

Uzmanlık Tezleri Serisi No: 164

REKABET KURUMU

MOBİL CİHAZLARDA ADLİ BİLİŞİM İNCELEMELERİ VE REKABET HUKUKUNDAKİ UYGULAMALARI

FATİH ÇİROĞLU

MOBİL CİHAZLARDA ADLİ BİLİŞİM İNCELEMELERİ ve REKABET HUKUKUNDAKİ UYGULAMALARI

FATİH ÇİROĞLU

Ağustos 2020

©Bu eserin tüm telif hakları
Rekabet Kurumuna aittir. 2020

Baskı, Ağustos 2020
Rekabet Kurumu-ANKARA

Bu kitapta öne sürülen fikirler eserin yazarına aittir;
Rekabet Kurumunun görüşlerini yansıtmaz.

Bu tez, Rekabet Kurumu Başkan Yardımcısı Hasan Hüseyin ÜNLÜ, Rekabet Kurumu Başkan Yardımcısı Kürşat ÜNLÜSOY, Bilgi Yönetimi Dairesi Başkanı Haluk Recai BOSTAN, Doç. Dr. Mahmut YAVAŞI ve Yrd. Doç. Dr. Fatih Cemil ÖZBUĞDAY'dan oluşan Tez Değerlendirme Heyeti tarafından 08.08.2017 tarihinde yürütülen Tez Savunma Toplantısı sonucunda yeterli ve başarılı kabul edilmiştir.

Tez yazarı Fatih ÇİROĞLU, 11.12.2017 tarihinde yapılan Yeterlik Sınavında başarılı olmuş ve Başkanlık Makamının 10.01.2018 tarih ve 427 sayılı onayı ile Rekabet Uzmanı olarak atanmıştır.

YAYIN NO

347

İÇİNDEKİLER

KISALTMALAR.....	ix
GİRİŞ	1

BÖLÜM 1

MOBİL CİHAZ KAVRAMI ve MOBİL CİHAZLARDA ADLİ BİLİŞİM

1.1. MOBİL CİHAZ TEKNOLOJİLERİNE GENEL BAKIŞ	5
1.1.1. Mobil Cihazlarda İletişim Protokolleri.....	7
1.1.2. Mobil Cihazlarda Veri Depolama.....	8
1.1.3. Mobil Cihazlarda Kullanılan İşletim Sistemleri.....	10
1.1.3.1. Android İşletim Sistemi ve Rootlama Kavramı	11
1.1.3.2. iOS İşletim Sistemi ve Jailbreak Kavramı	12
1.2. MOBİL CİHAZLARDA DİJİTAL DELİL KAVRAMI	13
1.3. MOBİL CİHAZLARDA ADLİ BİLİŞİM KAVRAMI.....	14
1.4. MOBİL CİHAZLARDAN VERİ ELDE ETME YÖNTEMLERİ	15

BÖLÜM 2

MOBİL CİHAZ İNCELEMELERİNDE KULLANILAN ADLİ BİLİŞİM ARAÇLARI ve YERİNDE İNCELEMELER İÇİN SÜREÇ MODELLERİ OLUŞTURULMASI

2.1. MOBİL CİHAZ İNCELEMELERİNDE KULLANILAN ADLİ BİLİŞİM ARAÇLARININ SINIFLANDIRILMASI.....	17
2.1.1. Manuel İnceleme (Manuel Extraction).....	18
2.1.2. Mantıksal İmaj Alma (Logical Extraction)	18
2.1.3. Fiziksel İmaj Alma (Hex Dumping / JTAG)	19
2.1.4. Çip Sökme (Chip-Off).....	19
2.1.5. Mikro İnceleme (Micro Read).....	20
2.2. MOBİL CİHAZLARDA ADLİ BİLİŞİM ARAÇLARI	20
2.2.1. Cellebrite	21

2.2.2. XRY	21
2.2.3. Paraben	22
2.2.4. Oxygen Forensics	23
2.2.5. AccessData	23
2.3. YERİNDE İNCELEMELER KAPSAMINDA SÜREÇ MODELLERİ OLUŞTURULMASI	24
2.3.1. Koruma	24
2.3.2. Elde Etme	27
2.3.3. İnceleme ve Analiz	30
2.3.4. Raporlama	31
2.4. YERİNDE İNCELEMELERDE MOBİL CİHAZ İNCELEMELERİNİ ZORLAŞTIRMASI MUHTEMEL ETMENLER	33

BÖLÜM 3

MOBİL CİHAZLARIN ADLİ BİLİŞİM ARAÇLARIYLA İNCELENMESİ

3.1. ÖRNEK OLAY.....	35
3.1.1. Araştırma Yöntemi ve İncelenen Mobil Cihaz.....	36
3.1.2. Cihazın Fabrika Verilerine Sıfırlanarak İncelenmeye Hazırlanması.....	37
3.1.3. Örnek Olay Kapsamında Oluşturulan Veriler.....	37
3.2. İNCELEME ORTAMI VE KULLANILAN ADLİ BİLİŞİM ARAÇLARI	39
3.2.1. XRY	39
3.2.2. Cellebrite UFED Touch ve Physical Analyzer	41
3.2.3. Oxygen Forensics Detective.....	44
3.3. REKABET İHLALİNE YÖNELİK İNCELEME SONRASINDA ELDE EDİLEN BULGULAR.....	45
3.3.1. WhatsApp Messenger.....	46
3.3.2. Google Hangouts.....	48
3.3.3. Gmail	50

3.3.4. Google Chrome	51
3.3.5. Arama Kayıtları ve Rehber	52
3.3.6. SMS	54
3.3.7. Konum Bilgileri	55
3.3.8. Fotoğraflar ve Ses Kayıtları	57
3.3.9. Elektronik Belgeler	58
3.3.10. Oxygen Forensics Detective Analizleri	60
3.4. İNCELEMEDE KULLANILAN ADLİ BİLİŞİM ARAÇLARININ DEĞERLENDİRİLMESİ	62
3.4.1. Test Cihazından Elde Edilen Sonuçlar Kapsamında Değerlendirme	62
3.4.2. Bölüm Değerlendirmesi	63

BÖLÜM 4

AB ve TÜRKİYE REKABET HUKUKU UYGULAMASINDA MOBİL CİHAZLARIN İNCELENMESİ

4.1. AB UYGULAMASI	65
4.1.1. Yerinde İncelemelere İlişkin Açıklayıcı Not	65
4.1.2. Bring Your Own Device (BYOD) Kavramı	66
4.1.3. Wipe Kavramı	67
4.1.4. Mühürlü Zarf Prosedürü	67
4.1.5. Kişisel Verilerin Korunması	68
4.1.6. Mobil Cihazların İncelenme Süreci	68
4.2. MOBİL CİHAZLARIN İNCELENMESİNE İLİŞKİN AB ÜYESİ ÜLKE UYGULAMALARINDAN ÖRNEKLER	72
4.2.1. İspanya Uygulaması	72
4.2.2. Macaristan Uygulaması	73
4.2.3. Hollanda Uygulaması	73
4.3. MOBİL CİHAZLARIN İNCELENMESİNE İLİŞKİN TÜRKİYE	

UYGULAMALARI	74
4.3.1. Mobil Cihazlarda Dijital Delil Kavramının Kurum Perspektifinden Değerlendirilmesi	74
4.3.2. 4054 Sayılı Kanun'un Yİ'lerde Kuruma Verdiği Yetki	75
4.3.3. Mevzuatta Yer Alan Diğer Düzenlemeler.....	77
4.3.4. Mobil Cihazlarda Adli Bilişim Araçlarının Kullanılmasına İlişkin Yetki Tartışması	78
SONUÇ	82
ABSTRACT	84
KAYNAKÇA	85
 GRAFİK DİZİNİ	
Grafik 1: Dünyada İnternet Kullanımı (Statcounter 2016)	4
Grafik 2 : Türkiye'de Toplam Mobil Abone Sayısı ve Nüfusa Göre Penetrasyon (BTK 2016, 39)	6
 ŞEKİL DİZİNİ	
Şekil 1: SIM kart çeşitleri ve boyutları	8
Şekil 2: NOR, RAM ve NAND hafızalar ve nesilleri (Ayers vd. 2014, 6).....	10
Şekil 3: Mobil Adli Bilişim Araçlarının Sınıflandırılması (Brothers 2014, 2)...	18
Şekil 4: Mobil Cihazlarda Adli Bilişim Süreçleri	24
Şekil 5: Faraday Çantası Örneği	26
Şekil 6: Yİ'lerde Mobil Cihazlar İçin Önerilen Koruma Süreci	27
Şekil 7: Alghafli vd. (2011, 6) Tarafından Oluşturulan Model Baz Alınarak Tasarlanan Yİ'lerde Mobil Cihazlar İçin Önerilen Elde Etme Süreci ...	29
Şekil 8: Yİ'lerde Mobil Cihazlar İçin Önerilen İnceleme ve Analiz Süreci	31
Şekil 9: Yİ'lerde Mobil Cihazlar İçin Önerilen Raporlama Süreci	32
Şekil 10: LG G2 D802 4G LTE	37

Şekil 11: XRY Office Kullanılarak Cihazın Kopyalarının Alınması	40
Şekil 12: XRY Reader Arayüzü	40
Şekil 13: UFED Touch’la Cihazın Kopyalarının Alınması.....	42
Şekil 14: OFD Veri Elde Etme Ekranı	44
Şekil 15: OFD Analytics Seçenekleri	45
Şekil 16: WhatsApp Grup İletileri	47
Şekil 17: Google Hangouts İletileri	49
Şekil 18: Gmail’den Elde Edilen İki Farklı E-posta Yazışması	50
Şekil 19: Tarayıcı Geçmişi Verileri.....	51
Şekil 20: Ypersonel ve Zpersonel’e Ait İletişim Bilgileri.....	52
Şekil 21: Xpersonel ve Ypersonel arasında gerçekleşen Çağrı Geçmişi Örneği..	53
Şekil 22: Xpersonel tarafından Ypersonel ve Zpersonel’e Gönderilen SMS’ler .	54
Şekil 23: Here Maps ve Google Maps konumları.....	56
Şekil 24: Toplantıda Konuşulan Konulara Dair Fotoğraf Örneği	57
Şekil 25: Elektronik Belge Örnekleri.....	59
Şekil 26: OFD İletişim İstatistikleri Analiz Ekranı.....	60
Şekil 27: OFD Konum Analiz Ekranı	61
Şekil 28: İletişim Kayıtları Analiz Ekranı.....	61
Şekil 29: Oxygen Forensics Cloud Extractor Ekranı.....	62
Şekil 30: Komisyon’un İnceleme Yönergesi Işığında İnceleme Süreci (Erps ve Doury 2013, 213-214)	69
Şekil 31: Mühürlü Zarf Prosedürü Kapsamındaki Verinin Komisyon’da İncelendiği Usul	70

TABLO DİZİNİ

Tablo 1: SD Standartları.....	9
Tablo 2: Akıllı Telefon İşletim Sistemi Pazar Payları.....	11

Tablo 3: Örnek Olay Kapsamında Oluşturulan Teşebbüsler ve Çalışanları.....	35
Tablo 4: XRY'dan Elde Edilen Veriler	41
Tablo 5: UFED Physical Analyzer Kullanılarak Elde Edilen Veriler	43
Tablo 6: WhatsApp'tan Elde Edilen Veriler Tablosu	48
Tablo 7: Hangouts'tan Elde Edilen Veriler Tablosu.....	49
Tablo 8: Gmail'den Elde Edilen Veriler Tablosu	51
Tablo 9: Chrome'dan Elde Edilen Veriler Tablosu	52
Tablo 10: Arama Kayıtları ve Adres Defterinden Elde Edilen Veriler Tablosu ...	53
Tablo 11: SMS'lerden Elde Edilen Veriler Tablosu	55
Tablo 12: Konum Bilgilerine Ait Veriler Tablosu	56
Tablo 13: Fotoğraflar ve Ses Kayıtlarına Ait Veriler Tablosu	58
Tablo 14: Elektronik Belgeler Tablosu	59

KISALTMALAR

ACM	: Hollanda Rekabet Otoritesi (The Authority for Consumers and Markets)
Bkz.	: Bakınız
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
BYOD	: Bring Your Own Device
CDMA	: Code Division Multiple Access
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
CNMC	: İspanya Rekabet Otoritesi (Comisión Nacional de los Mercados y la Competencia)
EB	: Eksabayt
EXIF	: Exchangeable Image File
GB	: Gigabayt
GSM	: Global System for Mobile Communications
GVH	: Macaristan Rekabet Otoritesi (Gazdasági Versenyhivatal)
ICCD	: Integrated Circuit Card Identifier
ICN	: Uluslararası Rekabet Ağı (International Competition Network)
IMEI	: International Mobile Equipment Identity
IMSI	: International Mobile Subscriber Identity
iDEN	: Integrated Digital Enhanced Network
JTAG	: Joint Test Action Group
Kanun	: 4054 Sayılı Rekabetin Korunması Hakkında Kanun
Komisyon	: Avrupa Birliği Komisyonu
Kurul	: Rekabet Kurulu
Kurum	: Rekabet Kurumu
LAI	: Location Area Identity
LCD	: Sıvı Kristal Ekran (Liquid Cristal Display)
MMC	: Multimedia Card
MSISDN	: Mobile Subscriber Integrated Services Digital Network
NIST	: National Institute of Standards and Technology
OCR	: Optical Character Recognition
OECD	: Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organization for

	Economic Cooperation and Development)
OHA	: Open Handset Alliance
PDA	: Personal Digital Assistant
PIN	: Personal Identification Number
PUK	: Personal Unlocking Key
RAM	: Rastgele Erişilebilir Bellek (Random Access Memory)
ROM	: Salt Okunur Bellek (Read Only Memory)
SD	: Secure Digital
SDHC	: Secure Digital High Capacity
SDXC	: Secure Digital Extended Capacity
SIM	: Subscriber Identity Module
SMS	: Short Message Service
TB	: Terabayt
TDMA	: Time Division Multiple Access
UFED	: Universal Forensic Extraction Device
USB	: Universal Serial Bus
vb.	: ve benzeri
vd.	: ve diğerleri
WiFi	: Wireless Fidelity
Yİ	: Yerinde inceleme

GİRİŞ

Rekabet otoriteleri rekabet ihlallerine ilişkin delillere farklı araçları kullanarak ulaşmaktadır. Bu araçlar, bilgi isteme veya yerinde inceleme (Yİ) yoluyla teşebbüslerin¹ ceza tehdidiyle delil vermeye zorunlu bırakılmaları ve gönüllü olarak otoritelere pişmanlık başvurularında bulunmaları olarak sıralanmaktadır (Wils 2006, 4). Rekabet ihlallerinin açıklığa kavuşturulmasına yönelik verdiği geniş yetkiler bakımından en önemli delil elde etme yönteminin Yİ'ler olduğu kabul edilmektedir (Gündüz 2009, 18). Rekabet hukukunda en ciddi rekabet ihlali olarak değerlendirilen (OECD 1998, 2) ve delilleri saklamak konusunda gelişmiş yöntemlere başvuran karteller, ihlale kanıt olabilecek dijital delilleri gizleme bağlamında sınırsız imkânlarla sahipken, rekabet otoritelerinin Yİ'lerde kullanabileceği imkânların sınırlı olması, Yİ'lerin etkinliği sorusunu gündeme getirmektedir. Ayrıca Yİ'lerde, ispat gücü yüksek delillerin elde edilmesinin giderek zorlaştığı ve hatta istisnai bir hale geldiği de bilinmektedir (Can 2012, 18). Kartellerle mücadelenin rekabet otoriteleri ve karteller arasında bir silahlanma yarışı olduğu varsayımı altında, otoritelerin bu yarışı kazanmak için gelişmiş bir rekabet hukuku sistemine sahip olmaları gerektiği sonucu ortaya çıkmaktadır.

Söz konusu yarışın bir parçası olan Rekabet Kurumu (Kurum) tarafından gerçekleştirilen Yİ'ler, teşebbüslere ait bilişim altyapısında (sunucular ve istemciler) anahtar kelime aramalarıyla sınırlı kalmakta ve Yİ'lerde rekabet ihlallerine yönelik dijital delillerin ortaya çıkarılmasında meslek personeline herhangi bir adli bilişim² donanımı ve yazılımı kullanılmamaktadır. Bununla birlikte, Yİ'lerde teşebbüs çalışanlarına ait akıllı telefon ve tablet gibi mobil cihazlar da inceleme konusu yapılmamaktadır. İnceleme konusu yapılmayan mobil cihazlar, giderek daha fazla oranda teşebbüslerin iş akışlarında yer edinmekte ve

¹ Teşebbüs ifadesi, teşebbüs birliklerini de kapsayacak şekilde kullanılmaktadır.

² Adli Bilişim kavramı Türkçe'ye "*Computer Forensics*" teriminin çevrilmesiyle kazandırılmıştır (Henkoğlu 2014, 1).

teşebbüslerin elektronik dünyayla etkileşimlerinde aktif rol oynamaktadır. Bu bilgiler ışığında, Yİ'lerde mobil cihazların incelenmemesi hususunun, anılan silahlanma yarışında Kurum'u açık bir şekilde geriye düşürdüğü görülmektedir. Bu nedenle, mobil cihazların incelenmesi konusunda bir çalışma yapılması ihtiyacı ortaya çıkmaktadır.

Yİ'lerde mobil cihazların incelenmesi hususunda, delil bütünlüğünün ve elde edilen sonuçların hukuki makamlarca kabul edilebilirliğinin sağlanması için adli bilişim disiplininin faydalanılması gerekmektedir (Tamma ve Tindal 2015,3). Ayrıca, mobil cihaz incelemelerinin de dâhil olduğu adli bilişim süreçlerinde, dijital veri elde etme amacıyla gerçekleştirilen tüm işlemlerin genel kabul edilen yöntemler kullanılarak yapılması önemli olan bir diğer husustur (Henkoğlu 2014, 2).

Mobil cihazların Yİ'lerde incelenmesi konusunun hukuki boyutundan ziyade teknik boyutunu ayrıntılı olarak inceleyen bu çalışmanın birinci bölümünde, mobil cihaz kavramı ve mobil cihazlarda adli bilişim konularına yer verilmektedir. Mobil cihaz kavramı genel olarak incelendikten sonra mobil cihazlarda dijital delil ve adli bilişim kavramları aktarılmaktadır.

İkinci bölümde öncelikle, mobil cihazlarda adli bilişim araçlarının kullanımına yer verilmekte, ardından Yİ'lerde mobil cihazlar incelenirken karşılaşılabilecek muhtemel sorunlar da değerlendirilerek adli bilişim süreçleri iş akış diyagramları aktarılmaktadır. Böylelikle mobil cihazların Yİ'lerde incelenmesinde kullanılmak üzere Kurum ihtiyaçlarına yönelik bir prosedür listesi oluşturulması amaçlanmaktadır.

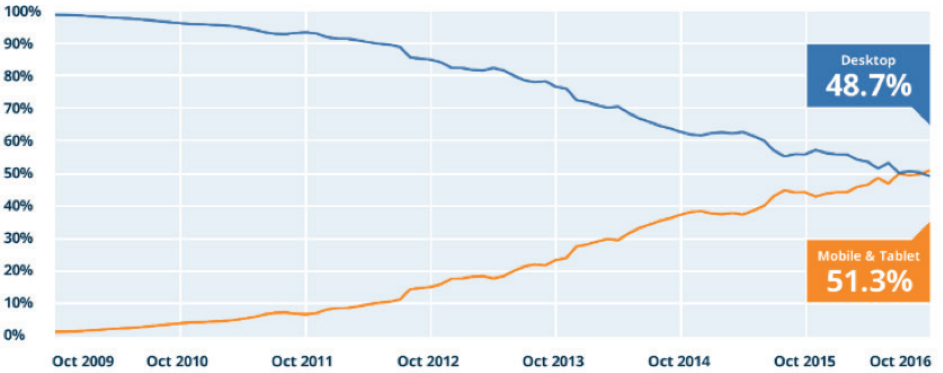
Üçüncü bölümde, ilk iki bölümde oluşturulan mobil cihaz ve adli bilişim temasının tamamlanması amacıyla kurgulanan örnek olay kapsamında mobil cihaz incelemesi gerçekleştirilmektedir. Bölüm kapsamında hayali bir kartel kurulmakta ve bahse konu kartelin organizatörü olan teşebbüs çalışanının mobil cihazında incelemeler yapılmaktadır. Bu bölümle, Yİ'de bir teşebbüs çalışanının mobil cihazının incelenmesiyle ne tür verilere ulaşılabileceği konusunun vurgulanması amaçlanmaktadır.

