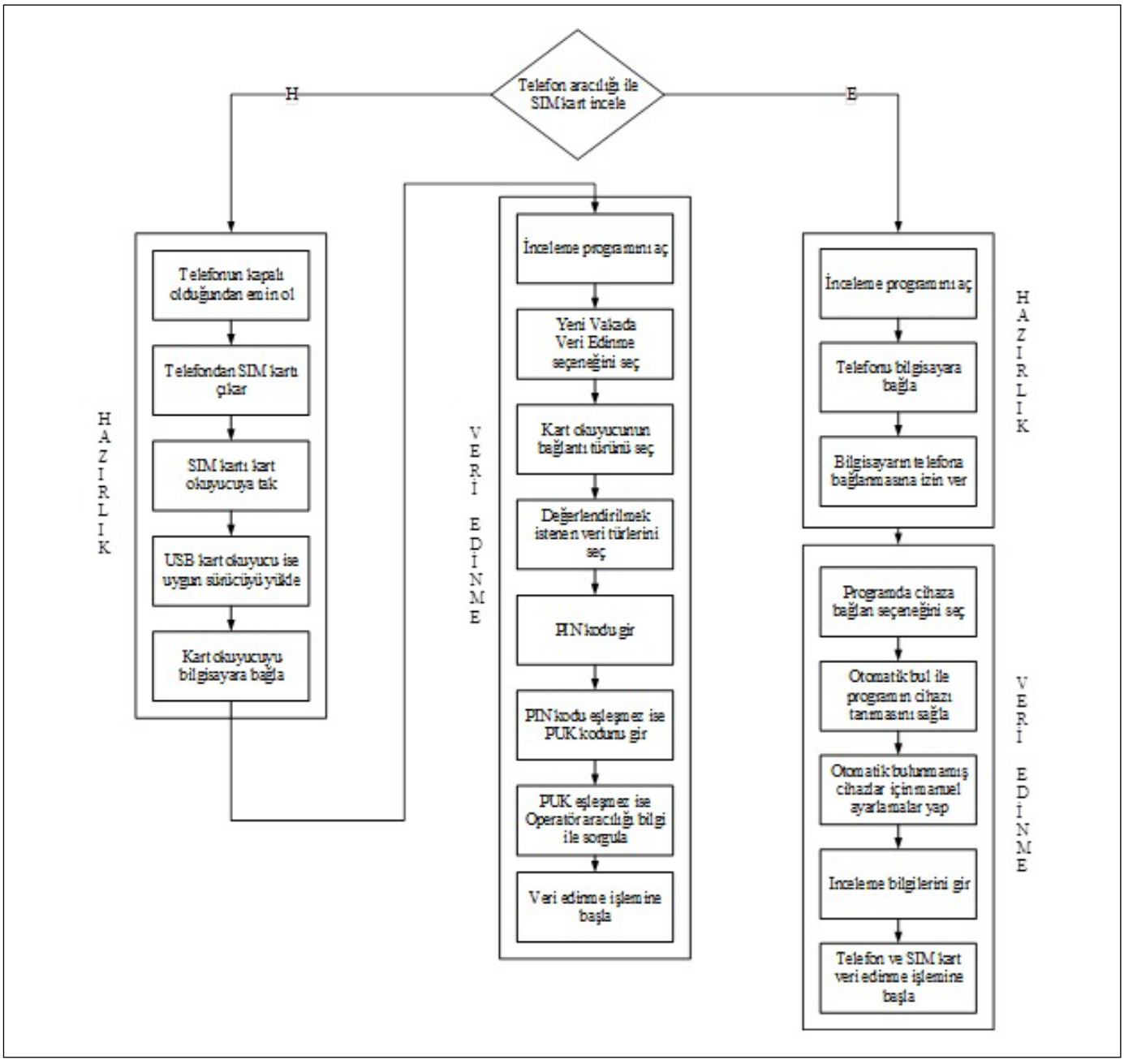
Sim kart inceleme yazılımları inceleme sürecinde belirli özellikleri sağlaması gerekmektedir. Aksi halde delilin doğruluğu ve bütünlüğü garanti edilemez. Bunun için yazılımlar içinde MD5, SHA-256 gibi hash hesaplama yöntemleri, silinen mesajların kurtarılması, temel sim bilgilerine erişilebilmesi, sim kartın klonlanması gibi işlemleri gerçekleştirmesi gerektir.