Dördüncü bölümde ise ilk olarak Avrupa Birlięi Komisyonu'nun (Komisyon) Yİ'lerde uyguladığı prosedürlerin mobil cihazlarla ilgili olduęu deęerlendirilen kısımlarıyla ilgili bilgiler aktarıldıktan sonra İspanya, Macaristan ve Hollanda uygulamalarıyla ilgili bilgiler aktarılmaktadır. Bölüm sonunda mobil cihazların Kurum perspektifinden incelenmesi açısından, yürürlükte bulunan farklı mevzuat karşılaştırılarak yetki tartışması yapılmakta ve Türkiye uygulamasına ilişkin önerilere yer verilmektedir.

BÖLÜM I

MOBİL CİHAZ KAVRAMI ve MOBİL CİHAZLARDA ADLİ BİLİŞİM

3 Nisan 1973 tarihinde Martin COOPER ile Dr. Joel S. ENGEL arasında gerçekleşen ilk cep telefonu³ görüşmesinden bu yana mobil cihaz teknolojisi gelişmeye ve değişmeye devam etmektedir (Hebert vd. 2008, 19). İletişim ihtiyacının karşılanmasında kullanılan, giderek küçülen, buna karşılık güçlenen mobil cihazlar, elektronik dünyayla etkileşimin sağlanması bakımından önemli iletişim aktörleri olarak ifade edilmektedir. Mobil cihazlar, artan işlem güçleri ve kazandıkları fonksiyonlarla iş hayatı ile günlük hayatın vazgeçilmez bir parçası haline gelmekte ve her geçen gün yeni özellikler kazanmaktadır. Mobil cihaz ve tabletlerde internet kullanımının masaüstü bilgisayarlarda internet kullanımını geçmesi mobil cihazların tüm dünyada yoğun şekilde kullanıldığını doğrular niteliktedir (Bkz. Grafik 1).



Grafik 1: Dünyada İnternet Kullanımı (Statcounter 2016)

³ 1,1 kg ağırlığa sahip olan ilk cep telefonu prototipi, otuz dakikalık görüşme süresini on saatin üzerinde şarj edilmesiyle sağlamaktaydı (Das 2016, 5).

Tüm dünyada yoğun bir şekilde kullanılan cep telefonu ve cep bilgisayarları şu şekilde tanımlanmaktadır (Henkoğlu 2014, 270):

“(…) iletişim amaçlı olarak kullanılan, üzerinde veri ve kişisel bilgiler saklanabilen, dijital fotoğraf ve video/ses kaydı yapabilen, navigasyon amacıyla kullanılabilen ve üzerine yüklenen yazılımlara bağlı olarak (Metin dosyaları, günlük, şifre bilgileri saklama ve takvim /görevler gibi) birçok farklı amaç için kullanılabilen taşınabilir aygıtlardır.”

Yukarıda tanımı verilen mobil cihazlar kullanıcılarına hareketlilik sunabilmek adına bataryayla çalışmakta, nispeten küçük ve hafif olarak tasarlanmakta olup, mikroişlemci, *ROM* (Salt Okunur Bellek), *RAM* (Rastgele Erişilebilir Bellek), radyo modülü, sayısal işaret işlemcisi, mikrofon, hoparlör, *LCD* (Sıvı Kristal Ekran) ve ihtiyaçlara göre özelleştirilmiş donanım ve arayüzlerden oluşmaktadır (Ayers vd. 2014, 3). Bu çerçevede, çalışma kapsamında sıklıkla kullanılacak olan “mobil cihaz” kavramı, iş hayatında yoğun şekilde kullanılan “cep telefonları ve akıllı telefonlar ile tabletleri” kapsamaktadır.

1.1. MOBİL CİHAZ TEKNOLOJİLERİNE GENEL BAKIŞ

Mobil cihaz sektöründe çeşitli ihtiyaçlara çözüm sunan birçok mobil cihaz bulunmakla birlikte, bu mobil cihazların donanımları, işletim sistemleri, uygulamaları, servisleri ve çevre elemanları farklılık gösterebilmektedir (Murphy 2009, 1). Konuşma yapmaya ve *SMS* (Short Message Service)⁴ gönderip almaya yarayan temel fonksiyonlara sahip telefonlar ile taşınabilir birer bilgisayar haline gelmiş akıllı telefonların donanımları arasında performans ve kapasite bakımından büyük farklılıklar bulunmaktadır (Ayers vd. 2014, 4).

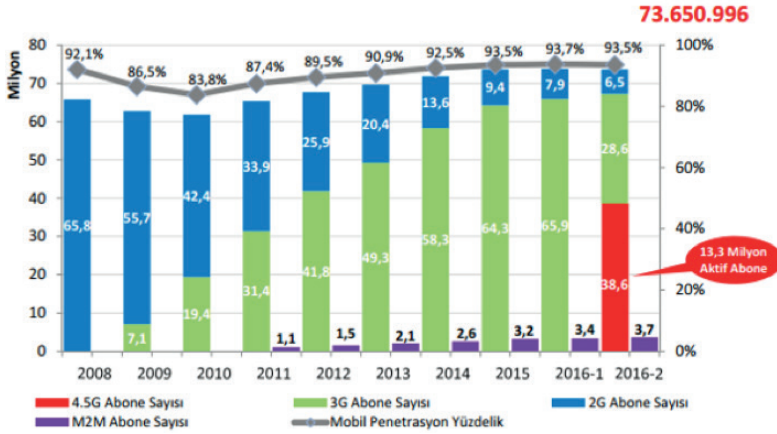
Gelişimine devam etmekte olan mobil cihaz teknolojisi, bireysel kullanıcılar ve iş dünyasınca ilgiyle takip edilmektedir. 2015 yılında araştırma şirketi The Radicati Group (2015, 2) tarafından yayımlanan raporda⁴ dünya genelinde 2015 yılı içinde 9,5 milyarın üzerinde olan mobil cihaz sayısının 2019 yılında 14,8 milyarı aşacağı öngörülmektedir. Ayrıca anılan raporda 2015 yılında 1,4 milyarın üzerindeki mobil e-posta kullanıcısı sayısının 2019 yılında 2,5 milyar seviyesine ulaşacağı tahmin edilmektedir. Bu rakamlar, dünya genelindeki

⁴ Mobile Statistics Report, 2015-2019, <http://www.radicati.com/wp/wp-content/uploads/2015/02/Mobile-Statistics-Report-2015-2019-Executive-Summary.pdf>, Erişim Tarihi: 27.09.2016.

e-posta kullanıcılarının %85'nin e-posta hesaplarına mobil cihazlar vasıtasıyla erişebileceklerine işaret etmektedir (Radicati Group 2015, 3).

2017 yılında Cisco (2017, 2) tarafından yayımlanan raporda⁵ 2016 yılında 7,2 EB⁶ (Eksabayt) civarında olan aylık mobil veri trafiğinin, 2021 yılında 49 EB'ye kadar yükseleceği öngörülmektedir.

Türkiye İstatistik Kurumu'nun (TÜİK) haber bültenine⁷ göre 2016 yılı Nisan ayında ülke genelindeki hanelerin %96,9'unda cep telefonu veya akıllı telefon bulunmaktadır. Bilişim Teknolojileri ve İletişim Kurumu (BTK) tarafından hazırlanan ve 2016 yılı Eylül ayında yayımlanan rapora⁸ göre Türkiye'de 73.650.996 mobil abone bulunmaktadır (Bkz. Grafik 2).



Grafik 2 : Türkiye'de Toplam Mobil Abone Sayısı ve Nüfusa Göre Penetrasyon (BTK 2016, 39)

⁵ Global Mobile Data Traffic Forecast Update, 2016-2021, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf>, Erişim Tarihi: 05.03.2017.

⁶ 1 EB = 10¹⁸ bayt.

⁷ Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2016, <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779>, Erişim Tarihi: 29.09.2016.

⁸ Üç Aylık Pazar verileri Raporu, 2016 Yılı 2. Çeyrek Nisan – Mayıs – Haziran, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fPazar_Verileri%2f2016-Q2.pdf, Erişim Tarihi: 29.09.2016.

Mobil cihazların sundukları özellikler ve sahip oldukları uygulamalar, cihazların kullanım sürelerini arttırmış ve kullanıcılar birçok alanda bilgisayarlarında gerçekleştirebilecekleri işlemleri mobil cihazlarından da gerçekleştirebilir hale gelmişlerdir.

Mobil cihazların artan teknolojik kapasiteleri, teşebbüslerin iş akışlarını mobil cihazlar üzerinden gerçekleştirmelerine de olanak sunmaktadır. E-posta alışverişinden teşebbüs ihtiyaçlarına uygun geliştirilmiş uygulamaların kullanımına kadar birçok işlem mobil cihazlarla gerçekleştirilebilmektedir (Tomlin 2016, 1). Bu bağlamda, yapılan araştırmalardan elde edilen istatistikler ışığında mobil cihazların kullanımının artmasıyla, bahse konu cihazlardan üretilen verinin giderek artacağı değerlendirilmektedir.

Çalışmanın kapsamını oluşturan günümüz modern mobil cihazlarının daha iyi tanınması amacıyla mobil cihazlar, iletişim protokolleri, veri depolama yöntemleri ve işletim sistemleri başlıkları altında incelenmektedir.

1.1.1. Mobil Cihazlarda İletişim Protokolleri

Mobil cihazlarda; *hücresele*, *WiFi* (Wireless Fidelity) ve *Bluetooth* gibi teknolojilerle haberleşme işlemi gerçekleştirilmektedir. Hücresele iletişimde, geniş alanlar, daha küçük coğrafi alanlara bölünüp hücre olarak adlandırılmakta ve her hücrede baz istasyonları kullanılarak mobil cihazlara radyo sinyalleri iletilmektedir (Gonzalez vd. 2011, 1). Halihazırda farklı ülke ve bölgelerde *CDMA* (Code Division Multiple Access), *GSM* (Global System for Mobile Communications), *TDMA* (Time Division Multiple Access) ve *iDEN* (Integrated Digital Enhanced Network) gibi hücresele ağ teknolojileri kullanılmaktadır (Punja ve Mislan 2008, 1).

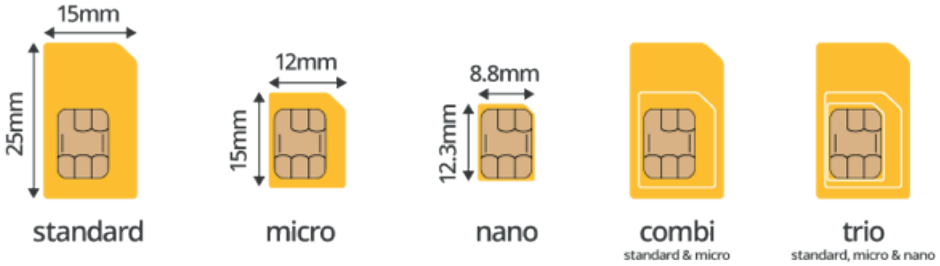
WiFi teknolojisi radyo dalgalarını kullanarak ağ bağlantısı oluşturan teknolojidir. *WiFi* bağlantısı, cihazların kablosuz adaptörler aracılığıyla ağa ve internete erişimlerinin sağlanması için kablosuz bağlantı noktalarından sağlanmaktadır (Sidhu vd. 2007, 44).

Bluetooth teknolojisi, belli bir mesafedeki cihazların birbirleriyle kablosuz olarak eşleşip, aralarında veri aktarımı ve bağlantı işlemlerini gerçekleştirmelerini sağlayan, kısa mesafe radyo frekansı teknolojisine verilen addır (Haartsen 2000, 28).

1.1.2. Mobil Cihazlarda Veri Depolama

Mobil cihazlarda veri depolama işlemi; *SIM* (Subscriber Identity Module) kartlarda, hafıza kartlarında (*Micro SD* vb.) ve mobil cihazın hafızasında gerçekleştirilmektedir (Al-Hadadi ve AlShidhani 2013, 576).

SIM kart, mobil cihazlarda kullanılan bir akıllı kart olup hücresel ağlara bağlanmak için yetki denetiminin sağlanması amacıyla gerekli bilgileri barındırmaktadır (Reiber 2016, 17). Mobil cihazdan gerçekleştirilen aramalara dair kayıtlar, alınan veya gönderilen *SMS*'ler ve kayıtlı telefon numaraları gibi önemli kullanıcı bilgileri *SIM* kartta depolanmaktadır. Ayrıca *SIM* kartta, kartın seri numarası *ICCD* (Integrated Circuit Card Identifier), karta atanan telefon numarası *MSISDN* (Mobile Subscriber Integrated Services Digital Network), şebekede aboneyi tanımlayan *IMSI* (International Mobile Subscriber Identity) ve abonenin *GSM* şebekesinde bulunduğu yeri tanımlayan *LAI* (Location Area Identity) bilgileri yer almaktadır (Willassen 2003, 6). *SIM* kart çeşitlerine Şekil 1'de yer verilmektedir.



Şekil 1: SIM kart çeşitleri ve boyutları⁹

Hafıza kartları, mobil cihazların depolama kapasitelerini arttırmak amacıyla kullanılan depolama çözümleridir. Hafıza kartlarına uygulama bilgileri, belgeler, fotoğraflar, videolar ve diğer medyalar gibi birçok verinin depolanması mümkündür. *SD* kartlar için *SD* (Secure Digital Standard Capacity), *SDHC* (Secure Digital High Capacity) ve *SDXC* (Secure Digital Extended Capacity) olmak üzere üç adet kapasite standardı bulunmaktadır (Bkz. Tablo 1). *SD* standardı 2 *GB* (Gigabayt)

⁹ Bkz. <http://www.simcardwarehouse.com/wp-content/uploads/2014/11/simcards.png>, Erişim Tarihi: 19.10.2016.

civarı veri saklama sınırına sahipken, *SDXC* standardıyla üretilen kartlara yaklaşık 2 TB (Terabayt)'a kadar veri kopyalanabilir.

		SD Standard	SDHC Standard	SDXC Standard
Capacity		up to 2GB	more than 2GB up to 32GB	more than 32GB up to 2TB
File System		FAT 12, 16	FAT 32	exFAT
SD Logo				
Card Specifications	SD	32 x 24 x 2.1 mm, Approx 2g		
	miniSD	20 x 21.5 x 1.4 mm, Approx 1g		
	microSD	11 x 15 x 1.0 mm, Approx 0.5g		

Tablo 1: SD Standartları¹⁰

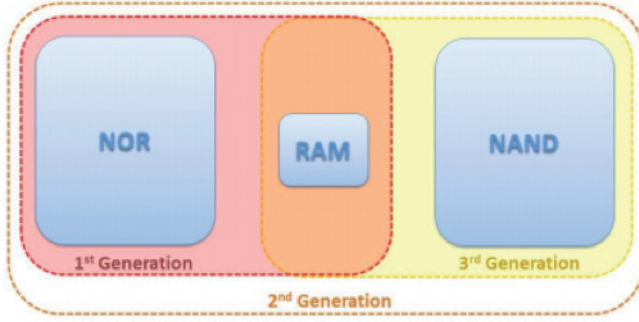
Mobil cihazlar, uçucu¹¹ ve uçucu olmayan verilerin¹² depolandığı uçucu ve uçucu olmayan bellekleri barındırmaktadır. Uçucu hafıza (*RAM*) dinamik bir depolama alanı olup cihazın gücünün kesilmesi durumunda veriyi saklamamaktadır. Uçucu olmayan hafızalarda veriler kalıcı olarak saklanmakta ve cihazın gücünün kesilmesi durumunda dahi mevcut veriler korunmaktadır. Mobil cihazlarda kalıcı hafıza türleri olarak *NAND* ve *NOR* bulunmakta olup, bahse konu cihazlar genellikle bir veya iki farklı uçucu olmayan hafıza türünü barındırmaktadır (Bkz. Şekil 2). *NAND* tipi hafızalar, *NOR*'a göre daha yüksek işlem hızı ve depolama alanı sunmaktadır. *NAND*, *NOR*'a oranla daha yüksek yazma ve silme hızına sahipken; *NOR* daha yüksek okuma hızına sahiptir (Tal

¹⁰ Bkz. <https://www.sdcard.org/developers/overview/capacity/>, Erişim Tarihi: 20.10.2016.

¹¹ Uçucu veri cihazın geçici depolama birimlerine kaydedilen ve cihazın gücünün kapatılmasıyla cihazın geçici depolama birimlerinde saklanmayan geçici veridir (Panchal 2013, 965).

¹² Uçucu olmayan veriler cihazda depolanan kalıcı veriler olup, cihazın gücünün kesilmesi durumunda veri kaybı yaşanmamaktadır (Panchal 2013, 965).

2002, 4). Temel fonksiyonlara sahip telefonlarda depolama çözümü için *NOR* ve *RAM* kullanılırken; yeni nesil akıllı telefonlarda *NAND* ve *RAM* kullanılmaktadır. *RAM*'de kullanıcı şifreleri, yapılandırma dosyaları saklanırken, *NOR*'da işletim sistemi kodları, cihaz sürücüler, sistem kütüphaneleri, çekirdek (*kernel*) saklanmakta ve son olarak *NAND*'da grafik, ses, video ve diğer kullanıcı dosyaları yer almaktadır.



Şekil 2: NOR, RAM ve NAND hafızalar ve nesilleri (Ayers vd. 2014, 6)

1.1.3. Mobil Cihazlarda Kullanılan İşletim Sistemleri

Mobil işletim sistemi pazarında, başta *Android*, *Apple iOS* (eski adıyla *iPhone OS*), *Windows Phone OS*, *BlackBerry OS*, *Tizen* ve *Ubuntu Touch OS* olmak üzere birçok farklı mobil işletim sistemi yer almaktadır. International Data Group (IDG) tarafından yayımlanan 2016 yılı Ağustos verilerine göre *Android* ve *iOS* mobil işletim sistemlerinin 2016 yılının ikinci çeyreğinde akıllı telefon işletim sistemi pazarında kullanım oranları toplam %99,3'tür (Bkz. Tablo 2).

<i>Periyot</i>	<i>Android</i>	<i>iOS</i>	<i>Windows Phone</i>	<i>Diğerleri</i>
2015 – 3. Çeyrek	%84,3	%13,4	%1,8	%0,5
2015- 4. Çeyrek	%79,6	%18,6	%1,2	%0,5
2016 – 1. Çeyrek	%83,4	%15,4	%0,8	%0,4
2016 – 2. Çeyrek	%87,6	%11,7	%0,4	%0,3

Tablo 2: Akıllı Telefon İşletim Sistemi Pazar Payları¹³

Ayrıca *Symbian*, *Nokia X Platform*, *Firefox OS*, *Bada*, *Palm OS*, *webOS*, *Maemo*, *MeeGo* ve *LiMo* gibi mobil işletim sistemlerinin geliştirilmesi geçmiş yıllarda durdurulmuş olup, bahse konu işletim sistemlerine sahip mobil cihazlar halen piyasada bulunabilmektedir. Kullanım oranlarının oldukça yüksek olması nedeniyle bu bölümde yalnızca *Android* ve *iOS* işletim sistemleri hakkında ayrıntılı bilgi verilecektir.

1.1.3.1. Android İşletim Sistemi ve Rootlama Kavramı

Google’ın açık kaynak kodlu bir platformu olan *Android*, *Linux* tabanlı mobil işletim sistemi olarak tanımlanmaktadır (Dixit 2014, 29). *Android* mobil işletim sistemi, 84 farklı şirketin birlikteliğiyle oluşturulan *Open Handset Alliance* (OHA)’nın desteğiyle geliştirilmektedir (Lessard ve Kessler 2010,1). *Android* platformunun açık kaynak kodlu yapısı cihaz üreticilerine, işletim sistemlerini, ürettikleri cihazlara göre özelleştirme imkânı sunmakta ve *Android*’i popüler işletim sistemlerinden biri haline getirmektedir (Tamma ve Tindall 2015, 12).

Android, *Linux*’le benzer bir kullanıcı yönetim mekanizmasına sahiptir. *Linux* çoklu kullanıcı¹⁴ tabanlı bir işletim sistemi olup, *Linux*’te önemli sistem dosyalarına erişimin sağlanması ve kullanıcıların yetkilendirilmesi gibi ayrıcalıklı işlemler “*superuser*” veya “*root*” adı verilen hesaplarla yapılmaktadır. *Root*¹⁵ kullanıcısı yazılım yükleme, normal kullanıcıların silmeye yetkilerinin

¹³ Bkz. <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>, Erişim Tarihi: 01.10.2016.

¹⁴ *Linux* işletim sisteminde *root*, *sistem* ve *normal* kullanıcı adında üç tür kullanıcı bulunmaktadır. (Ray ve Ray 2015, 287).

¹⁵ *Root* kullanıcısı *Unix* tabanlı sistemlerde en yüksek yetkiye sahip kullanıcıdır (Raggi vd. 2011,446).

olmadığı dosyaları silme, işletim sistemi servislerini açma veya kapatma, diğer kullanıcıların yetkilerini ve kullanıcı parolalarını değiştirme gibi haklara sahiptir (James 2012, 97). Bu noktada, *Android* işletim sistemini kullanan mobil cihazın *rootlanması*¹⁶, *Linux* işletim sistemine benzer şekilde cihaz üzerinde normal kullanıcı yetkilerinin yetmediği işlemlerin yapılmasına olanak sağlanmaktadır. *Rootlama*¹⁷ işlemiyle mobil cihaz kullanıcıları, mobil cihazlarını daha yüksek yetkilerle kullanmakta ve cihaz üzerindeki kontrollerini arttırmaktadırlar (Sun vd. 2015, 3). *Android*'de bulunan *Linux Kernel* katmanındaki bazı güvenlik zafiyetlerinin kullanılmasıyla gerçekleştirilen *rootlama* teknikleri, işletim sisteminin güncelleştirilmesiyle kullanım dışı kalmaktadır (Xu ve Fu 2015, 1).

Android'de her uygulama ayrı bir kullanıcı gibi *UID*'ye (*User ID*)'ye sahiptir. Bu nedenle uygulamaların sistem kaynaklarına erişimleri sınırlı olmaktadır. Uygulamalara has özel veriler *Android* işletim sisteminde */data/data* klasörü altında tutulmakta ve bu verilere sadece veriyi oluşturan uygulama erişebilmektedir (Tamma ve Tindall 2015, 61). Mobil cihazın *rootlanması* işlemiyle uygulamaların oluşturdukları veriye erişim mümkün olmaktadır.

1.1.3.2. iOS İşletim Sistemi ve Jailbreak Kavramı

iOS işletim sistemi Apple'a ait *iPhone*, *iPad*, *Apple TV* ve *iPod Touch* gibi mobil cihazlarda kullanılan bir mobil işletim sistemidir (Hoog ve Strzempka 2011, 70). Mobil cihaza ait donanımı yönetmekle birlikte uygulamaların cihazla uyumlu çalışması için gerekli teknolojileri barındıran *iOS*, *Phone*, *Mail* ve *Safari* gibi yerleşik uygulamalarla birlikte gelmektedir (Epifani ve Stirparo 2015, 91). *iOS* yüklü mobil cihaz kullanıcıları ihtiyaçlarına uygun uygulamalara *App Store*¹⁸ vasıtasıyla ulaşabilmektedirler.

¹⁶ *Android* işletim sistemini kullanan mobil cihazlarda gerçekleştirilen adli bilişim incelemelerinde cihazdan *fiziksel* elde etme yönteminin kullanılması için cihaz *rootlama* yapılması söz konusu olabilir. (Tamma ve Tindall 2015, 61). Mobil cihazlardan veri elde etmede kullanılan adli bilişim yöntemlerine çalışmanın ilerleyen bölümlerinde yer verilmektedir.

¹⁷ Yanlış yapılan *rootlama* işleminin mobil cihazın kullanım dışı kalmasına sebebiyet verebilir. Ayrıca mobil cihaza *rootlama* yapılması sebebiyle bazı üreticilere ait mobil cihazların garanti dışı kalması olasılığı da göz önünde bulundurulmalıdır.

¹⁸ *App Store*, Apple tarafından işletilen çevrimiçi uygulama mağazasıdır.

iOS işletim sistemi *App Store* haricinde dağıtılan uygulama, eklenti veya temaların kurulmasına izin vermemektedir (Govindaraj vd. 2014, 1). Bu kısıtlamaların önüne geçmek amacıyla iOS kullanıcıları cihazlarında *jailbreak* işlemini gerçekleştirebilmektedirler. *Jailbreak*, iOS'un (yazılım veya donanım zafiyetlerinin kullanılmasıyla) kırılması prosedürü olup, kullanıcılara işletim sisteminin daha yüksek yetkiyle kullanılması, iOS dosya sistemine erişim sağlanması ve GSM, ağ kullanımı gibi bazı kısıtlamaların kaldırılmasını sağlamaktadır (Chang vd. 2015, 20). *Jailbreak*¹⁹ çeşitleri şu şekilde sıralanmaktadır:

- **Tethered Jailbreak:** Cihaz yeniden başlatıldığında *jailbreak* işlemi devre dışı kalmaktadır.
- **Untethered Jailbreak:** Cihaz yeniden başlatıldığında *jailbreak* işlemi devre dışı kalmamaktadır.
- **Semi-Tethered Jailbreak:** Cihazın yeniden başlatıldığında *jailbreak*'in aktif olduğu fakat bazı uygulamaların kullanılması için bilgisayara bağımlılığın söz konusu olduğu *jailbreak* çeşididir.

*Jailbreak*²⁰, iOS sistem dosyalarının yer aldığı disk bölümünde değişiklikler gerçekleştirmekte olup, kullanıcı dosyalarının yer aldığı disk bölümünde herhangi bir müdahalede bulunmamaktadır (Epifani ve Stirparo 2015, 17).

1.2. MOBİL CİHAZLARDA DİJİTAL DELİL KAVRAMI

ICN²¹ (2014, 5) tarafından dijital delil "(...) bir dosyada kullanılabilecek dijital formdaki tüm bilgiler" olarak tanımlanmış olup, dijital delillerin, depolama medyalarından (veri taşıyıcılar), ağ trafiğinin izlenmesinden ya da incelemelerde dijital kopyaların (adli bilişim kopyalarının alınması, dosyaların kopyalanması vb.) oluşturulmasından elde edilebileceği belirtilmektedir. ICN (2014, 5) veri taşıyıcılarına örnek olarak *PDA*'ları (Personal Digital Assistant), cep telefonlarına

¹⁹ *Jailbreak* çeşitleriyle ilgili daha detaylı bilgi için bkz. <http://www.oguzhantopgul.com/2013/04/tethered-untethered-semi-tethered.html>, Erişim Tarihi: 05.11.2016.

²⁰ iOS işletim sistemini kullanan mobil cihazlarda gerçekleştirilen adli bilişim incelemelerinde cihazdan *fiziksel* elde etme yönteminin kullanılması için bahse konu mobil cihaza *jailbreak* yapılması durumu söz konusu olabilir (Epifani ve Stirparo 2015, 17). Mobil cihazlardan veri elde etmede kullanılan adli bilişim yöntemlerine çalışmanın ilerleyen bölümlerinde yer yerilmektedir.

²¹ Uluslararası Rekabet Ağı.

ait *SIM* kartları ve hafıza kartlarını da sıralamaktadır. Bu bağlamda çalışmanın konusunu oluşturan mobil cihazlardan aşağıdaki başlıklar altında dijital delillerin elde edilmesi mümkündür:

- **Adres Defteri:** Kayıtlı kişi bilgileri, numaralar, e-postalar,
- **Çağrı Geçmişi:** Gelen, giden, cevapsız aramalar,
- **SMS, MMS:** Alınan, gönderilen mesajlar,
- **Takvim Bilgileri:** Takvime yapılan veri girişleri,
- **Anlık Mesajlaşma Uygulamaları:** *WhatsApp, Skype, Tango, Viber* vd. gibi uygulamalarla yapılan yazışmalar ve multimedya kayıtları,
- **E-postalar:** Alınan, gönderilen, taslaklara kaydedilen, silinen vd. gibi e-posta mesajları,
- **Web Tarayıcı Geçmişi:** Ziyaret edilen web sitelerine ait geçmiş bilgileri,
- **Fotoğraflar ve Videolar:** Mobil cihaza ait kameradan çekilen, web tarayıcısından indirilen veya anlık mesajlaşma uygulamalarıyla alınan, gönderilen resimler ile videolar,
- **Ses Kayıtları ve Müzikler:** Mobil cihazın mikrofonundan kaydedilen veya farklı bir cihazdan alınan ses kayıtları ve müzikler,
- **Haritalar:** Aranan konumlar, indirilen haritalar,
- **Yer ve Konum Bilgisi:** Cihaza ait geçmiş konum bilgileri,
- **Elektronik Belgeler:** Mobil cihaz üzerindeki bir uygulamayla oluşturulan, indirilen veya farklı bir cihazdan elde edilen belgeler,
- **Silinmiş Veriler:** Mobil cihazdan kurtarılan silinmiş veriler,
- **Uygulamalar:** Cihaz üzerinde yüklü uygulamalara ait veriler.

1.3. MOBİL CİHAZLARDA ADLİ BİLİŞİM KAVRAMI

Henkoğlu (2014, 1) adli bilişim kavramını; “*Bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçta işlemede veya yasaklanmış bir*

faaliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür.” şeklinde tanımlamaktadır. Adli bilişim, ICN (2014, 2) tarafından şu şekilde ifade edilmektedir:

Adli bilişim dijital bilginin koruması, tanımlanması, dışarı çıkartılması, kimlik doğrulamasının yapılması, incelenmesi, analiz edilmesi, yorumlanması ve dokümanite edilmesi için özel tekniklerin kullanılmasıdır.

Adli bilişim disiplini bilgisayar, disk, ağ, güvenlik duvarı, cihaz, veri tabanı, yazılım, canlı sistemler ve mobil cihazlar gibi alt dalları kapsamaktadır (Sindhu ve Meshram 2012, 196). Mobil cihazlarda adli bilişim kavramı ise Tamma ve Tindall (2015, 3) tarafından “(...) *delil veya verilerin doğru adli bilişim koşulları altında dışarı çıkartılması, kurtarılması ve analiz edilmesi konularıyla ilgili adli bilişim dallarından biridir.*” şeklinde tanımlamaktadır.

Mobil cihazlarda adli bilişim incelemelerinin, adli bilişim tekniklerine ve metodolojilerine uygun olarak yerine getirilmesi oldukça önemlidir (Willassen 2003, 1). Bu kapsamda, mobil cihazlarda gerçekleştirilecek incelemelerde belirli veri elde etme yöntemlerinin kullanılmasına ihtiyaç duyulmaktadır.

1.4. MOBİL CİHAZLARDAN VERİ ELDE ETME YÖNTEMLERİ

Mobil cihazlardan veri elde etme yöntemleri *fiziksel (physical)*, *mantıksal (logical)* ve *manuel* olmak üzere üçe ayrılmaktadır.

Fiziksel elde etme, mobil cihazın tamamının birebir imajının alınmasıyla gerçekleştirilen veri elde etme yöntemidir (Öztürkci 2014, 1). *Fiziksel* veri elde etme yöntemiyle, mobil cihazlardan silinen veriler de dâhil olmak üzere cihaza ait tüm verilere erişim sağlanmaktadır (Mahalik vd. 2016, 23). Anılan yöntemle elde edilen delil, en iyi delil olarak nitelendirilmektedir (Bolat 2015, 28).

Mantıksal elde etme yöntemiyle mobil cihazdaki veriye zarar verilmeden mobil dosya sisteminin *mantıksal* kopyası alınmaktadır (Bader ve Baggili 2010, 5). Dolayısıyla *fiziksel* elde etme yönteminde mobil cihazdaki verinin disk düzeyinde birebir kopyası alınırken, *mantıksal* elde etme yönteminde mobil cihaza ait veriler dosya ve klasör düzeyinde elde edilmekte ve silinen veya tahsis

edilmemiş alanlarda (*Unallocated Disk Space*²²) yer alan bazı veriler tümüyle kurtarılamamaktadır (Holt vd. 2015, 372).

Manuel elde etme, incelemeyi gerçekleştiren uzmanın, mobil cihaza ait tuş takımı veya dokunmatik ekranı kullanarak, cihazın işletim sistemi arayüzü ve menülerinde gezinip elde ettiği dijital delillerin ekran görüntülerini alması yoluyla gerçekleştirdiği veri elde etme yöntemidir (Hoog ve Strzempka 2011, 216). İnsan faktörü ve dijital delillerin silinmesi gibi ihtimaller göz önünde bulundurulduğunda, bu veri elde etme yönteminin oldukça riskli olduğu belirtilmektedir (Mahalik vd 2016, 24).

Yİ'nin durumuna göre mümkünse önce *fiziksel* elde etme yöntemiyle veri elde edilmesine gayret gösterilmelidir. *Fiziksel* veri elde etme yöntemiyle veri elde edilememesi durumunda *mantıksal* veri elde etme yöntemine başvurulmalıdır. *Fiziksel* veya *mantıksal* elde etme yöntemlerinin kullanılamaması durumunda risk faktörleri de göz önünde bulundurularak son çare olarak *manuel* elde etme yöntemi kullanılmalıdır (Casey ve Turnbull 2011, 21).

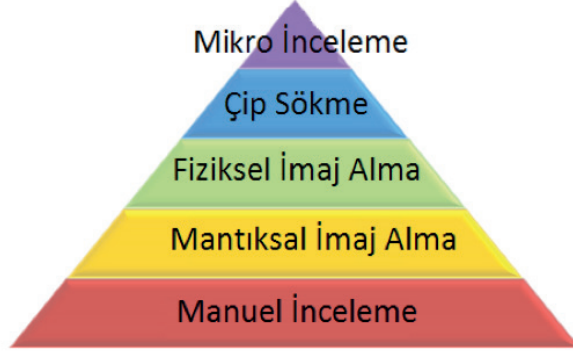
²² Henkoğlu (2014,58) tahsis edilmemiş alanları “(...) işletim sisteminin yazma işlemi yapabileceği, disk üzerindeki boş alanlardır.” olarak tanımlamaktadır.

BÖLÜM 2

MOBİL CİHAZ İNCELEMELERİNDE KULLANILAN ADLİ BİLİŞİM ARAÇLARI ve YERİNDE İNCELEMELER İÇİN SÜREÇ MODELLERİ OLUŞTURULMASI

2.1. MOBİL CİHAZ İNCELEMELERİNDE KULLANILAN ADLİ BİLİŞİM ARAÇLARININ SINIFLANDIRILMASI

Piyasada farklı marka ve modele sahip birçok mobil cihaz bulunmakta olup, bu mobil cihazlara ait işletim sistemleri, uygulamalar, çevresel donanımlar ve servisler farklılaşmaktadır. Mobil cihazlarda adli bilişim incelemelerini gerçekleştirecek uzmanların mobil cihaz dünyasına ek olarak mobil cihazlarda kullanılan adli bilişim araçlarını hazırlayan şirketlerin araçlarına ait gelişmeleri de yakından takip etmeleri zorunlu hale gelmektedir. Ayrıca, incelemeyi gerçekleştirecek olan uzmanın, inceleme süresince hangi aracı hangi aşamada kullanabileceğini bilmesi de gerekmektedir. Bu noktada, adli bilişim araçlarının hangi seviyelerde kullanılabileceğinin tespitinde, adli bilişim uzmanı Sam BROTHERS tarafından mobil cihazlarda kullanılan adli bilişim araçlarına ait sınıflandırma sisteminden yararlanılmaktadır (Bkz. Şekil 3).



Şekil 3: Mobil Adli Bilişim Araçlarının Sınıflandırılması²³ (Brothers 2014, 2)

2.1.1. Manuel İnceleme (Manuel Extraction)

Delillerin, incelenen mobil cihazın tuş takımı veya dokunmatik ekranın kullanılarak ekranda görülen dijital verilerin fotoğraflanmasıyla elde edildiği seviyeye *manuel inceleme* seviyesi denir. (Zareen ve Baig 2010, 51). *Manuel inceleme* teknik bir eğitim gerektirmemekte olup, bu seviyede kullanılan metot ve adli bilişim araçlarıyla silinmiş verilere erişim mümkün olmamaktadır (Hoog ve Strzempka 2011, 11). *Manuel inceleme* seviyesinde *Paraben Project-A-Phone ICD8000*, *Paraben Project-A-Phone Flex*, *Fernico ZRT3* ve *Teel Technologies Eclipse 2* gibi adli bilişim araçları kullanılmaktadır (Reiber, 2016, 134).

2.1.2. Mantıksal İmaj Alma (Logical Extraction)

Mantıksal imaj alma seviyesinde, mobil cihazla adli bilişim iş istasyonu (*Forensics Workstation*) kablolu (*USB*²⁴ veya *RS-232*) veya kablosuz (*WiFi*, *Bluetooth* vb.) olarak birbirine bağlanmaktadır (Ayers vd. 2014, 17). Kurulan bağlantı vasıtasıyla adli bilişim iş istasyonu mobil cihaza belli komutlar göndermekte ve gönderilen komutlarla ilgili dijital deliller mobil cihazdan adli bilişim iş istasyonuna aktarılmaktadır. (Reiber 2016, 129). Bu seviyede yapılan işlemlerle tüm silinmiş verilere erişim sağlanmadığı gibi, veri aktarım işlemi

²³ Sınıflandırma piramidinin alt basamaklarından üst basamaklarına doğru çıkıldıkça yapılan işlemler daha fazla teknik bilgi ve konuyla ilgili eğitim gerektirmekte olup, bahse konu işlemler daha pahalı adli bilişim araçları ve daha uzun süreli analizleri gerektirmektedir (Murphy 2009, 6).

²⁴ *USB*: Universal Serial Bus.

süresince mobil cihazdaki verilerin değişimine de sebebiyet verilebilmektedir (Mahalik vd 2016, 23). Bu seviyede, *Paraben Device Seizure*, *XRY Logical* ve *Cellebrite UFED*²⁵ *Logical Analyzer* gibi adli bilişim araçları yer almaktadır.

2.1.3. Fiziksel İmaj Alma (Hex Dumping / JTAG)

Mobil cihaza *boot loader*²⁶ yüklenerek cihaz hafızasındaki tüm verilerin elde edildiği seviyedir. *Boot loader*, cihazın normal açılış yükleyicisinin yerine geçerek cihazdan veri elde edilmesini sağlamaktadır (Engler ve Miller 2013, 1). *Boot loader* yüklenmesi işlemiyle mobil cihazın dâhili hafızasına erişimi engelleyen güvenlik sistemi atlatılmaktadır (Reiber 2016, 129). Mobil cihazdan elde edilen veri ikili (*binary*) formatta olduğu için, veri üzerinde teknik inceleme yapılması zaruridir. *Hex Dumping* seviyesindeki metotlarla ve adli bilişim araçlarıyla, mobil cihazdan silinen ve cihazın menüsünden erişilemeyen tüm verilere erişim sağlanabilmektedir.

Bu seviyede yer alan bir diğer metot olan *JTAG* (Joint Test Action Group) ile, mobil cihazın işlemcisiyle direkt olarak iletişime geçilerek mobil cihazın tüm kopyası alınmaktadır (Tamma ve Tindall 2015, 166). *JTAG* metodunun kullanılması için özelleştirilmiş donanımlara gereksinim duyulmasının yanı sıra, konuyla ilgili daha detaylı teknik bilgi de gerekmektedir. Bu seviyede, *Cellebrite UFED Touch Ultimate* ve *MSAB XRY Complete* gibi araçlar kullanılmaktadır (Brothers 2014, 13).

2.1.4. Çip Sökme (Chip-Off)

Mobil cihazın hafıza yongasının sökölüp ikinci bir mobil cihaza veya *EEPROM Reader* cihazına takılmasıyla tüm verilerin elde edildiği seviyedir (Zareen ve Baig 2010, 51). *JTAG*'a göre daha pahalı bir metot olan *Chip-Off*, konuyla ilgili özelleştirilmiş donanımlar gerektirmektedir. Metodun karmaşıklığından dolayı *JTAG* daha yaygın olarak kullanılmaktadır (Ayers vd. 2014, 19). Bu seviyede *SD Flash Doctor* ve *UP-828* gibi araçlar yer almaktadır (Brothers 2014, 13).