2.2.3. Sim Karttan Delil Olarak Elde Edilebilecek Veriler

Sim kartlardan delil olarak elde edilebilecek veriler dosya sistemi yapısı içerisinde bulunan dizinlerin altındaki dosyalarda saklanır. Delil olarak kullanılabilecek 4 temel veri kategorisi bulunmaktadır. Bunlar Servis bilgileri, Telefon defteri ve Arama bilgileri, mesajlar ve konum bilgisidir. Tüm



Şekil 3. Sim kart dosya yapısı.



Şekil 4. Sim kart inceleme işlem adımları.

Şekil 5. Sim kart okuyucu ve dönüştürücüler.

bilgiler dosya sistemi altındaki MF dizini altındaki EF'lerin içerisinden elde edilmektedir. Elde edilecek verilerin karşılıkları Şekil 6'da verilmiştir.

Servis bilgisi olarak ICCID, IMSI, MSISDN, SPN ve SDN numara bilgileri elde edilebilmektedir. Bu bilgiler doğrultusunda sim karta özel ve tek olan tanımlayıcı servis numaraları elde edilebilmektedir.

Telefon rehberi ve arama bilgileri eğer kullanıcı mobil aygıt üzerindeki yapılandırma ayarlarından sim kart kullan seçeneğini seçtiyse elde edilebilen verilerdir. Kullanıcının telefon rehber bilgilerini sim kart üzerinde depolaması gerekmektedir. EF dizini altında bulunan ADN ve LDN bilgileri ile kullanıcının kısaltılmış arama numaraları ile en son aranan numara bilgileri elde edilebilir. Suçlu mobil aygıtta sim kartı kullan seçeneği ile kullanım sağlıyorsa bu bilgiler adli bilişim açısından önemli verilerdir.

Sim kartlar kullanıcı tarafından seçildiği takdirde kapasitesiyle orantılı olarak SMS text dosyalarını saklayabilmektedir. Birçok mobil cihaz bu verileri cihaz hafızalarında saklar. Fakat eski nesil telefonların bu gibi bir özelliği bulunmadığından verileri sim kart hafızasında saklamaktadır. Tek mesajda 160 basit karakter içeriği saklar. Mesaj boyutu 160 karakteri aştığında mesaj bölünerek ikinci bir mesaj olarak saklanır. Adli incelemede mesaj bilgileri elde edilebilmektedir. Ayrıca silinmiş SMS'lerin kurtarılması da mümkündür.

Konum bilgisi sim kartlar üzerinden elde edilebilecek önemli verilerden biridir. Kullanıcı mobil servis sağlayıcının baz istasyonları ile konum bilgileri üzerinden iletişime geçer. Mobil aygıtlar baz istasyonlarından aldıkları sinyalleri izlerler ve iletişimi sürekli tutmaya göre yapılandırılmıştır. LOCI, LOCIGPRS, LAC, RAI ve RAC bilgileri EF dizini altında bulunmaktadır ve konumla ilgili verileri saklamaktadır. Suçun aydınlatılabilmesi için kullanıcının sim kartından elde edilecek veriler ile istenilen zaman diliminde sim karttaki konum bilgileri elde edilerek sim kartın en son nerede kullanıldığı gibi veriler elde edilebilir (Jansen ve Ayers 2006, Anwar vd. 2016).

Belirlenen ana başlıklar için adli bilişim alanında SIM kart ve Telefon incelemelerinde yaygın kullanılan programlar ve incelediği özellikler Çizelge 3'de verilmiştir.

Çizelge 3'de telefon ve SIM kart aracılığı ile elde edilecek bilgiler servis, konum, çağrı, mesaj ve telefon defteri bilgileri gruplandırılmıştır (Jansen ve Ayers 2006).

3. Bulgular ve Tartışma

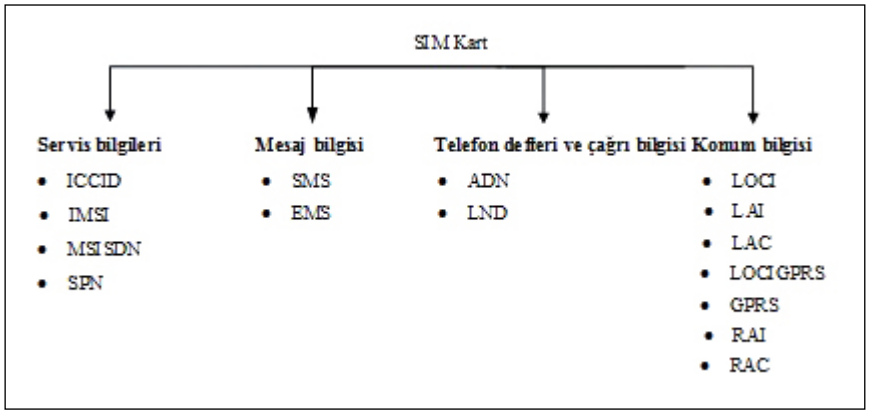
Sim kartta bulunan verilerin belirtildiği şekilde elde edilebildiği gerçekleştirilen uygulama ile gösterilmiştir.

3.1. Uygulama Ortamı

Uygulama ortamında ilk olarak mikro boyutunda bir sim kart, kart okuyucu ve SIMCon sim kart inceleme yazılımı kullanılmıştır. İkinci olarak Iphone 6 Plus cihaza takılı aynı sim kart Mobiledit yazılımı ile incelenmiş ve elde edilebilen veriler gösterilmiştir. Her iki uygulama içinde Intel I5 işlemcili, 4 GB RAM'li bilgisayar kullanılmıştır.

3.2. Yöntem

Şekil 3'de gösterilen sim kart inceleme adımları uygun iki farklı yöntem kullanılarak sim kart incelemesi yapılmıştır. Sim kartlardan adli delil olarak elde edilebilecek veriler kart okuyucu ve mobil aygıt üzerinden ne şekilde ve neler olduğu gösterilmiştir. Üzerinde 27 adet mesaj, 10 adet rehber bilgisi, 20 adet son arama kaydı bulunan bir sim kart kullanılarak bu verilerin incelemeden elde edilebilip edilemeyeceği, mesaj bilgilerinin silinmesinden sonra kurtarmanın olup olmadığı ve servisle ilgili verilerin neler olduğu Çizelge 4'de gösterilmiştir.



Şekil 6. Sim kart inceleme verileri.

Çizelge 3. Telefon ve sim kartların incelemesinde yaygın kullanılan programların karşılaştırması.

		Mobiledit	SIMCon	XRY Forensic	SIMIS	FCR	Paraben Device Seizure
Servis Bilgileri	**ICCID**	✓	✓	✓	✓	✓	✓
	IMSI	✓	✓	✓	✓	✓	✓
	MSISDN	✘	✓	✓	✓	✓	✓
	SPN	✘	✓	✘	✓	✘	✓
Mesaj Bilgileri	**SMS**	✓	✓	✓	✓	✓	✓
	EMS	✓	✓	✓	✓	✓	✓
Telefon Defteri ve Çağrı Bilgileri	**ADN**	✓	✓	✓	✓	✓	✓
	LND	✓	✓	✓	✓	✓	✓
Konum Bilgisi	**LOCI**	✘	✓	✓	✓	✓	✓
	LAI	✓	✓	✓	✓	✓	✓
	LAC	✘	✓	✓	✓	✓	✓
	LOCIGPRS	✘	✓	✘	✓	✘	✓
	RAI	✘	✓	✘	✓	✘	✓
	RAC	✘	✓	✘	✓	✘	✓
SIM ve Kart Okuyucu		✓	✓	✓	✓	✓	✓
SIM ve Telefon		✓	✘	✓	✘	✘	✘

Çizelge 4. İncelenen kartta Telefon ve SIM kart aracılığı ile elde edilen veriler.