²⁵ *UFED*: Universal Forensic Extraction Device.

²⁶ *Boot loader*, işletim sistemi başlatılmadan önce çalıştırılan programdır (Tamma ve Tindall 2015, 29).

2.1.5. Mikro İnceleme (Micro Read)

Hafıza yongasındaki verinin elektron mikroskoplarının kullanılmasıyla *manuel* olarak incelendiği oldukça pahalı, detaylı teknik bilgi gerektiren ve pek fazla kullanılmayan bir metottur (Mahalik vd 2016, 23). Hafıza yongaları fiziksel olarak zarar görmüş mobil cihazlar bu metotla incelenebilir. Bu seviyede, çok güçlü mikroskoplar kullanılmaktadır.

2.2. MOBİL CİHAZLARDA ADLİ BİLİŞİM ARAÇLARI

Mobil cihaz teknolojilerinin gelişimiyle birlikte dijital verilerin elde edilmesi, arşivlenmesi, analiz edilmesi ve sunulması gibi konularda görev yapacak adli bilişim araçlarına ihtiyaç artmaktadır (Anobah vd. 2014, 222). Bu ihtiyaca cevap verme noktasında farklı adli bilişim çözümleri üreten şirketler tarafından hazırlanmış olan çeşitli adli bilişim araçları (yazılım / donanım) piyasada yer almaktadır. Mobil cihazlarda kullanılan adli bilişim araçlarında olması gerektiği değerlendirilen özellikler aşağıda sıralanmaktadır. Buna göre adli bilişim aracı;

- Dijital delil elde etme sürecinde veriler üzerinde değişiklik gerçekleştirmemeli ve aracın kullanımıyla elde edilen sonuçlar tekrarlanabilir olmalıdır (Henkoğlu 2014, 43).
- Sunduğu sonuçları doğrulayabilmeli, aynı prosedürler kullanıldığında yine aynı sonuçları verebilmeli ve incelemeyi yapan uzmana gerektiğinde tüm veriye erişim imkânı sağlayabilmelidir (Carrier 2003, 8).
- Değişen teknolojiye uygun çözümleri hızlı bir şekilde sunabilmeli ve farklı işletim sistemlerine (*Android, iPhone, Blackberry, Symbian, Windows Mobile, Meego, Bada* vd.) sahip mobil cihazları desteklemelidir.
- Önemli uygulama (*WhatsApp, Skype, Evernote, Dropbox, Outlook* vb.) verilerine ek olarak cihazda bulunan bulut hesaplarından veri elde edebilmelidir (Hoog ve Strzempka 2011, 216).
- Arama ve gelişmiş filtreleme fonksiyonlarıyla elde edilen sonuçları daraltabilmeli ve farklı formatlarda okunması kolay raporları sunabilmelidir.
- Mobil adli bilişim araçları piyasasındaki mevcut kullanım eğilimleri de

göz önündeki bulundurularak çalışmanın ilerleyen bölümünde, bahse konu araçlar *Cellebrite*, *XRY*, *Paraben*, *Oxygen Forensics* ve *AccessData* başlıkları altında incelenmektedir.

2.2.1. Cellebrite

1999 yılında kurulan *Cellebrite*'a ait adli bilişim çözümleri, kolluk kuvvetleri, istihbarat teşkilatları, özel kuvvetler, sınır devriyeleri, askeri birimler ve özel sektör tarafından 100 ülkede 40.000'den fazla lisansla kullanılmaktadır²⁷. *UFED* (*Universal Forensic Extraction Device*), mobil cihazlardan *fiziksel* ve *mantıksal* veri elde edebilen, *Cellebrite* şirketi tarafından geliştirilmiş bir araçtır (Hayes 2015, 357). Anılan şirkete ait adli bilişim araçları sınıfında aşağıdaki çözümler yer almaktadır:

- *UFED (Universal Forensic Extraction Device) Pro*: Kapsamlı bir mobil veri çıkartma ve çözümleme araçları bütünüdür.
- *UFED Field*: Mobil cihazlar üzerinde sahada inceleme yapılmasını sağlayan araçlar bütünüdür.
- *UFED Analytics*: Mobil cihazlardan elde edilen verileri bilgisayar ortamında incelemeye yarayan yazılımdır. *Desktop* versiyonu sadece tek bir bilgisayarda çalışırken, *Workgroup* ve *Enterprise* versiyonları istemci-sunucu mimarisinde çalışmaktadır.

Ayrıca bahse konu şirkete ait veri çıkartma sınıfında; *UFED Touch2*, *UFED 4PC*, *UFED TK*, *UFED InField Kiosk* ve *UFED Cloud Analyzer* araçları bulunmaktayken, veri çözümleme ve inceleme sınıfında *UFED Physical Analyzer*, *UFED Logical Analyzer* ve *UFED Reader* araçları kullanılmaktadır. Çinli üreticilere ait yonga setlerinden *fiziksel* veri çıkartma işlemi için kullanılan *UFED Chinex* çözümüyle de Çin malı mobil cihazlara destek sağlanmaktadır.

2.2.2. XRY

İsveç merkezli *Micro Systemation (MSAB)* şirketine ait *XRY* adli bilişim çözümleri 100'den fazla ülkede emniyet kuvvetleri, kamu kurumları, askeri birimler, istihbarat servisleri ve adli bilişim laboratuvarları tarafından

²⁷ Bkz. <http://www.cellebrite.com/About-Cellebrite>, Erişim Tarihi: 29.09.2016

kullanılmaktadır²⁸. *XRY* yazılım ve donanımlarıyla mobil cihazlardan *fiziksel* ve *mantıksal* veri elde etme yöntemleriyle veri elde edilebilmektedir (Joshi ve Pilli 2016, 180). *MSAB* şirketine ait adli bilişim çözümleri sınıfında aşağıdaki araçlar yer almaktadır:

- *MSAB Office*: *XRY* yazılım ve donanım çözümlerinin tek bir pakette yer aldığı seridir. *MSAB Office* kullanımıyla, *fiziksel* ve *mantıksal* olarak veri elde edilmekle birlikte buluttan da veri çekilebilmektedir.
- *MSAB Field*: İçerdiği yazılım ve donanımlar saha kullanımına uygun olarak hazırlanmıştır.
- *MSAB Kiosk*: Mobil cihaz takıldıktan sonra 19.5 inç ekrana sahip dokunmatik ekranının kullanımıyla veri çıkartılmasını sağlayan kioskur.
- *MSAB Tablet*: Mobil cihazlardan hızlı bir şekilde veri çıkartılması için kullanılan tablet çözümdür.

Ayrıca veri çıkartma sınıfında *XRY Logical*, *XRY Physical*, *XRY Cloud*, *XRY PinPoint* ve *XRY Camera* araçları; analiz sınıfında *XAMN Viewer*, *XAMN Spotlight* ve *XAMN Horizon* araçları; yönetim araçları sınıfında da *XEC Director* ve *XEC Export* araçları yer almaktadır.

2.2.3. Paraben

1999 yılında kurulan *Paraben*²⁹ şirketi, 2001 yılından bu yana adli bilişim alanında faaliyet göstermektedir. *Paraben's Device Seizure*, mobil cihazlardan veri elde edebilen adli bilişim aracına *Paraben* şirketi tarafından verilen addır (Maras 2015, 344). *Paraben* şirketine ait mobil adli bilişim çözümleri aşağıda yer almaktadır:

- *Paraben's E3:DS*: Farklı mobil cihazlardan *fiziksel* ve *mantıksal* olarak veri çıkartabilme ve analiz edebilme yeteneğine sahip kapsamlı bir adli bilişim çözümdür.
- *Paraben's Mobile Field Kit*: *Paraben's DS*'nin taşınabilir ve sahada

²⁸ Bkz. <https://www.msab.com/company/>, Erişim Tarihi: 11.10.2016.

²⁹ Bkz. <https://www.paraben.com>, Erişim Tarihi: 11.10.2016.

kullanılabilen versiyonudur. Windows tabanlı bir dizüstü bilgisayar, kablolar, mobil cihazlara ait güç seçenekleri ve *Project-A-Phone ICD-8000* içermektedir.

Ayrıca bahse konu şirkete ait mobil cihaz izolasyonunda kullanılan *StrongHold Faraday Protection*, manuel incelemelerde kullanılan *Project-A-Phone* ve *JTAG* ile veri çıkartmada kullanılan *JTAG Analysis Tool* araçları bulunmaktadır.

2.2.4. Oxygen Forensics

Oxygen Forensics adli bilişim araçları, 100'den fazla ülkede emniyet kuvvetleri, kanun uygulayıcılar, askeri birimler, istihbarat servisleri ve özel şirketler tarafından kullanılmaktadır³⁰. *Oxygen Forensics* şirketine ait mobil adli bilişim çözümleri aşağıda sıralanmaktadır:

- *Oxygen Forensic Detective: Mobil cihazlardan veri elde etme ve elde edilen verilerin analizi için sunulan adli bilişim çözümüdür.*
- *Oxygen Forensic Detective Enterprise: Oxygen Forensic Detective'in tüm özelliklerine sahip olmakla birlikte birden fazla bilgisayarda yerel veya uzaktan bağlantı yoluyla çalışabilen adli bilişim çözümüdür.*
- *Oxygen Forensic Kit: Sahada ve laboratuvar ortamında kullanımı için özelleştirilmiş adli bilişim çözümüdür.*

Ayrıca bahse konu şirkete ait araçlar arasında *Oxygen Forensic Analyst*, *Oxygen Forensic Extractor* ve *Oxygen Forensic Viewer* da bulunmaktadır.

2.2.5. AccessData

1987 yılında kurulan *AccessData*'ya ait adli bilişim araçları, şirketler, kamu kurumları ve hukuk firmaları gibi 130.000'den fazla müşteri tarafından kullanılmaktadır³¹. *AccessData*'nın mobil cihazlar konusunda yoğunlaşan *Mobile Phone Examiner Plus (MPE+)* ve *nFIELD* adında iki adli bilişim aracı bulunmaktadır. *AccessData* şirketine ait mobil adli bilişim çözümleri aşağıda sıralanmaktadır:

³⁰ <https://www.oxygen-forensic.com/en/company>, Erişim Tarihi: 11.10.2016.

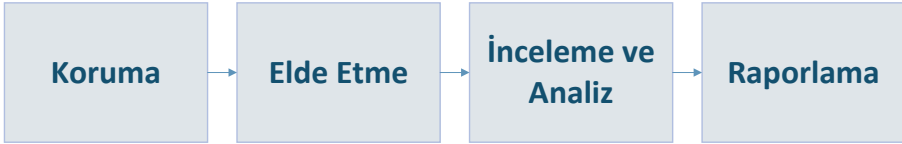
³¹ Bkz. <http://accessdata.com/company>, Erişim Tarihi: 11.10.2016.

- *Mobile Phone Examiner Plus (MPE+)*: Mobil cihazlardan veri çıkartma ve elde edilen verinin analizinde kullanılabilen *AccessData* şirketine ait komple bir adli bilişim çözümüdür (Hosmer 2017, 55).
- *nFIELD*: Sahada çalışan incelemeler için hazırlanmış *AccessData* çözümüdür.

Çalışmanın ilerleyen bölümlerinde yukarıda anılan *Cellebrite*, *XRY* ve *Oxygen Forensics* şirketlerine ait adli bilişim araçlarıyla ilgili detaylı bilgiler örnek olay kapsamında tekrar ele alınacaktır.

2.3. YERİNDE İNCELEMELER KAPSAMINDA SÜREÇ MODELLERİ OLUŞTURULMASI

Mobil cihazlarda adli bilişim incelemelerinin belli bir süreç dâhilinde gerçekleştirilmesi; dijital delil bütünlüğünün bozulmaması, delil zincirinin korunması ve elde edilen dijital delillerle ilgili raporlamanın eksiksiz yapılması adına önem taşımaktadır. Çalışma kapsamında mobil cihazlarda adli bilişim süreçleri dört ana başlık altında incelenecektir³² (Bkz. Şekil 4).



Şekil 4: Mobil Cihazlarda Adli Bilişim Süreçleri

2.3.1. Koruma

Mobil cihazlarda adli bilişim süreçlerinin ilki olan koruma süreci; arama, tanımlama, belgelendirme ve dijital verinin toplanması süreçlerini içermektedir (Ayers vd. 2014, 27). Koruma süreciyle, inceleme mahallindeki dijital verilerin delil bütünlüğünün korunması amaçlanmaktadır (James vd. 2012, 7).

³² Çalışma kapsamında *Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)* tarafından hazırlanan “*Mobil Cihazlarda Adli Bilişim Kılavuzu*” içeriğinde yer alan adli bilişim süreçleri örnek alınmıştır (Ayers vd. 2014, 1). Adı geçen adli bilişim süreçlerinin incelenmesinde Komisyon’un ve Kurum’un mevcut Yİ uygulamaları da göz önünde bulundurulmuştur.

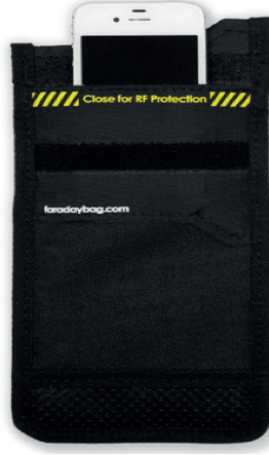
Mobil cihaza takılan çıkarılabilir hafıza kartları, *SIM* kartlar, cihaza ait kablolar, şarj üniteleri ve varsa mobil cihazın bağlandığı bilgisayardaki veriler incelemenin kapsamına girmektedir (Jones ve Valli 2008, 9). Şayet bilgisayar ve mobil cihaz arasında bağlantı veya eşleme işlemi gerçekleştirilmişse kilitli cihazlara erişim için bilgisayardaki verilerden yararlanma hususu da göz önünde bulundurulmalıdır (Ayers vd. 2014, 27). Mobil cihaza girilmiş güvenlik kodları, uygulamalara ait parolalar ve ekran kilitleri (desen, PIN³³ veya şifre) cihaz sahibinden elde edilmeye çalışılmalıdır (Çakır 2014, 388).

Mobil cihaz izolasyonunun sağlanması amacıyla *Faraday* çantaları yaygın olarak kullanılmaktadır (Bkz. Şekil 5). *Faraday* çantası, yapıldığı malzemeyle mobil cihazı dışarıdan gelen radyo dalgaları da dâhil olmak üzere statik elektrik alanlarından korumaya yarayan bir ekipmandır (Mahalik vd. 2016, 16). *Faraday* çantasının kullanılmasıyla cihazın sinyal alması veya vermesi engellenmekte ve mobil cihaz dış dünyadan izole hale getirilmektedir (Croft ve Olivier 2006, 5).

Açık halde bulunan ve kendi iletişim kanallarına bağlantı sağlayan cihazın veri bütünlüğünün değişmesi mümkündür (Reiber 2016, 29). Bu bağlamda, inceleme süresince mobil cihaz, bağlantı sağlayabileceği iletişim kanallarından (*Bluetooth*, *Infrared* (kızılötesi), *WiFi* ve *hücresel ağlar*) izole hale getirilmelidir. İzolasyon neticesinde; cihazın uzaktan kilitlenmesi, cihazdaki verilerin uzaktan silinmesi veya cihazdaki delil bütünlüğünün bozulması gibi durumlara karşı önlem alınmış olması sağlanacaktır³⁴.

³³ Personal Identification Number.

³⁴ *Faraday* ekipmanlarının kullanıldığı, fakat doğru izolasyon şartlarının sağlanmadığı durumlarda cihaz farklı ağlarla iletişim kurabilir ve cihaza ait veri bütünlüğü zarar görebilir.



Şekil 5: Faraday Çantası Örneği³⁵

Faraday çantasının kullanılmasının yanı sıra mobil cihazın radyo şebekeleriyle bağlantısının kesilmesi amacıyla mobil cihaz uçak moduna alınabilir veya cihaz tamamen kapatılabilir. Cihazın kapatılması, cihaza ait kimlik doğrulama kodlarını (*PIN*, *PUK*³⁶, cihaz güvenlik kodları vb.) aktif hale getirebilir. Kimlik doğrulama kodlarının aktif hale gelmesi ise, cihazdan delil elde edilme işlemi zorlaştırabilir ve bu durum inceleme sürecinin uzamasına sebebiyet verebilir. Cihazdan sadece kapatıldığı durumlarda delil elde edilmesi söz konusuysa cihaz tamamen kapatılmalıdır. Aksi hallerde açık durumdaki cihaz kesinlikle kapatılmamalıdır (Çakır 2014, 388).

Koruma süreci kapsamında Yİ'lerde (Yİ konsepti ve adli bilişim teknikleri kapsamında) aşağıdaki adımların izlenilmesinin uygun olacağı değerlendirilmektedir (Bkz. Şekil 6):

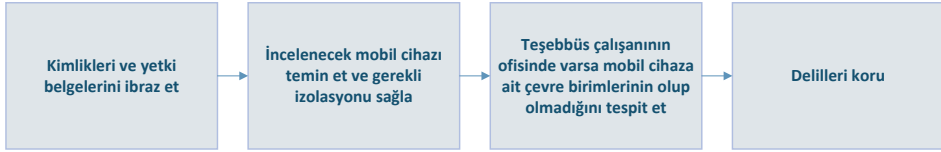
- Teşebbüse öncelikle kimlik ve yetki belgeleri ibraz edilmelidir.
- Teşebbüs çalışanına ait incelenecek mobil cihaz dış dünyadan izole edilmelidir (*Faraday* çantası, uçak modunun açılması vb.).
- Teşebbüs çalışanından mobil cihaza girilmiş güvenlik kodları, uygulamalara ait parolalar ve ekran kilitleri (desen, *PIN* veya şifre)

³⁵ <http://www.disklabs.com/faraday-bags/>, Erişim Tarihi: 30.10.2016.

³⁶ *PUK*: Personal Unlocking Key.

talep edilmelidir. Mobil cihaza ait desen, PIN veya şifrenin teşebbüs çalışanından elde edilememesi durumunda, bahse konu giriş engellerinin adli bilişim araçlarının kullanımıyla aşılması sağlanabilmektedir.

- Teşebbüs çalışanına ait masa, çekmece ve dolap gibi fiziksel saklama bölümlerinde varsa mobil cihaza ait hafıza kartı, *SIM* kart ve veri kablosu tespit edilmelidir.
- Teşebbüs çalışanın mobil cihazını herhangi bir bilgisayarla senkronize edip etmediği tespit edilmelidir.
- Yapılan tüm işlemler dokümente edilmeli, gerekli görülen durumlarda inceleme mahallinin fotoğraflandırılması işlemine başvurulmalıdır.



Şekil 6: Yİ'lerde Mobil Cihazlar İçin Önerilen Koruma Süreci

3.2.3. Elde Etme

Mobil cihazda saklanan dijital delillerin toplandığı süreçtir. Elde etme süreci kapsamında adli bilişim araçlarının kullanılarak mobil cihazdan veri elde edilmesi amaçlanmaktadır.

Bu süreçte, incelenecek cihazla ilgili cihaz üreticisinin markası, modeli, cihaz üzerinde yüklü işletim sistemi, seri numarası, *SIM* kart takılıysa cihaza ait telefon numarası ve *IMEI* (International Mobile Equipment Identity) gibi cihaza ait tüm tanımlayıcı detaylar kayıt altına alınmalıdır (Mahalik vd. 2016, 15).

Mobil cihaz tanımlanırken, cihazla ilgili genel bilgiler varsa kullanma kılavuzlarından, arama motorlarından veya cihaz üreticisinin web sitesinden elde edilmelidir. Cihazın tanımlanma işleminin tamamlanması sonrasında, cihazdan dijital delil elde edilmesi amacıyla hangi adli bilişim aracının kullanılmasının uygun olacağı tespit edilmelidir (Ayers 2014, 37).