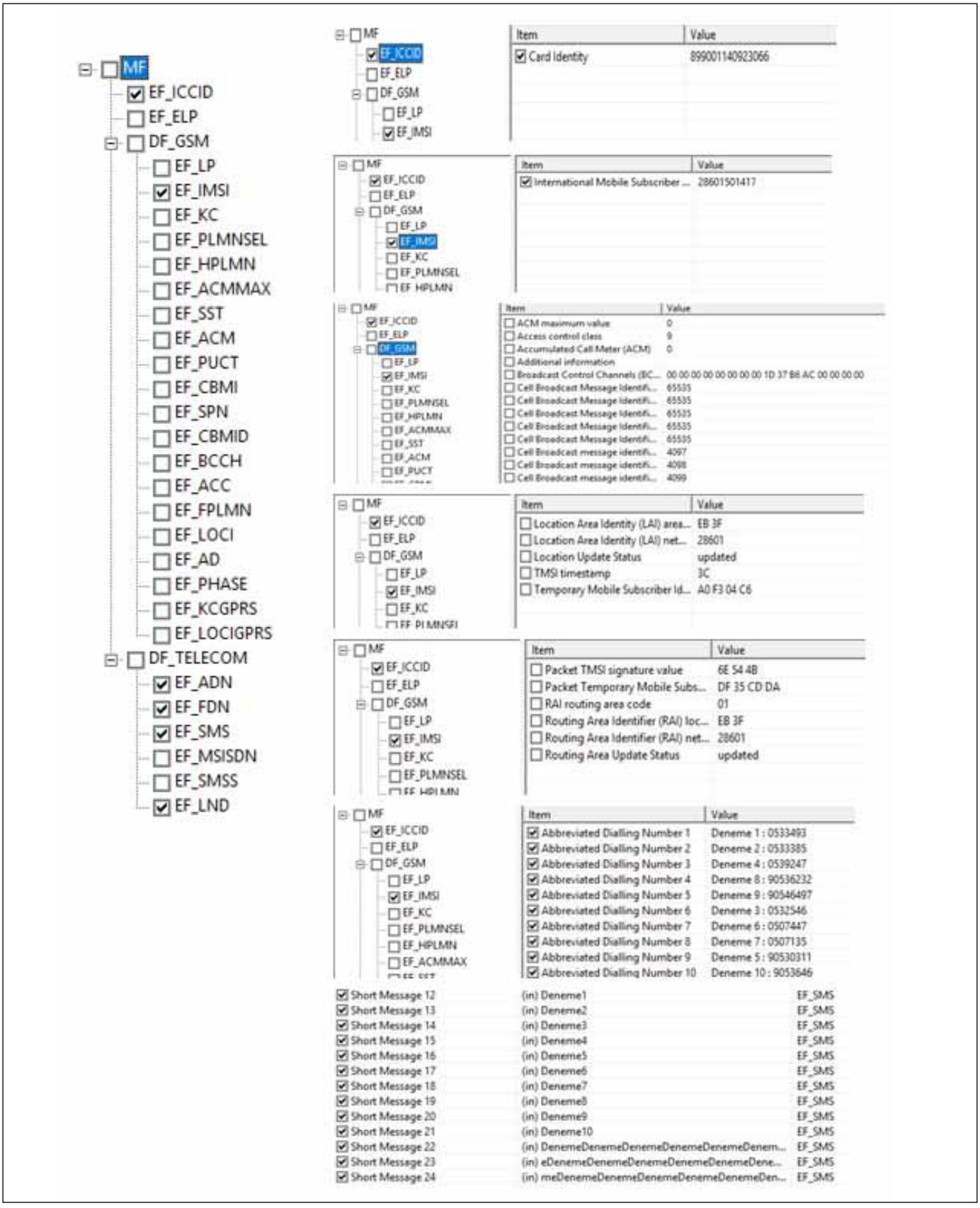
		Telefon ve SIM Kart	SIM Kart
Servis Bilgileri	**ICCID**	899001140923066****	899001140923066****
	IMSI	28601501417****	28601501417****
	MSISDN	✘	905333******
	SPN	✘	Turkcell
Mesaj Bilgileri	**SMS**	25 SMS	25 SMS
	EMS	2 EMS	2 EMS
Telefon Defteri ve Çağrı Bilgileri	**ADN**	10 kayıtlı kişi	10 kayıtlı kişi
	LND	20 numara	20 numara
Konum Bilgisi	**LOCI**	✘	✓
	LAI	82F610EB3F	A0 3F
	LAC	✘	28601
	LOCIGPRS	✘	✓
	RAI	✘	A0 3F, 28601
	RAC	✘	01

SIM kart ve kart okuyucu aracılığı ile elde edilen verilerin ekran çıktıları Şekil 7'de telefon ve sim kart aracılığı ile elde edilen verilerin ekran çıktıları ise Şekil 8'de verilmiştir.

Aynı zamanda sim kart ve telefon hafızası kullanımı ile elde edilecek veriler Çizelge 5'te sunulmuştur. Çizelge 5'de gösterildiği gibi telefon hafızasını kullanan mobil cihazlarda mesaj, telefon ve çağrı bilgilerine erişilememektedir.

3. Sonuç ve Öneriler

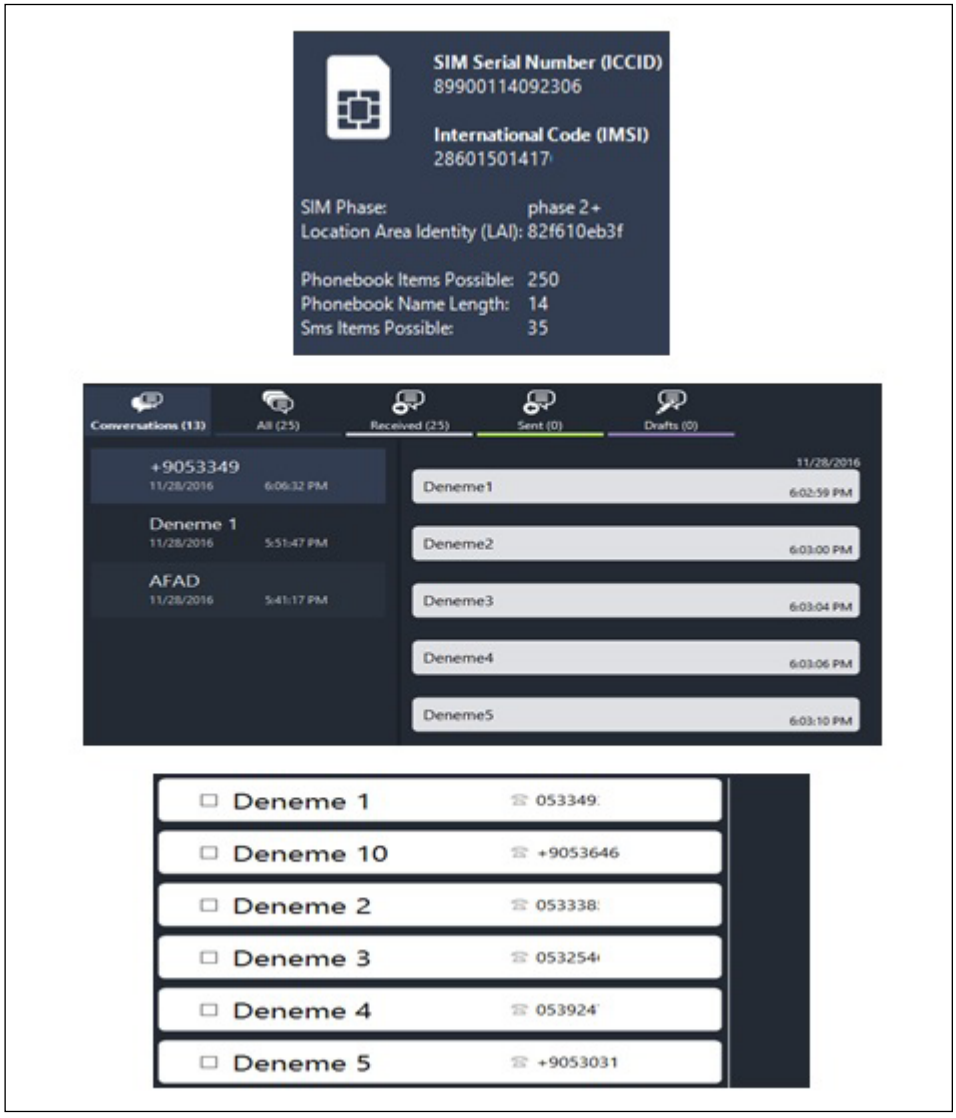
Mobil telefonlar insanların sürekli yanlarında taşıdıkları ve teknolojisini yakından takip ettiği cihazlardır. Bu cihazların amacına uygun çalışabilmesi için sim karta ihtiyaç duyarlar. En yaygın kullanılan cihazların başında gelen mobil telefonlar sim kartları ile beraber adli bilişim alanında işlenen suçların tespiti ve analizi için vakanın seyrini değiştirecek önemli bilgilere ulaşmamızı sağlayabilir. Bir sim kart analiz