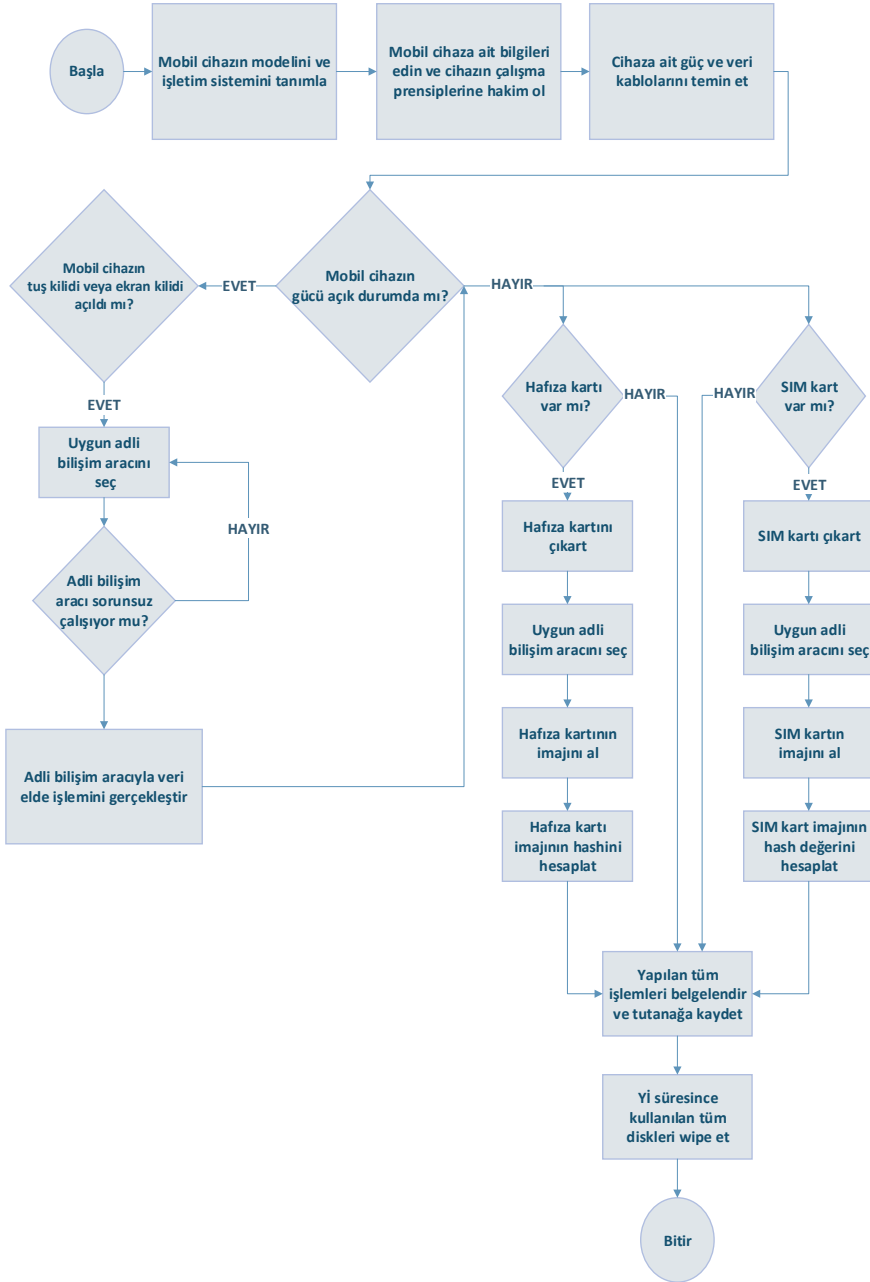
Cihaz incelemesinde kullanılacak adli bilişim araçlarının tespitinden sonra cihazın adli bilişim tekniklerine uygun olarak kopyaları alınmalıdır (Farjamfar vd. 2014, 360). Bazı mobil cihazlar çıkarılabilir hafıza kartları (*microSD* veya *MMC*³⁷) bulundurmaktadır. Çıkarılabilir hafıza kartlarının, yazma korumalı okuyuculara takılarak adli bilişim araçlarıyla kopyaları alınmalıdır. Ayrıca *SIM* kartların da kopyaları, *SIM* kart kopyası almak için özel üretilmiş adli bilişim araçlarıyla elde edilmelidir (Çakır 2014, 390). Cihazdan ve çevre ekipmanlarından adli bilişim tekniklerine uygun olarak kopya alınmasından sonra mutlaka *hash*³⁸ değeri hesaplatılmalıdır (Agarwal vd. 2011, 127). Çalışmaya devam eden bir mobil cihazdan adli bilişim kopyası alınması esnasında, sistemin çalışması ve dolayısıyla mobil cihaz üzerinde değişikliklerin devam etmesi nedeniyle farklı zamanlarda alınan kopyaların *hash* değerleri eşleşmeyecek olup, bu bağlamda tüm inceleme ve değerlendirmeler alınan ilk kopya üzerinden gerçekleştirilmelidir (Özbek 2013, 261).

Elde etme süreci kapsamında Yİ'lerde (Yİ konsepti ve adli bilişim teknikleri boyutuyla) aşağıdaki adımların izlenilmesinin uygun olacağı değerlendirilmektedir (Bkz. Şekil 7) :

- Mobil cihazın modeli ve işletim sistemi tespit edilir.
- Mobil cihazla ilgili detaylı bilgiler, cihaz üreticisinin web sitesinden veya kullanım kılavuzlarından öğrenilir.
- Hangi adli bilişim aracının hangi aşamada kullanılacağı belirlenir.
- Mobil cihazın tuş veya ekran kilidi, güç durumu ve varsa *SIM* kart ve hafıza kartıyla ilgili işlemler göz önünde bulundurularak veri kopyalama işlemi gerçekleştirilir.

³⁷ MMC: Multimedia Card.

³⁸ Henkoğlu (2014, 56) *hash* algoritmasını: “*Hash algoritması, ait olduğu dosya ya da diskin sabit uzunluktaki şifreli özetini oluşturur ve üzerinde çalışılan delil kopyalarının orijinali ile aynı olup olmadığının doğruluğunu ortaya koyar.*” olarak ifade etmektedir.



Şekil 7: Alghaffi vd. (2011, 6) Tarafından Oluşturulan Model Baz Alınarak Tasarlanan Yİ’lerde Mobil Cihazlar İçin Önerilen Elde Etme Süreci

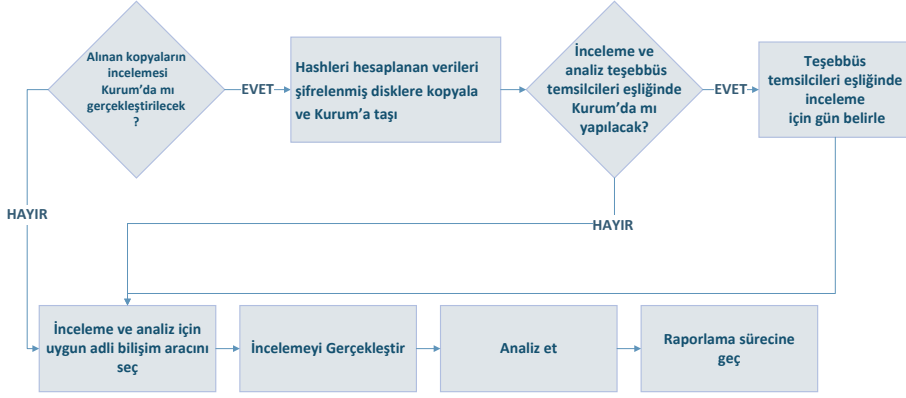
2.3.3. İnceleme ve Analiz

İnceleme ve analiz sürecinde, adli bilişim yazılım ve donanımlarıyla elde edilen mobil cihaz kopyaları üzerinde gerekli inceleme işlemleri gerçekleştirilmektedir (Quick vd. 2013, 18). Bu süreçte, elde edilen verilerin kapsamlı şekilde nasıl inceleneceği konusundaki ayrıntıların aktarılması amaçlanmaktadır.

Mobil cihazlarda gerçekleştirilen tüm incelemeler yasal çerçevede gerçekleştirilmeli (Reiber 2016, 27) ve incelemeden önce hangi adli bilişim araçlarının kullanılacağı incelemenin durumuna göre tespit edilmelidir (Murphy 2009, 7). İnceleme işlemi alınan kopyanın orijinali üzerinde değil, kopyaları üzerinde gerçekleştirilmelidir (Marcella ve Menendez 2007, 378). Böylelikle, incelenen kopyanın orijinalinde değişiklik oluşmasına sebebiyet verilmeyecektir. İnceleme işleminde kullanılması mümkün olan ve veri elde etme konusunda bir diğerine göre daha üstün yönleri bulunan birçok adli bilişim aracı piyasada yer almaktadır.

Mobil cihazdan elde edilen dijital kopyaların incelendiği bu süreçte Yİ'lerde (Yİ konsepti ve adli bilişim teknikleri kapsamında) inceleme ve analiz sürecinde aşağıdaki adımların izlenilmesinin uygun olacağı değerlendirilmektedir (Bkz. Şekil 8):

- Dijital kopyanın incelenmesi aşamasında hangi adli bilişim araçlarının kullanımının uygun olacağı tespit edilir.
- Dijital kopyanın inceleme işlemi gerçekleştirilir.
- Yİ'nin konusunu oluşturan dosya kapsamında yer alabilecek deliller analiz edilerek kişisel ve dosya kapsamında olmayan veriler ayıklanır.
- Dijital kopyaların Kurum'da incelenmesine karar verilen durumlarda, inceleme ve analiz işlemleri Kurum'a ait adli bilişim laboratuvarında gerçekleştirilecekse, *hash* değeri hesaplanan dijital veriler disklere kopyalanır ve alınan *hash* değerleri tutanağa geçirilir.



Şekil 8: Yİ'lerde Mobil Cihazlar İçin Önerilen İnceleme ve Analiz Süreci

2.3.4. Raporlama

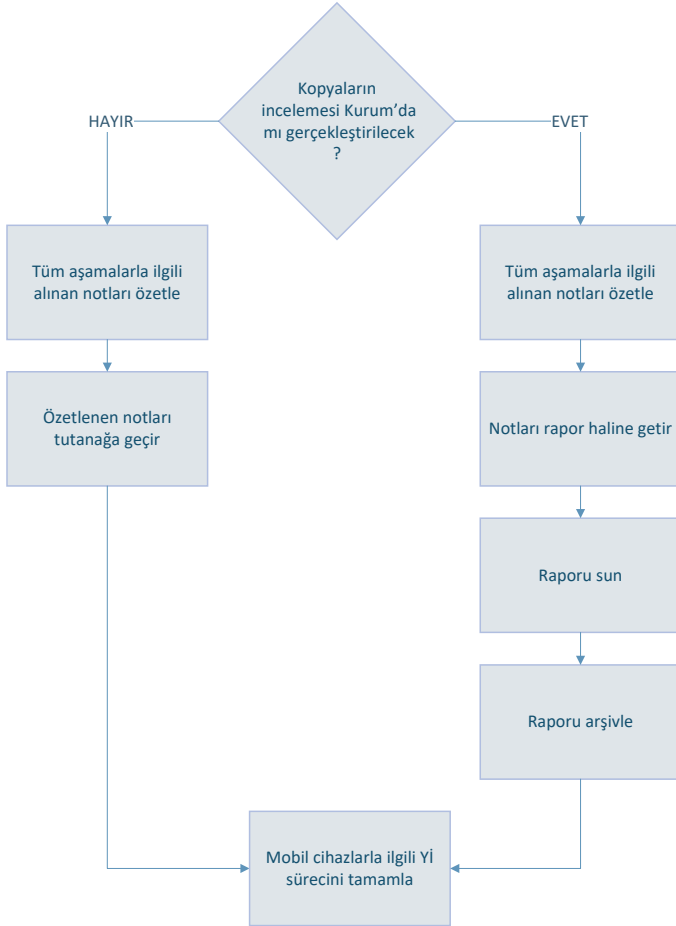
Raporlama işlemi mobil cihaza uygulanan tüm işlemlerin detaylı olarak belgelendirildiği süreçtir (Ayers vd. 2014, 55). Adli bilişim donanımları ve yazılımlarıyla mobil cihazlardan dijital delil elde etme işlemi teknik boyutuyla cihazdan cihaza farklılık gösterebilmektedir. Mahalik vd. (2016, 13)'e göre bu farklılıklara rağmen mobil cihazlarla ilgili yapılan tüm işlemlerin ayrıntılı olarak raporlandırılması ve adli bilişim teknikleriyle elde edilen sonuçların aynı rapor kapsamında tekrar edilebilir ve gerekli görüldüğü durumlarda savunulabilir olması gerekmektedir.

Raporda, yapılan tüm işlemlere ek olarak karşılaşılan sorunlara da yer verilmelidir (Reiber 2016, 28). Bu nedenle, Murphy (2009, 8)'ye göre mobil cihaz üzerinde gerçekleştirilen tüm işlemler tek tek not edilmeli ve bahse konu kayıtlarda ve raporlarda aşağıdaki maddelerde yer alan içerikler bulunmalıdır:

- İncelemenin başlatıldığı tarih ve saat,
- Telefonun fiziksel durumu,
- Telefona ait her bir bileşenin resimleri (SIM kart, harici hafıza kartı vb.),
- Telefonun açık veya kapalı olma durumu,
- Marka, model ve tanımlayıcı bilgiler,
- Kullanılan adli bilişim araçları,
- İnceleme süresince belgelendirilen dijital deliller.

Raporlama süreci özelinde Yİ'lerde (Yİ konsepti ve adli bilişim teknikleri kapsamında) aşağıdaki adımların izlenilmesinin uygun olacağı değerlendirilmektedir (Bkz. Şekil 9):

- Yİ süresince mobil cihazla ilgili yapılan ve tek tek kayıt altına alınan işlemler öncelikle özetlenir.
- Özetlenen işlemler tutanağa geçirilir.
- Mobil cihazla ilgili Yİ süreci tamamlanır.



Şekil 9: Yİ'lerde Mobil Cihazlar İçin Önerilen Raporlama Süreci

2.4. YERİNDE İNCELEMELERDE MOBİL CİHAZ İNCELEMELERİNİ ZORLAŞTIRMASI MUHTEMEL ETMENLER

Mobil cihazların donanım ve yazılımları, cihazlardaki teknolojik gelişimle birlikte her geçen gün farklılaşmaktadır. Bununla birlikte cihazların farklı işletim sistemlerine, kablolar, güvenlik giriş engellerine, şifreleme düzeylerine sahip olmaları da incelemeleri zorlaştırmaktadır (SWGDE 2013, 4). Bu noktada, Yİ'lerde mobil cihaz incelemelerini zorlaştırması muhtemel faktörler aşağıda sıralanmaktadır:

- **Donanım Farklılıkları:** Çeşitli marka, model, donanım, özellik ve işletim sistemine sahip çok sayıda mobil cihaz piyasada yer almakta ve her geçen gün yeni mobil cihazlar, marka sahipleri tarafından piyasaya sürülmektedir (Mahalik vd. 2016, 11). Bu bağlamda, piyasaya sürülen her bir mobil cihazdan veri elde edilmesiyle ilgili adli bilişim tekniklerine uygun metotlar geliştirilmelidir. İncelencek mobil cihazın doğru tanımlanamadığı durumlarda, cihazdan veri elde edilmesi de zorlaşmaktadır (Dashti vd. 2013, 26). Ayrıca incelemeyi gerçekleştirecek bilgi teknolojileri konusunda uzman meslek personelinin cihazlarla ilgili bilgilerini düzenli olarak güncellemeleri gerekmektedir.
- **Mobil İşletim Sistemi Farklılıkları:** *Android, iOS, Blackberry OS, Symbian OS, Windows Phone OS* ve *webOS* gibi farklı mobil işletim sistemleri piyasada bulunan cihazlarda yer almaktadır. İşletim sistemlerinin ve versiyonlarının farklılaşması, incelemeyi zorlaştıran etmenler arasında yer almaktadır (Engler ve Miller 2013, 1).
- **Mobil Cihazdaki Verinin Korunması:** Mobil cihazın kapalı durumdan açık hale getirilmesi veya bir uygulamanın açılması dahi mobil cihaz üzerindeki verilerin değişimine sebebiyet verebilmektedir. Mobil cihazlardan veri elde edilirken, veri elde edilen cihaz üzerindeki verinin değişmemesini sağlamak pratikte mümkün olmamaktadır (Tamma ve Tindall 2015, 10).

- **Farklı Adli Bilişim Araçlarına Bağımlılık:** Mobil cihaz dünyasında farklı özelliklere sahip pek çok adli bilişim aracı bulunmakta ve tek bir adli bilişim aracının bütün cihazları desteklememesi durumu söz konusu olabilmektedir (Davydov 2014, 1). Bu nedenle bazı incelemelerde birden fazla adli bilişim aracının kullanılmasının gerekli olabileceği göz önünde bulundurulmalıdır.
- **Mobil Cihaz Güvenlik Önlemleri:** Bazı yeni nesil mobil cihazlar ön tanımlı olarak şifrelenmiş halde piyasaya sürülmektedir. Ayrıca kullanıcılar mobil cihazlarını ekran kilitleriyle (desen, *PIN* veya şifre) de korumaktadırlar (Çakır 2014, 387). Mobil cihazdan veri elde edilebilmesi için bu güvenlik önlemlerinin aşılması gerekmektedir.

BÖLÜM 3

MOBİL CİHAZLARIN ADLİ BİLİŞİM ARAÇLARIYLA İNCELENMESİ

Önceki bölümlerde verilen kavram ve prosedürlerin belirli noktalarda detaylandırılması ve mobil adli bilişim araçlarının Yİ'lerden nasıl kullanılabileceğinin araştırılması adına Tablo 3'te yer alan hayali teşebbüsler ve teşebbüs çalışanları tasarlanmış ve hayali teşebbüs çalışanları arasında iletişim kayıtları oluşturularak örnek bir olay kurgulanmıştır.

<i>Teşebbüs Adı</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
Teşebbüs Çalışanı Adı	Xpersonel	Ypersonel	Zpersonel

Tablo 3: Örnek Olay Kapsamında Oluşturulan Teşebbüsler ve Çalışanları

3.1. ÖRNEK OLAY

Sanal gerçeklik gözlüğü sektöründe faaliyet gösteren *X*, *Y* ve *Z* teşebbüsleri ilgili sektörde rekabet etmektedir. Sektördeki aktif rekabet, nihai satış fiyatlarını düşürerek *X*, *Y* ve *Z* teşebbüslerinin karlılık oranlarını 2014, 2015 ve 2016 yıllarına göre oldukça azaltmıştır.

Sektör birliği çatısı altında yapılan toplantılarda, müşteri ve bölgelerin paylaşılmasından sonra nihai satış fiyatının belirlenmesinin ve gerekirse arz miktarının tespit edilen oranlarda kısıtlanmasının kararı alınmıştır. Bu kapsamda *X* teşebbüsü Kurumsal Satış Direktörü *Xpersonel*, *Y* teşebbüsü Satış Koordinatörü *Ypersonel* ve *Z* teşebbüsü Pazarlama Müdürü *Zpersonel* anlaşmayı sağlamak adına kendi teşebbüsleri tarafından görevlendirilmişlerdir. Yapılan toplantıda anlaşma

koordinatörü olarak sektörde en yüksek pazar payına sahip *X* teşebbüsünün Kurumsal Satış Direktörü *Xpersonel* seçilmiştir.

Anlaşma kapsamında belirli aralıklarla bir araya gelen teşebbüs çalışanları sadece teşebbüslerince verilen mobil cihazları kullanarak iletişime geçmişler ve rekabet ihlallerini saklamak adına iletişimlerinde kesinlikle kurumsal e-posta adreslerini veya uygulamalarını kullanmamışlardır.

X teşebbüsünün, teşebbüsler arasında yapılan anlaşmaya aykırı hareketleri nedeniyle, *Z* teşebbüsü “Kartellerin Ortaya Çıkarılması Amacıyla Aktif İşbirliği Yapılmasına Dair Yönetmelik (Pişmanlık Yönetmeliği)³⁹” kapsamında Kurum’a pişmanlık başvurusunda bulunmuştur. *Z* teşebbüsünün pişmanlık başvurusu sürecinde sunduğu bilgi ve belgeler üzerine *X*, *Y* ve *Z* teşebbüslerinde meslek personeline eş zamanlı Yİ’ler gerçekleştirilmiştir. Çalışmadaki veriler, *Xpersonel*’in cihazından elde edilen verilerdir.