Şekil 7. SIMCon programı ile elde edilen veriler.

Çizelge 5. Sim kart ve telefon hafızası kullanımından elde edilebilecek verilerin karşılaştırılması.

	SIM kart hafızasını kullanan mobil cihazlar	Telefon hafızasını kullanan mobil cihazlar
Servis Bilgileri	✓	✓
Mesaj Bilgileri	✓	✘
Telefon Defteri ve Çağrı Bilgileri	✓	✘
Konum Bilgisi	✓	✓



Şekil 8. Mobiledit programı ile elde edilen veriler.

edildiğinde adli bilişim alanında kullanılan çeşitli yazılımlar ile servis, mesaj, telefon defteri, çağrı ve konum bilgilerinin tamamına veya bir kısmına ulaşılabilmektedir. Elde dilecek veriler kullanılacak yazılım ve donanıma göre değişebilmektedir.

Bu çalışmada sim kartların mimari yapısı, dosya sistemi, fiziksel özellikleri ve bileşenleri ayrıntılı bir şekilde incelenerek adli bilişim alanında kullanılabilecek verilerin analizi yapılmıştır. Bu analizlerin yapılması için Mobiledit, SIMCon, XRY Forensic, SIMIS gibi yaygın kullanılan programlar belirtilerek elde edilecek veriler sunulmuştur. Aynı zamanda bir sim kartın doğrudan ve telefon aracılığı ile incelenmesi sonucu elde edilebilecek verilerin analizi SIMCon ve Mobiledit programları aracılığı ile analiz edilmiştir. Bu analiz için

işlemlerini sim kart bellekleri üzerinden gerçekleştiren eski nesil mobil cihaz kullanılmıştır. Çalışmada üzerinde 27 adet mesaj, 10 adet rehber bilgisi, 20 adet son arama kaydı bulunan bir sim kart kullanılmıştır. ICCID, IMSI, SMS, EMS, ADN, LND, LAI bilgilerine telefon-sim kart ve yalnızca sim kart incelemesinin her ikisi aracılığı ile de elde edildiği tespit edilmiştir. Yalnızca sim kart incelemesinde aynı zamanda MSISDN, SPN, LOCI, LAC, LOCIGPRS, RAI ve RAC bilgilerine de erişildiği gözlemlenmiştir.

4. Kaynaklar

Abdelazim, M. T., AbdelBaki, N., Shosha, AF. 2016. Digital Forensic Analysis of SIM Cards. *In Proc. of the Inter. Conf. on Sec. and Man.(SAM) (p. 244)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Anwar, N., Riadi, I., Luthfi, A. 2016. Forensic SIM card cloning using authentication algorithm. *Inter. J. Elect. Infor. Eng.*, 4(2): 71-81.

Casadei, F., Savoldi, A., Gubian, P. 2006. Forensics and SIM cards: an Overview. *Inter Journal of Dig. Evi.,* 5(1), 1-21.

Garfinkel, SL. 2010. Digital forensics research: The next 10 years. *Dig. Inves.,* 7: S64-S73.

Gloe, T., & Böhme, R. 2010. The dresden image database for benchmarking digital image forensics. *J. Dig. For. Pract.,* 3(2-4): 150-159.

Hiremath, R., Malle, M., Patil, P. 2016. Cellular Network Fraud & Security, Jamming Attack and Defenses. *Proc. Comp. Sci.*, 78:, 233-240.

Jansen, W., Ayers, R. 2006. Forensic software tools for cell phone subscriber identity modules. *In Proc. of the Conf. on Dig. For.,* Security and Law (p. 93). Association of Digital Forensics, Security and Law.

Kadhiwal, S., Zulfiquar, AUS. 2007. Analysis of mobile payment security measures and different standards. *Comp. Fraud & Sec.*, 2007(6), 12-16.

Mayes, K., Markantonakis, K. (Eds.). 2007. Smart cards, tokens, security and applications. *Sprin. Sci. & Busi. Media*.

Ok, K., Coskun, V., Yarman, SB., Cevikbas, C., Ozdenizci, B. 2016. SIMSec: A Key Exchange Protocol Between SIM Card and Service Provider. *Wir. Pers. Comm.*, 1-20.

Reith, M., Carr, C., Gunsch, G. 2002. An examination of digital forensic models. *Inter. J. Dig. Evi.,* 1(3): 1-12.

Richard III, GG., Roussev, V. 2006. Next-generation digital forensics. *Comm. ACM*, 49(2): 76-80.

Rongyu, H., Guolei, Z., Chaowen, C., Hui, X., Xi, Q., Zheng, Q. 2009. A PK-SIM card based end-to-end security framework for SMS. *Comp. Stan. Inter.,* 31(4): 629-641.

Sanou, B. 2015. The World in 2015: ICT facts and figures. International Telecommunications Union.

Scourias, J. 1995. Overview of the global system for mobile communications. *Univer. of Waterloo*, 4.

Sesia, S., Baker, M., Toufik, I. 2011. LTE-the UMTS long term evolution: from theory to practice. John Wiley & Sons.

Srivastava, A., Vatsal, P. 2016. Forensic Importance of SIM Cards as a Digital Evidence. *J. Foren. Res.*

Swenson, C., Manes, G., Shenoi, S. 2005. Imaging and analysis of GSM SIM cards. *In IFIP Inter. Conf. on Dig. Foren.* (pp. 205-216). Springer US.

Walsh, EI., Brinker, JK. 2016. Should participants be given a mobile phone, or use their own? Effects of novelty vs utility. *Tele. Infor.,* 33(1): 25-33.

Willassen, S. 2003. Forensics and the GSM mobile telephone system. *Inter. J. Dig. Evi.,* 2(1): 1-17.

Willassen, S. 2005. Forensic analysis of mobile phone internal memory. *In IFIP Inter. Conf. on Dig. Foren.* (pp. 191-204). Springer US.