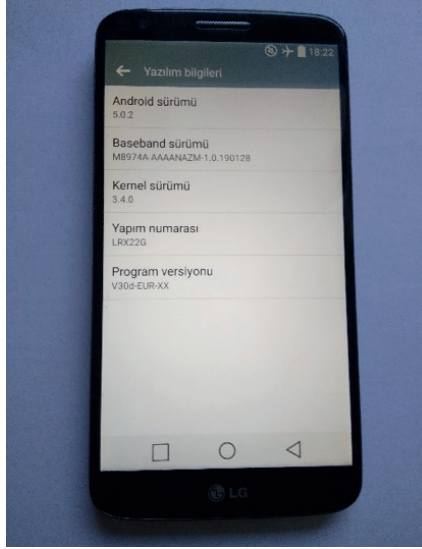
3.1.1. Araştırma Yöntemi ve İncelenen Mobil Cihaz

Adli bilişim araçlarıyla incelenecek mobil cihazın *fiziksel* ve *mantıksal* yöntemlerle imajı alınmıştır. Alınan imajlardan elde edilen sonuçlar belli başlıklar altında irdelenmiş ve genel değerlendirme aşamasına geçilmiştir.

Örnek olay kapsamında *Android 5.0.2* işletim sistemi yüklü *LG G2 D802 4G LTE 32 GB* modeline sahip akıllı telefonda⁴⁰ incelemeler gerçekleştirilmiştir (Bkz. Şekil 10). Adli bilişim araçlarının yeni işletim sistemlerine destek verme süreçlerinin belli bir zaman aralığı gerektirmesi (Tassone vd. 2013, 2) nedeniyle anılan cihaz, piyasaya çıktığı tarih ve işletim sisteminin yaşı da göz önünde bulundurularak inceleme için uygun görülmüştür.

³⁹ Bkz. [http://www.rekabet.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fnel+%C4%B0%C3%A7erik%2fyonetmelik8+\(1\).pdf](http://www.rekabet.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fnel+%C4%B0%C3%A7erik%2fyonetmelik8+(1).pdf), Erişim Tarihi: 11.02.2017.

⁴⁰ Mobil cihazda; *Microsoft Outlook*, *Word* ve *Excel*, *Gmail*, *Google Haritalar*, *Chrome Tarayıcı*, *Hangouts*, *HERE WeGO*, *WhatsApp Messenger* uygulamalarıyla veri üretilmiştir.



Şekil 10: LG G2 D802 4G LTE

3.1.2. Cihazın Fabrika Verilerine Sıfırlanarak İncelenmeye Hazırlanması

Cihazın fabrika verilerine sıfırlanması, cihazın fabrikadan çıktığı haline getirilmesi işlemidir (Huddleston 2012, 219). Bu işlemle cihazdaki ayarlar, kullanıcı verileri, uygulamalar ve uygulamalara ait veriler cihazın dâhili hafızasından silinir (Soper 2015, 590). Cihazın fabrika verilerine sıfırlanması işleminden sonra cihaz üzerinde bazı verilerin kalması söz konusu olabilir (Schwamm ve Rowe 2014, 218). Ayrıca bu işlem sonrasında cihazın dâhili hafızasında kalan verilerin kurtarılması durumu da söz konusudur (Simon ve Anderson 2015, 1). İncelemede kullanılan mobil cihazın dâhili hafızası tamamen şifrelendikten (*Full disk encryption*)⁴¹ sonra cihaz fabrika verilerine sıfırlanmıştır.

Cihazın dâhili hafızasının tamamen şifrelenmesi ve fabrika verilerine sıfırlanması işlemleriyle, cihazdaki eski verilerin kısmen de olsa silinmesi ve sadece rekabet ihlaliyle ilgili verilerin ortaya çıkarılması amaçlanmaktadır.

3.1.3. Örnek Olay Kapsamında Oluşturulan Veriler

Ypersonel ve *Zpersonel* çalışmanın bu bölümünde diğer teşebbüs çalışanları olarak ifade edilecek olup, *Xpersonel*'in mobil cihazında oluşturulan ve rekabet

⁴¹ *Full-Disk Encryption: Android* işletim sistemi yüklü cihazdaki tüm kullanıcı verilerinin şifreli bir anahtar kullanılarak şifrelenmesi anlamına gelmektedir (Dubey ve Misra 2013, 168).

ihlalinin varlığına işaret eden hususlar şunlardır:

- **Arama Kayıtları:** Diğer teşebbüs çalışanları toplamda on kez aranmış ve arama kayıtlarının üçü silinmiştir.
- **SMS:** Diğer teşebbüs çalışanlarına “toplantı, anlaşma ve fiyat tespiti” anahtar kelimelerini içeren beş SMS gönderilmiş ve SMS’lerin üçü silinmiştir.
- **E-posta:** Diğer teşebbüs çalışanlarına “fiyat tespiti, toplantı yeri, sözleşme şartları” gibi konu başlıklarını içeren yedi e-posta gönderilmiş, buna karşılık beş e-posta alınmıştır. E-postaların ikisi silinmiştir.
- **Web Tarayıcı Geçmişi:** Kartel toplantısının yapılacağı yerin seçimi adına web tarayıcısında “en iyi oteller, en iyi toplantı salonları, en yüksek puana sahip restoranlar” kelime veya kelime grupları aranmıştır.
- **Fotoğraf ve Videolar:** Toplantı tutanaklarının dört adet fotoğrafı çekilmiş ve fotoğraflardan biri silinmiştir.
- **Haritalar:** Harita uygulamalarından “otel, toplantı salonu, restoran, Rekabet Kurumu” kelimeleri aranmıştır.
- **Elektronik Belgeler:** Cihazda, teşebbüsler arasında kurulan kartelle ilgili beş *Microsoft Office Word*, iki *Microsoft Office Excel*, bir adet *Microsoft Office Powerpoint* uzantılı elektronik belgeyle ilgili işlem yapılmıştır.
- **Anlık Mesajlaşma Uygulamaları:** *WhatsApp* uygulaması üzerinden “VR Gözlük Grubu” isimli *WhatsApp* grubu oluşturulmuş, bu gruptan diğer teşebbüs çalışanlarıyla yazışmalar gerçekleştirmiş, gruptaki bazı mesajlar silinmiştir. Buna ek olarak *WhatsApp* grubundan çıkılmış ve bahse konu grup silinmiştir. Ayrıca *Google Hangouts* üzerinden ihlale konu olabilecek yazışmalar gerçekleştirilmiştir.
- **Ses Kaydı:** Toplantılarda üç tane ses kaydı alınmış, bu ses kayıtlarından biri silinmiştir.

3.2. İNCELEME ORTAMI VE KULLANILAN ADLİ BİLİŞİM ARAÇLARI

İnceleme kapsamında *Windows 10 Enterprise 1607* sürümü yüklü *Intel(R) Core(TM) i7-3520M @3.30GHz* işlemci, *16 GB DDR3 1333MHz* bellek ve *500 GB Samsung SSD 850 EVO* sabit diskli bilgisayarda, *XRY Version 7.1*, *UFED Physical Analyzer 5.4.0.203* ve *Oxygen Forensics Detective 9.0.2.106* adli bilişim araçlarının yazılımları⁴² kurularak inceleme işlemi gerçekleştirilmiştir⁴³.

3.2.1. XRY

İncelemede *XRY*'in *Office* versiyonu kullanılmıştır. *XRY*'a ait donanım inceleme bilgisayarına bağlandıktan sonra, incelenecek cihazın marka ve modeli *XRY* arayüzünden seçilmiş ve sonrasında *XRY* donanımı kullanılarak cihazdan kopyalar (*fiziksel* ve *mantıksal*) elde edilmiştir. Cihazın kapalı şekilde bağlanması nedeniyle ekran kilidinin geçilmesine gerek kalmamıştır. Bunun yanı sıra *mantıksal* veri elde etme yöntemi kullanılırken *agent* metodu seçilerek incelenen mobil cihaz ayarlarında fazla değişiklik⁴⁴ yapılmadan *mantıksal* kopya elde edilmiştir. Yapılan testlerde⁴⁵ *fiziksel* veri elde etme yöntemiyle veri elde edilmesi ve elde edilen verinin işlenmesi ortalama 2 saat 15 dakika sürerken, *mantıksal* veri elde edilmesi ve verinin işlenmesi ortalama 24 dakikada tamamlanmıştır. Cihazın kopyalarının *XRY Office* kullanılarak alınması için kurulan sistem Şekil 11'de yer almaktadır.

⁴² Adli bilişim araçlarının farklı veri değerlendirme algoritmaları kullanmaları nedeniyle adli bilişim araçlarından elde edilen sonuç tablolarındaki sayılar farklılık gösterebilir.

⁴³ Yukarıda adı geçen üç adli bilişim aracı temin edildiği için incelemede kullanılmıştır.

⁴⁴ *Mantıksal* veri elde yönteminde cihazda yapılan değişikliklere örnek olarak; *USB* hata ayıklamanın açılması, ekran kilidinin kaldırılması, ekran açıklık süresinin en yüksek süreye getirilmesi ve uygulamaların *USB* üzerinden doğrulanmaması gibi manuel yapılan işlemler gösterilebilir.

⁴⁵ Her veri elde yöntemi ikiye kez uygulanmış ve ortalamalar alınmıştır. *Fiziksel* incelemede *SQLite* verisi tahsis edilmemiş alanlarda araştırılmıştır. Bu seçeneğin seçilmediği durumlarda inceleme süresi 1 saat 15 dakikaya kadar düşmektedir. Sürelerin, donanıma ve kullanılan yazılımlara göre değişiklik gösterebileceği dikkate alınmalıdır.



Şekil 11: XRY Office Kullanılarak Cihazın Kopyalarının Alınması

XRY donanımı kullanılarak elde edilen veriler *XRY Reader* yazılımı aracılığıyla incelenmiştir (Bkz. Şekil 12).

FLASH	Subject	Summary	Text	Sent	Related Application: Gmail
SUMMARY	Fiyat tespiti	Arkadaşlar merhaba, ne yazık ki fiyat tespiti...	<p dir="ltr">Arkadaşlar merhaba, ne yazık ki fiyat tespiti...	16.11.2016 19:15:41 U	Subject: Toplantı yeri 28.11.2016 - 11.00 https://www.google.com/maps/d/viewer?mid=1Ez...
CASE DATA	Rekabet Kurumu Faaliyetleri	Rekabet Kurumu'nun...	<p dir="ltr">Rekabet Kurumu'nun...	16.11.2016 19:20:24 U	Text: View as Text View Source View as HTML Save as a file
DEVICE	teşebbüs fiyat çalışması		<div dir="ltr"> </div>	18.11.2016 11:25:37 U	Toplantı yeri 28.11.2016 - 11.00 https://www.google.com/maps/d/viewer?mid=1EzSJFv0AbN4MchQ8Kroy2VXy4d4&hl=en_US&ll=39.88377500000003%2C32.75401796834321&z=21
CONTACTS	teşekkürler	Merhaba, Fiyat sabitleme konulu...	<div dir="ltr">Merhaba, 	29.11.2016 08:34:01 U	Sent: 28.11.2016 07:49:35 UTC
CALLS	sözleşme ve toplantı...		<div dir="ltr"> </div>	28.11.2016 07:55:10 U	Received: 28.11.2016 07:49:35 UTC (Network)
MESSAGES	sözleşme şartları	Lorem Ipsum Nedir? Lorem...	<div dir="ltr"><div style="margin:5px; 14.3906px...	28.11.2016 07:51:02 U	Device
SMS	Toplantı yeri	Toplantı yeri 28.11.2016 - 11.00	<div dir="ltr">Toplantı yeri 28.11.2016 - 11.00</div> </div>	28.11.2016 07:49:35 U	From: Xpersoneel Xpersoneel
MMS	Toplantı yeri	Toplantı yeri 28.11.2016 - 11.00	<div dir="ltr">Toplantı yeri 28.11.2016 - 11.00</div> </div>	28.11.2016 07:49:35 U	Display Name: tez.xpersoneel@gmail.com
EMAILS	fiyat tespiti	Ankara 200 İstanbul 240 olarak revize...	<div dir="ltr"> 	28.11.2016 07:47:49 U	Address: Xpersoneel Xpersoneel
CHAT	VR		<div dir="auto"></div>	30.11.2016 12:55:48 U	Name (Matched): tez.xpersoneel@gmail.com
LOCATIONS	F			16.11.2016 19:15:41 U	To: tez.xpersoneel@gmail.com
HISTORY	Outlook Uygulamasını...	Outlook: her şeyi tek bir...		16.11.2016 20:49:32 U	Name (Matched): tez.xpersoneel@gmail.com
BOOKMARKS	bumalsilmiştir		<div dir="ltr">bumalsilmiştir</div>	30.11.2016 12:41:15 U	Name (Matched): tez.xpersoneel@gmail.com
WEB					To: tez.xpersoneel@gmail.com
FILES					Address: tez.xpersoneel@gmail.com
SYSTEM					Name (Matched): tez.xpersoneel@gmail.com
TAGS					Related Account: tez.xpersoneel@gmail.com
					GMail ID: tez.xpersoneel@gmail.com

Şekil 12: XRY Reader Arayüzü

XRY dan elde edilen verilerin yer aldığı Tablo 4 incelendiğinde, mobil cihazdan *fiziksel* veri elde etme yöntemiyle daha fazla veri elde edildiği görülmektedir. Silinen verilerin bulunması hususunda *fiziksel* veri elde etme yöntemi bir adım öne

çıkmakta, fakat inceleme süresi artmaktadır. Bu bağlamda, Yİ’lerde kritik öneme sahip teşebbüs çalışanlarının mobil cihazlarından *fiziksel* veri elde yöntemiyle, daha az öneme sahip teşebbüs çalışanlarının mobil cihazlarından zamandan tasarruf sağlamak amacıyla *mantıksal* veri elde yöntemiyle veri elde edilmesinin daha uygun olacağı değerlendirilmektedir.

<i>Kriter</i>	<i>Fiziksel (ortalama 2 saat 15 dk.)</i>		<i>Mantıksal Agent (ortalama 24 dk.)</i>	
	Toplam	Silinen	Toplam	Silinen
Arama Kayıtları	144	2	142	0
SMS	214	127 ⁴⁶	87	0
E-Posta	12	3	0	0
Web Tarayıcı Geçmişi	39637	37444	0	0
Fotoğraflar	87756	83960	559	0
Videolar	38	27	22	0
Ses Dosyaları	348	65	435	0
Elektronik Belgeler	2112	374	380	0
WhatsApp	794	127	0	0
Adres Defteri	137	38	34	0
Ağ Bilgileri	804	0	0	0
Hangouts	0	0	0	0
Veri Tabanları	373	9	0	0
Cihaz Konumları	3	0	0	0
Yüklü Uygulamalar	199	0	199	0

Tablo 4: XRY’den Elde Edilen Veriler

3.2.2. Cellebrite UFED Touch ve Physical Analyzer

İncelemenin *Cellebrite* araçları kısmı, *Cellebrite UFED Touch Version 5.4.0.853* ve *Physical Analyzer 5.4.0.203* versiyonları kullanılarak gerçekleştirilmiştir⁴⁷. İncelenen cihaz *UFED Touch*’a bağlanmış ve *UFED Touch*’dan elde edilen veriler *Physical Analyzer* kullanılarak incelenmeye hazır hale getirilmiştir.

⁴⁶ Silinmiş olarak işaretlenen *SMS* verilerinin *Android* sistem mesajları olduğu tespit edilmiştir.

⁴⁷ Çalışmada *Cellebrite* araçları *UFED* olarak adlandırılacaktır.

Cihazın *fiziksel* kopyası *boot loader* yöntemiyle alınmış ve cihazın kapalı şekilde bağlanması nedeniyle ekran kilidinin geçilmesine gerek kalmamıştır. *Mantıksal* kopyada, incelemeyi gerçekleştiren kullanıcının dilediği veriyi (*Adres defteri, SMS, e-postalar, uygulama verileri* vd.) çekebileceği görülmüştür⁴⁸. *XRY*'a benzer şekilde, *mantıksal* veri elde yönteminde de cihazda manuel değişiklik yapılması söz konusudur. Yapılan testlerde⁴⁹ *fiziksel* veri elde etme yöntemiyle veri elde edilmesi ve elde edilen verinin işlenmesi 1 saat 50 dakika sürerken, *mantıksal* veri elde edilme süresi 27 dakika olarak tespit edilmiştir. UFED Touch kullanılarak cihazın kopyaları Şekil 13'teki sistem kurularak alınmıştır.



Şekil 13: UFED Touch'la Cihazın Kopyalarının Alınması

⁴⁸ Cihazdan verilerin seçilerek alınması metodunun, incelenecek veri miktarının düşürülmesi nedeniyle Yİ'lerde zaman tasarrufu bakımından fayda sağlayacağı değerlendirilmektedir.

⁴⁹ Her veri elde yöntemi ikişer kez uygulanmış ve ortalamalar hesaplanmıştır. Sürelerin donanım ve kullanılan yazılımlara göre değişiklik gösterebileceği dikkate alınmalıdır.

UFED Physical Analyzer kullanılarak elde edilen veriler Tablo 5’de yer almaktadır.

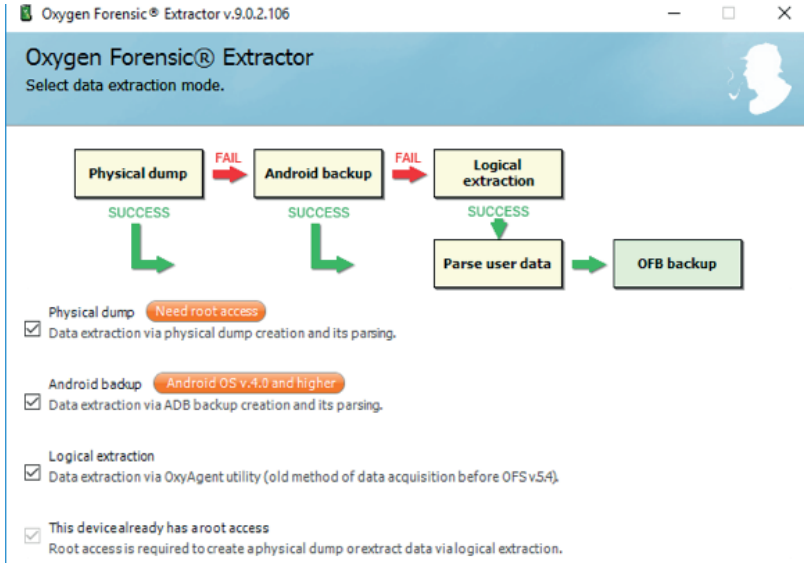
<i>Kriter</i>	<i>Fiziksel (ortalama 1 saat 50 dk.)</i>		<i>Mantıksal (ortalama 27 dk.)⁵⁰</i>	
	Toplam	Silinen	Toplam	Silinen
Arama Kayıtları	146	4	142	4
SMS	87	0	87	0
E-Posta	28	7	16	7
Web Tarayıcı Geçmişi	2128	1	2064	1
Fotoğraflar	4112	23	2660	0
Videolar	11	0	12	0
Ses Dosyaları	148	2	21	0
Elektronik Belgeler	37	3	1	0
WhatsApp	687	2	687	2
Adres Defteri	114	5	21	2
Aranan Metinler	231	0	211	0
Hangouts	13	0	0	0
Veri Tabanları	338	0	208	0
Cihaz Konumları	4004	26	412	1
Baz İstasyonları	2801	0	289	0
Yüklü Uygulamalar	2187	147	45	0
Timeline	8622	0	5083	0

Tablo 5: UFED Physical Analyzer Kullanılarak Elde Edilen Veriler

⁵⁰ İkinci kopya (*duplicate*) verileri sayılmamıştır.

3.2.3. Oxygen Forensics Detective

Oxygen Forensics Detective (OFD⁵¹) adlı bilişim aracı kullanılarak cihazın *fiziksel* ve *mantıksal kopyaları* sadece yazılım kullanılarak elde edilmiştir. *OFD* ile donanım kullanılmadan yazılım düzeyinde kopya elde edilmesi, cihazın manuel olarak rootlanması ve cihazdan kopya elde etme sürelerinin tam olarak ölçülememesi gibi nedenlerden ötürü çalışmanın bu bölümünde diğer adli bilişim araçlarıyla karşılaştırma yapılmamış, sadece *OFD* yazılımının *Analytics* özelliği üzerinde durulmuştur. *OFD*'nin cihazdan *fiziksel* veri elde etme yöntemiyle veri elde edememesi nedeniyle cihaz manuel olarak *rootlanmış*⁵² ve *fiziksel* kopya *rootlanmış* cihazdan elde edilmiştir⁵³. Çalışmada *OFD*'nin *Analytics* bölümünden faydalanılmıştır.



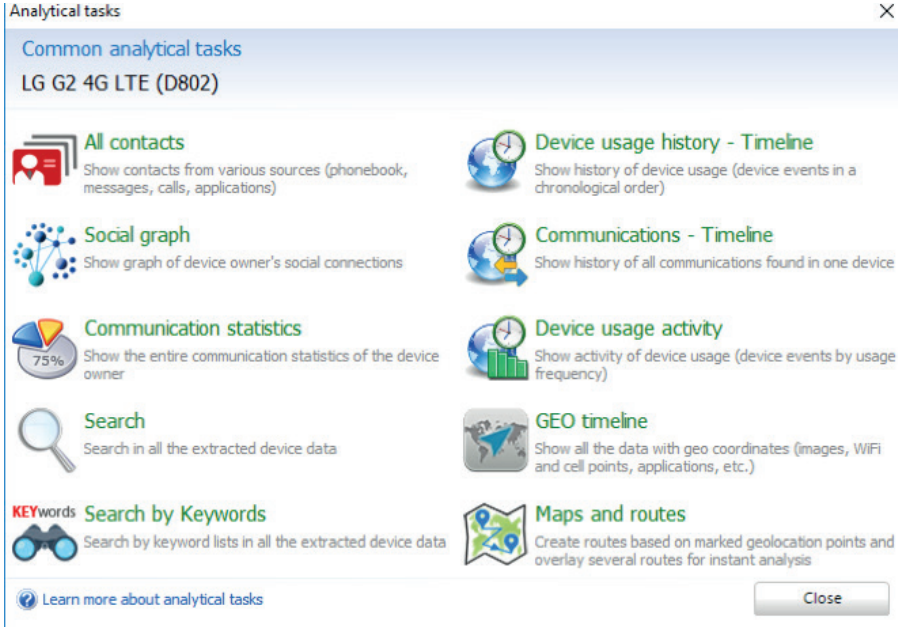
Şekil 14: OFD Veri Elde Etme Ekranı

⁵¹ Çalışmada *Oxygen Forensics Detective* aracı *OFD* olarak adlandırılacaktır.

⁵² Root işlemi için *LG One Click Root* kullanılmıştır.

⁵³ Ayrıca *OFD* kullanılarak *Android Backup* ve *mantıksal* veri elde etme yöntemleriyle de veri elde edilmesi mümkündür.

OFD'nin *Analytics* bölümü, incelemeyi gerçekleştiren uzmanlara, elde edilen bulgularla ilgili analiz ekranları sunmaktadır. Analiz ekranlarında; farklı kaynaklardan elde edilen tüm iletişim kayıtlarına, cihaz sahibinin sosyal bağlantılarına, konum bilgisi analizlerine, cihaz kullanım geçmiş bilgilerine ve anahtar kelime arama bölümlerine erişmek mümkün olmaktadır (Bkz Şekil 15).



Şekil 15: OFD Analytics Seçenekleri

3.3. REKABET İHLALİNE YÖNELİK İNCELEME SONRASINDA ELDE EDİLEN BULGULAR

Çalışmanın bu bölümünde, tez kapsamında incelenen test cihazında oluşturulan veriler adli bilişim araçlarıyla incelenmiş ve bulgular raporlanmıştır⁵⁴. Bu kapsamda ilk olarak cihazda kurulu uygulamalarla (*application*) ilgili bilgiler⁵⁵ aktarılmış, sonrasında adli bilişim aracından elde edilen bulgular rekabet ihlali boyutuyla değerlendirilmiştir.

⁵⁴ Çalışmada görüntü yeknesaklığının sağlanması amacıyla, *UFED Reader*'in arayüzünden elde edilen ekran görüntüleri tercih edilmiştir.

⁵⁵ Çalışmanın *Android* yüklü bir mobil cihazda gerçekleştirilmesi nedeniyle, aktarılan bilgiler *Android* işletim sistemiyle ilgili olacaktır.

Uygulama geliştiricilerinin, uygulamalarını düzenli olarak güncelleştirmeleri ve aynı uygulamanın farklı versiyonlarının verileri farklı yerlerde depolanması gibi durumlar nedeniyle, çalışma kapsamında kullanılan adli bilişim tekniklerinin uygulamaların farklı versiyonlarında geçersiz kalması söz konusu olabilmektedir (Tamma ve Tindall 2015, 192). Adli bilişim araçlarının veri elde etme performanslarının, aracın yazılım ve donanım sürümüne, incelenen mobil cihazın markasına ve modeline, cihazdaki işletim sistemi sürümüne ve yüklü uygulamaların versiyonlarına göre değişiklik gösterebileceği de göz önünde bulundurulmalıdır.

3.3.1. WhatsApp Messenger

WhatsApp Messenger (WhatsApp) ülkemizde de oldukça yaygın şekilde kullanılan ve kullanıcılarına hızlı ve kolayca mesajlaşma ve arama yapma özelliklerini sunan anlık mesajlaşma uygulamasıdır⁵⁶. *Android*'de *com.whatsapp* paket adına sahip uygulamanın çalışmada incelenen sürümü 2.16.352'dir. *WhatsApp*'la elde edilen veriler, *msgstore.db* ve *wa.db* adıyla iki *SQLite*⁵⁷ veri tabanından elde edilmiştir.

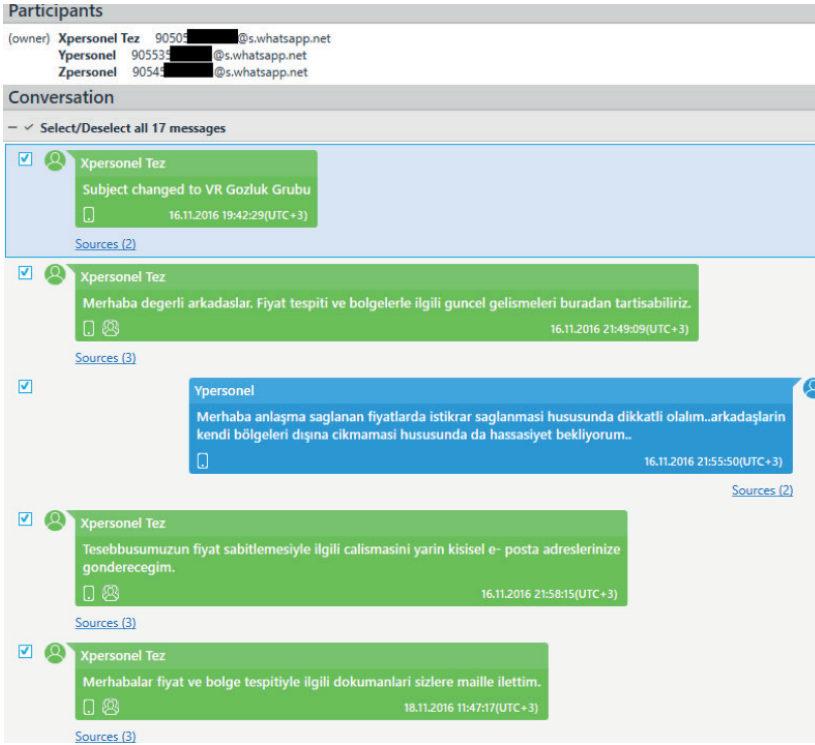
- **Mesajlaşma kayıtları:** *msgstore.db* veri tabanında tutulmaktadır. Veri tabanının yolu */data/com.whatsapp/databases/msgstore.db* şeklindedir. *msgstore.db*'de *chat_list*, *group_participants* ve *messages* tablolarından veriler elde edilmiştir. Bahse konu veri tabanından; göndericilere ait iletişim numaraları, mesajlar, mesajların durumları, mesajların gönderildiği veya alındığı zaman, konum bilgileri ve eklerin elde edilmesi mümkündür (Lone vd. 2015, 28).
- **İletişim bilgileri:** *wa.db* veri tabanında tutulmaktadır. Veri tabanının yolu */data/com.whatsapp/databases/wa.db-wal* şeklindedir. Veriler *wa.db*'de *wa_contacts* tablosundan elde edilmiştir.

⁵⁶ <https://www.whatsapp.com/features/>, Erişim Tarihi: 28.11.2016.

⁵⁷ *SQLite* veritabanı Batty ve Scott (2016, 3) tarafından şu şekilde tanımlanmaktadır: “*SQLite* veri tabanı birçok işlemi yapılandırma, değiştirme veya uzun yükleme işlemleri gerektirmeden gerçekleştiren küçük hafif bir veri tabanı motorudur.” Hızı, küçük boyutu, kolay kullanımı ve zorluk seviyesi düşük yapılandırması nedeniyle oldukça yaygın olarak kullanılan *SQLite*; *iOS*, *Android*, *Symbian OS*, *Maemo*, *Blackberry* ve *WebOS* işletim sistemlerinde kullanılabilmekte ve *C*, *C++*, *BASIC*, *C#*, *Python*, *Java* ve *Delphi* programlama dilleriyle bağlantı kurabilmektedir (Bhosale vd. 2015, 882).

İletişim kayıtlarının tespiti noktasında mesajlaşma kayıtları, adres defteri, konum bilgileri, resimler, videolar ve paylaşılan belgeler *WhatsApp*’tan elde edilebilecek önemli veriler arasında yer almaktadır. (Aiswarya 2016, 99).

“VR Gozluk Grubu” isimli gruptan yapılan yazışmalar Şekil 16’da yer almaktadır.



Şekil 16: WhatsApp Grup İletileri

Kullanılan adli bilişim araçları tarafından cihazdaki mesajlar ve paylaşılan veriler elde edilirken, “VR Gozluk Grubu” isimli *WhatsApp* grubundan silinen mesajlar her iki araç tarafından da elde edilememiştir. *XRY* ve *UFED* kapatılan grupları tespit edebilirken, bu duruma ek olarak *XRY* kapatılan gruptaki mesajları da elde etmiştir (Bkz. Tablo 6).

<i>Kriterler</i>	<i>Mobil Adli Bilişim Araçları</i>			
	<i>XRY Fiziksel</i>	<i>XRY Mantıksal Agent</i>	<i>UFED Physical Analyzer Fiziksel</i>	<i>UFED Physical Analyzer Mantıksal</i>
Cihazdaki mesajların bulunması	+	-	+	+
Silinen mesajların kurtarılması	Kısmen	-	Kısmen	Kısmen
Kapatılan gruplardaki mesajların kurtarılması	+	-	-	-
Paylaşılan verinin bulunması	+	-	+	+

Tablo 6: WhatsApp'tan Elde Edilen Veriler Tablosu

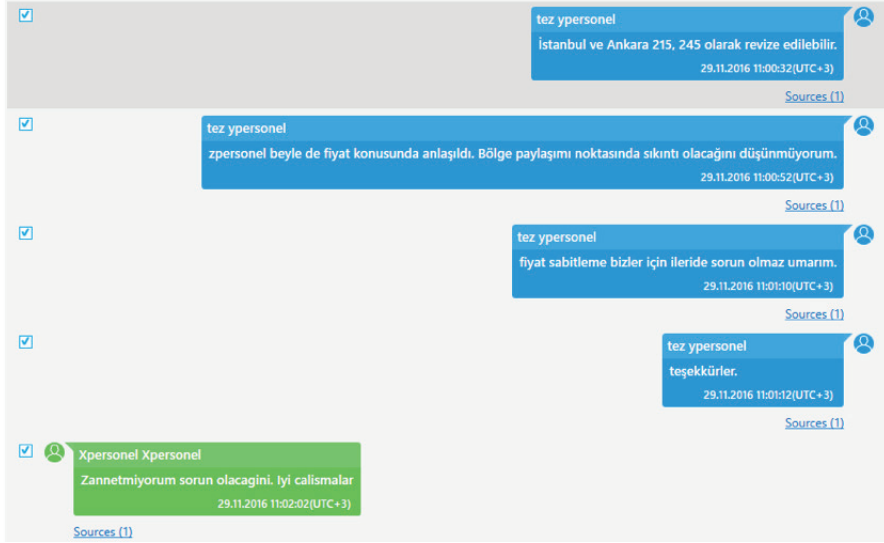
3.3.2. Google Hangouts

Google Hangouts (Hangouts), Google tarafından geliştirilen arama, anlık mesajlaşma, videolu görüşme ve resim, video, konum paylaşma özelliklerini sunan iletişim platformudur⁵⁸. *Android*'de *com.google.android.talk* paket adına sahip uygulamanın çalışmada incelenen sürümü 14.0'dır.

Hangouts'un incelenmesiyle birlikte *babel#⁵⁹.db* isimli veri tabanında yer alan *conversations*, *dismissed_contacts*, *messages* ve *participants* tablolarından konuşma bilgilerine, iletişim kurulmuş kullanıcı kayıtlarına, mesajlaşma geçmişine ve iletişim kurulan kullanıcıların tam isimlerine, profil fotoğraflarına ve kullanıcının mesajlaşma tablolarına erişilmiştir. İncelenen cihazın *babel1.db* veri tabanına ait *messages* ve *participants* tablolarından veri elde edilmiştir.

⁵⁸ <https://support.google.com/hangouts/answer/2944865?co=GENIE.Platform%3DDesktop&hl=en>, Erişim Tarihi: 29.11.2016.

⁵⁹ # = 0 veya 1.



Şekil 17: Google Hangouts İletileri

UFED, Hangouts kullanılarak yazılmış tüm iletileri elde etmiştir (Bkz Tablo 7).

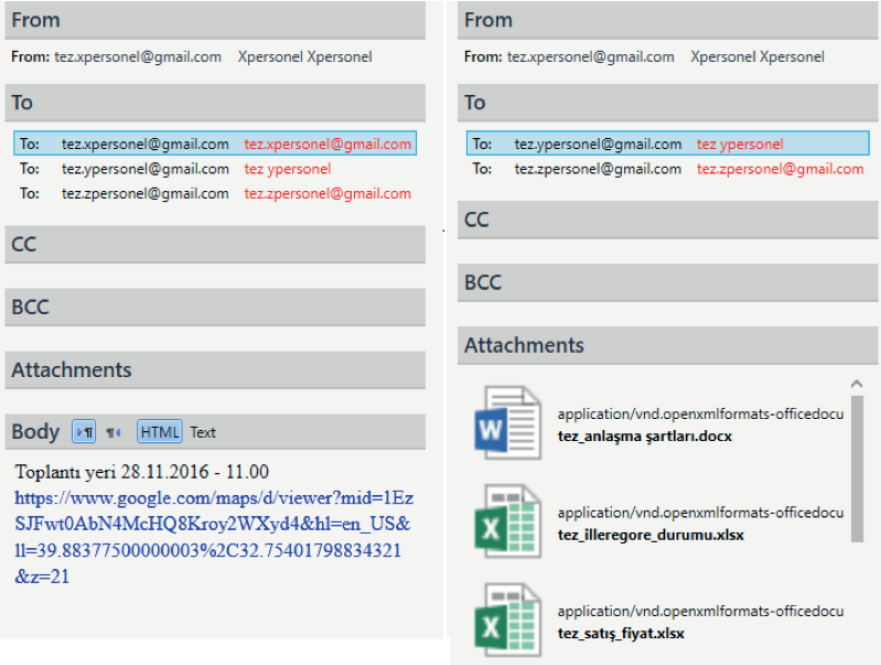
Kriter	Mobil Adli Bilişim Araçları			
	XRY Fiziksel	XRY Mantıksal Agent	UFED Physical Analyzer Fiziksel	UFED Physical Analyzer Mantıksal
Cihazdaki mesajların bulunması	-	-	+	-
Paylaşılan verinin bulunması	-	-	+	-

Tablo 7: Hangouts'tan Elde Edilen Veriler Tablosu

3.3.3. Gmail

Gmail, Google tarafından kullanıcılara sunulan e-posta servisi'dir. Paket adı *com.google.android.gm* olan *Gmail* e-posta servisinin incelenen sürümü *6.10.23.137993926.release*'dir. *Gmail* incelemesiyle birlikte aşağıdaki verilere erişilmiştir:

- */data/com.google.android.gm/databases/mailstore.tez.xpersonel@gmail.com.db* yolundan erişilen veri tabanında *messages*, *labels* ve *attachments* tablolarından veriler elde edilmiştir. *Gmail*'den gönderilen e-posta eklerine */data/com.google.android.gm/cache/tez.xpersonel@gmail.com/<DOSYA>* yolundan erişilmiştir.
- */databases/suggestions.db* yolundan bulunan *suggestions.db* veri tabanından uygulama içinde aranan kelimelere erişilmesi mümkündür. İncelenen cihazda bahse konu veri tabanı tespit edilmemiştir.



Şekil 18: Gmail'den Elde Edilen İki Farklı E-posta Yazışması

İncelenen cihazdaki e-posta verileri, ekler de dâhil olmak üzere *XRY* ve *UFED* tarafından elde edilmiştir. Her iki adli bilişim aracı, silinen tüm e-postaları kurtaramamakla birlikte, birbirinden farklı silinen e-postaları kurtarmışlardır (Bkz Tablo 8).

<i>Kriter</i>	<i>Mobil Adli Bilişim Araçları</i>			
	<i>XRY</i> <i>Fiziksel</i>	<i>XRY</i> <i>Mantıksal</i> <i>Agent</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Fiziksel</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Mantıksal</i>
Cihazdaki e-postaların bulunması	+	-	+	+
Silinmiş e-postaların kurtarılması	Kısmen	-	Kısmen	Kısmen
E-posta eklerinin bulunması	+	-	+	+

Tablo 8: Gmail’den Elde Edilen Veriler Tablosu

3.3.4. Google Chrome

Google Chrome (Chrome) web tarayıcı olarak birçok *Android* cihazda ön tanımlı şekilde kullanıcılara sunulmaktadır. Paket adı *com.android.chrome* olan *Chrome*’nin incelenen sürümü 54.0.2840.85’dir. */data/com.android.chrome/app_chrome/Default/History* yolundan erişilen veri tabanında yer alan *visits*, *urls* ve *keyword_search_terms* tablolarından tarayıcı geçmişine ve tarayıcıdan aranan anahtar kelimelere erişilmiştir.

Web History	Go to	Searched Item	Go to
Title: en iyi toplantı salonları - Google'da Ara Last Visited: 16.11.2016 22:02:49(UTC+3) Visits: URL: https://www.google.com.tr/search?q=en+iyi+toplanti+salonlari&oq=en+iyi+toplanti+salonlari&aqs=chrome..69j57j0j9559j0j48&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8 Source: Chrome Extraction: Physical Source file: userdata (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History : 0x1EF1D (Table: visits, urls, Size: 524288 bytes)		Timestamp: 16.11.2016 22:02:49(UTC+3) Source: Chrome Value: en iyi toplantı salonları Search Results: Extraction: Physical Source file: userdata (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History : 0x1EF1D (Table: visits, keyword_search_terms, Size: 524288 bytes)	
		Map Position: Map Address:	

Şekil 19: Tarayıcı Geçmişi Verileri

Adli bilişim araçlarının farklı sınıflandırma algoritmaları kullanmaları nedeniyle, tarayıcı geçmişindeki sonuçlar farklılık göstermekle birlikte her iki adli bilişim aracının da tarayıcı geçmişini elde edebildiği sonucuna ulaşılmıştır (Bkz. Tablo 9).

Kriter	Mobil Adli Bilişim Araçları			
	XRY Fiziksel	XRY Mantıksal Agent	UFED Physical Analyzer Fiziksel	UFED Physical Analyzer Mantıksal
Tarayıcı geçmişinin bulunması	+	-	+	Kısmen
Silinmiş geçmiş öğelerinin kurtarılması	+	-	Kısmen	Kısmen

Tablo 9: Chrome'dan Elde Edilen Veriler Tablosu

3.3.5. Arama Kayıtları ve Rehber

İncelenen cihaz, cihazla birlikte gelen ön tanımlı rehber ve çağrı uygulamasını kullanmakta olup, çağrı kayıtları, */data/com.android.providers.contacts/databases/contacts2.db* ile erişilen veri tabanında yer alan *calls* tablosunda bulunmaktadır. Bahse konu veri tabanının *raw_contacts* ve *data* tablolarından rehber bilgilerine erişmek mümkün olmaktadır.

Contact	Go to	Contact	Go to
Name: Zpersonel Source: Group: Contact Type: Created: Modified: Last time contacted: Times contacted: Extraction: Physical Source file: userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db : 0x6E3EB (Table: raw_contacts, data, Size: 487424 bytes) Details Mobil +905455 Mesaj +90 545 Mobil +90 545		Name: Ypersonel Source: Group: Contact Type: Created: Modified: Last time contacted: 27.11.2016 15:16:02(UTC+3) Times contacted: 27 Extraction: Physical Source file: userdata (ExtX)/Root/data/com.android.providers.contacts/databases/contacts2.db : 0x6D7DF (Table: raw_contacts, data, Size: 487424 bytes) Details Mobil +905535 Mesaj +90 553 Mobil +90 553	

Şekil 20: Ypersonel ve Zpersonel'e Ait İletişim Bilgileri



Şekil 21: Xpersonel ve Ypersonel arasında gerçekleşen Çağrı Geçmişi Örneği

Cihazdaki arama kayıtları ve adres defteriyle ilgili veriler her iki araç tarafından da elde edilmiştir. Silinen ögeler değerlendirildiğinde her iki adli bilişim aracının birbirlerini tamamlayacak şekilde farklı ögeleri kurtardıkları sonucuna varılmıştır⁶⁰ (Bkz. Tablo 10).

<i>Kriter</i>	<i>Mobil Adli Bilişim Araçları</i>			
	<i>XRY Fiziksel</i>	<i>XRY Mantıksal Agent</i>	<i>UFED Physical Analyzer Fiziksel</i>	<i>UFED Physical Analyzer Mantıksal</i>
Cihazdaki arama kayıtlarının bulunması	+	+	+	+
Silinmiş arama kayıtlarının kurtarılması	Kısmen	-	Kısmen	Kısmen
Adres defterinin bulunması	+	Kısmen	+	Kısmen
Adres defterinden silinmiş kayıtların kurtarılması	+	-	+	Kısmen

Tablo 10: Arama Kayıtları ve Adres Defterinden Elde Edilen Veriler Tablosu

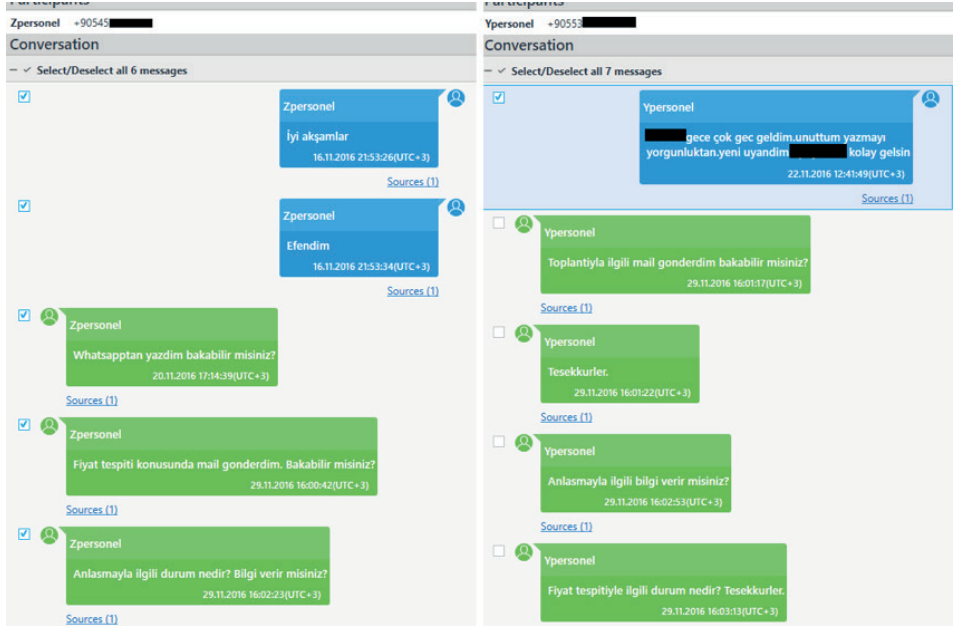
⁶⁰ SIM kartta yer alan arama kayıtları ve adres defteri verilerinin kopyalarının alınması, elde edilen veri miktarını arttırabilir.

3.3.6. SMS

İncelenen cihazda, cihazla birlikte gelen ön tanımlı *SMS* uygulaması kullanılmakta olup, *data/com.android.providers.telephony/databases/* dizininde bulunan *mmssms*.

db isimli veri tabanında yer alan *sms* tablosundan *SMS* kayıtlarına erişim sağlanmaktadır.

Her iki adli bilişim aracının da cihazdaki *SMS*'leri buldukları, fakat cihazdan silinmiş *SMS*'leri kurtaramadıkları tespit edilmiştir. Bu tür durumlarda *SIM* kartın kopyasının alınması ve silinmiş *SMS*'lerin kurtarılması için ilave tekniklerin kullanılması gerekmektedir.



Şekil 22: Xpersonel tarafından Ypersonel ve Zpersonel'e Gönderilen *SMS*'ler

SMS'lerden elde edilen veriler Tablo 11'de yer almaktadır.

<i>Kriter</i>	<i>Mobil Adli Bilişim Araçları</i>			
	<i>XRY</i> <i>Fiziksel</i>	<i>XRY</i> <i>Mantıksal</i> <i>Agent</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Fiziksel</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Mantıksal</i>
Cihazdaki SMS'lerin bulunması	+	+	+	+
Silinmiş SMS'lerin kurtarılması	-	-	-	-

Tablo 11: SMS'lerden Elde Edilen Veriler Tablosu

3.3.7. Konum Bilgileri

Teşebbüs çalışanlarının farklı uygulamaları kullanarak birbirlerine gönderdikleri konumlardan, bağlandıkları ortak kablosuz ağlardan, çektikleri fotoğrafların *EXIF*⁶¹ (Exchangeable Image File) bilgilerinden ve birbirleriyle yakın konumlarda bulunduklarında baz istasyonlarına ait kayıtlardan, ihlale ilişkin önemli verilerin elde edilebileceği değerlendirilmektedir. İncelenen cihazdan; *Google Maps*, *Hangouts*, *Here Maps* ve *WhatsApp* uygulamalarının yanı sıra fotoğraflardan, kablosuz ağlardan ve baz istasyonlarından da konum bilgileri elde edilmiştir. Cihazdan konum bilgileriyle ilgili veriler şu şekildedir:

- Cihazda bulunan *Here Maps* uygulamasına ait konum bilgileri */data/com.here.app.maps/databases/scbeEncrypted/scbeEncrypted.decrypted* konumunda yer alan veri tabanının, *ScbeDataObjects* tablosunda yer almaktadır.
- Cihazda bulunan *Google Maps* uygulamasına ait konum bilgileri */data/com.google.android.apps.maps/databases/gmm_myplaces.db* veri tabanında yer alan *sync_item* tablosunda yer almaktadır.

⁶¹ *EXIF* formatı çekilen görüntülerin enlem, boylam ve irtifa gibi bilgileri barındırmasını sağlayan ve *Android* tarafından da kullanılmakta olan bir veri tanımlama standartıdır (Sahu ve Chakraborty 2013, 1684). *EXIF* bilgileri arasında görüntüyü çeken cihazın bilgileri, çekim zamanı, çözünürlük gibi bilgiler de yer almaktadır.

Location	Go to	Location	Go to
Name: Meksika Caddesi Description: Type: Timestamp: End Time: Position: (39.902210, 32.696990) Map Address: Precision: Confidence: Map: Category: Here Maps Address: 06810 Ümit Ankara Extraction: Physical Source file: userdata (ExtX)/Root/data/com.here.app.maps/ databases/scbeEncrypted/ scbeEncrypted.decrypted : 0x21E4 (Table: ScbeDataObjects, Size: 9216 bytes)		Name: Rekabet Kurumu Description: http://maps.google.com/?cid=7507730909225623279 Type: Timestamp: 16.11.2016 21:39:12(UTC+3) End Time: Position: (39.883401, 32.753868) Map Address: Precision: Confidence: Map: Category: Google Maps Address: Extraction: Physical Source file: userdata (ExtX)/Root/data/ com.google.android.apps.maps/databases/ gmm_myplaces.db : 0x3ED0 (Table: sync_item, Size: 40960 bytes)	

Şekil 23: Here Maps ve Google Maps konumları

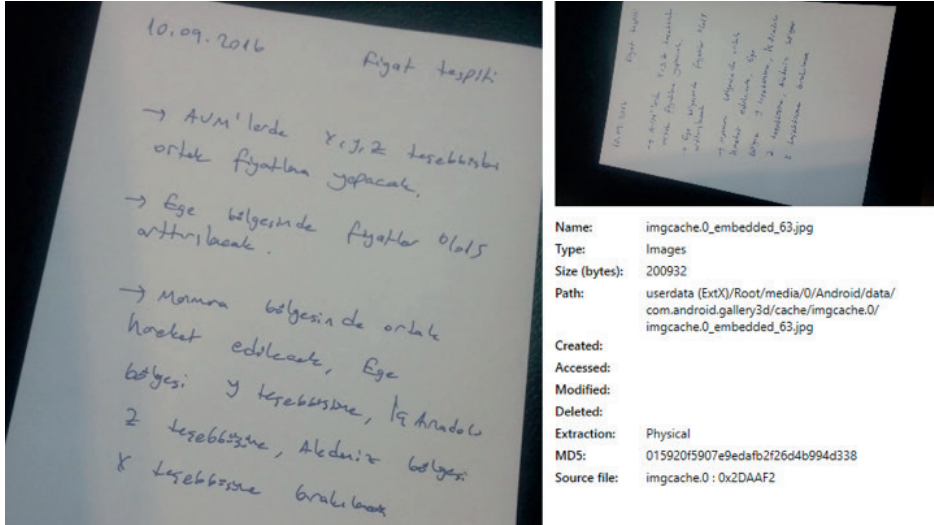
UFED’le yapılan incelemede farklı uygulamalarla oluşturulmuş konum bilgilerinin tamamı elde edilirken; XRY’la konum bilgilerinin bir kısmı elde edilebilmiştir (Bkz. Tablo 12).

Kriter	Mobil Adli Bilişim Araçları			
	XRY Fiziksel	XRY Mantıksal Agent	UFED Physical Analyzer Fiziksel	UFED Physical Analyzer Mantıksal
Google Maps	+	-	+	+
Hangouts	-	-	+	-
Here Maps	-	-	+	-
WhatsApp	+	-	+	+
WiFi Bağlantı Noktaları	-	-	+	Kısmen

Tablo 12: Konum Bilgilerine Ait Veriler Tablosu

3.3.8 Fotoğraflar ve Ses Kayıtları

Çekilen ve paylaşılan fotoğraflar, videolar ve alınan ses kayıtları da incelenen cihazdan elde edilebilecek veriler arasında yer almaktadır. Bahse konu verilerin konum bilgileri, elde edildikleri uygulamaya göre değişmektedir. Örneğin cihazın kamerasından elde edilen bir fotoğrafın yolu `/media/0/DCIM/Camera/<DOSYA_ADİ>` olarak kayıtlarda yer almaktayken, *WhatsApp* uygulaması kullanılarak çekilen bir fotoğrafın yolu `/media/0/WhatsApp/Media/WhatsApp Images/<DOSYA_ADİ>` olarak kayıtlarda yer almaktadır.



Şekil 24: Toplantıda Konuşulan Konulara Dair Fotoğraf Örneği

Her iki adli bilişim aracı da *fiziksel* veri elde etme metoduyla fotoğrafları ve ses kayıtlarını incelenen cihazdan elde etmişlerdir. Fakat silinmiş ses kaydı, adli bilişim araçları tarafından artık alandan kurtarılabılır olarak kazanamamıştır (Bkz. Tablo 13).

Kriter	Mobil Adli Bilişim Araçları			
	<i>XRY</i> <i>Fiziksel</i>	<i>XRY</i> <i>Mantıksal</i> <i>Agent</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Fiziksel</i>	<i>UFED</i> <i>Physical</i> <i>Analyzer</i> <i>Mantıksal</i>
Cihazdaki fotoğrafların bulunması	+	Kısmen	+	Kısmen
Silinmiş fotoğrafların kurtarılması	+	-	+	-
EXIF'lerin bulunması	+	+	+	+
Cihazdaki ses kayıtlarının bulunması	+	+	+	+
Silinmiş ses kayıtlarının kurtarılması ⁶²	Kısmen	-	Kısmen	-

Tablo 13: Fotoğraflar ve Ses Kayıtlarına Ait Veriler Tablosu**3.3.9. Elektronik Belgeler**

Mobil cihazda oluşturulan, görüntülenen, değiştirilen veya silinen elektronik belgeler de cihazdan elde edilen veri kaynakları arasında yer almaktadır. Cihazda bulunan elektronik belgelerin oluşturulma, değiştirilme ve erişilme tarihlerine ek olarak, belgenin elde edildiği kaynağa ve silinme tarihine de ulaşmak mümkün olmaktadır.

⁶² Silinmiş ses kaydına ait bilgiler adli bilişim araçları tarafından bulunmuş, fakat ses kaydı bahse konu araçlar tarafından kurtarılamamıştır.

	Name	Path	Size (by	Created	Modified	Accessed
1	tez_satış_fiyat.xlsx	userdata (ExtX)/Root/me...	11041	18.11.2016 15:08:00(UTC+3)	18.11.2016 15:08:00(UTC+3)	18.11.2016 15:08:00(UTC+3)
1	tez_illeregore_durumu.xlsx	userdata (ExtX)/Root/me...	12225	18.11.2016 15:07:58(UTC+3)	18.11.2016 15:07:58(UTC+3)	18.11.2016 15:07:58(UTC+3)
1	tez_anlaşma_sartları.docx	userdata (ExtX)/Root/me...	16678	18.11.2016 15:07:59(UTC+3)	18.11.2016 15:07:59(UTC+3)	18.11.2016 15:07:59(UTC+3)
1	tez_toplantı_tutanakları-2.docx	userdata (ExtX)/Root/dat...	17037	30.11.2016 13:41:25(UTC+3)	30.11.2016 13:41:25(UTC+3)	30.11.2016 13:41:25(UTC+3)
1	tez_toplantı_tutanakları.docx	userdata (ExtX)/Root/me...	17037	18.11.2016 15:08:04(UTC+3)	18.11.2016 15:08:04(UTC+3)	18.11.2016 15:08:04(UTC+3)
1	tez_sunum.pptx	userdata (ExtX)/Root/me...	39548	18.11.2016 15:08:02(UTC+3)	18.11.2016 15:08:02(UTC+3)	18.11.2016 15:08:02(UTC+3)
1	tez_vr_gözlük_bölgeler.docx	userdata (ExtX)/Root/me...	50888	18.11.2016 15:08:05(UTC+3)	18.11.2016 15:08:05(UTC+3)	18.11.2016 15:08:05(UTC+3)

Şekil 25: Elektronik Belge Örnekleri

İncelenen mobil cihazdan *fiziksel* veri elde etme yöntemiyle, rekabet ihlaliyle ilgili tüm elektronik belgelerin bulunduğu görülmüştür (Bkz. Tablo 14). Yapılan incelemede, belgeler içinde anahtar kelime araması yapılamadığı tespit edilmiştir. Bu noktada mobil cihazlardan elde edilen belgelerin, farklı bir adli bilişim aracına da yüklenerek yeniden incelenmesinin uygun olacağı değerlendirilmektedir.

Kriter	Mobil Adli Bilişim Araçları			
	XRY Fiziksel	XRY Mantıksal Agent	UFED Physical Analyzer Fiziksel	UFED Physical Analyzer Mantıksal
Cihazdaki belgelerin bulunması	+	+	+	Kısmen
Belgenin içinde anahtar kelime ile arama yapma ⁶³ ve OCR ⁶⁴	-	-	-	-

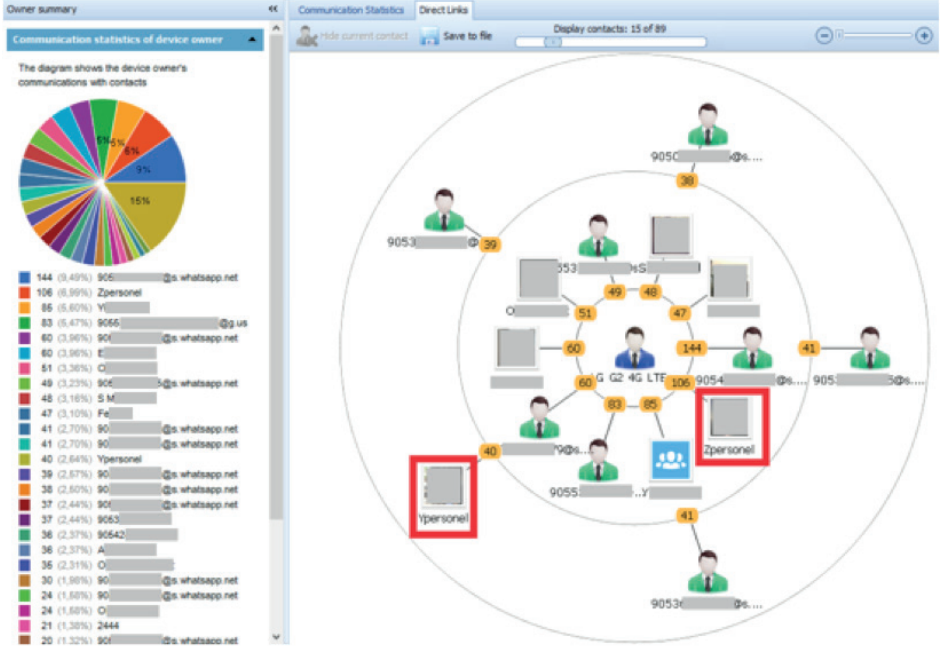
Tablo 14: Elektronik Belgeler Tablosu

⁶³ XRY Reader ve UFED Reader ile denenmiştir.

⁶⁴ OCR (Optical Character Recognition), optik karakter tanımlama anlamına gelmektedir.

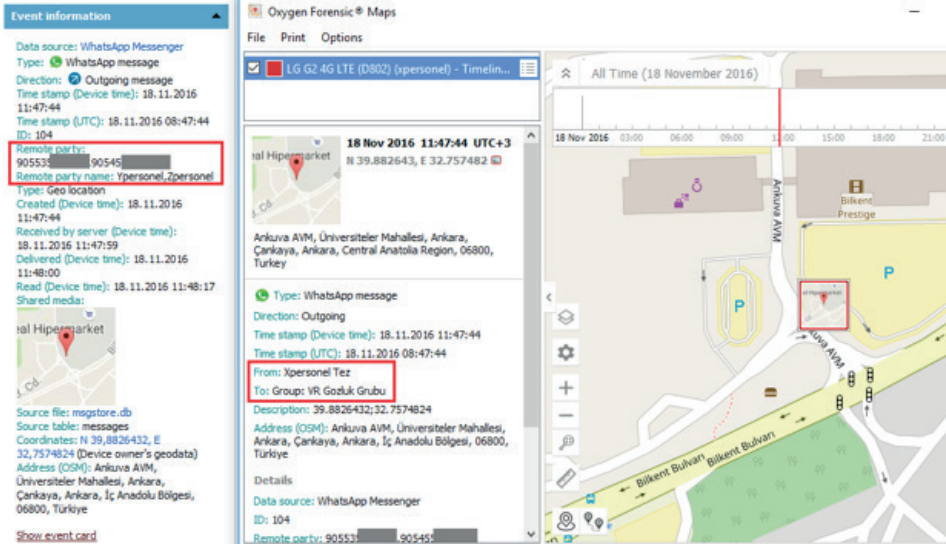
3.3.10. Oxygen Forensics Detective Analizleri

OFD'ye ait *Analytics* bölümünden erişilen iletişim kayıtları ekranı, cihaz sahibinin iletişim kurduğu diğer teşebbüs çalışanlarının tespiti hususunda analizi kolaylaştıran bir grafik arayüz sunmaktadır (Bkz. Şekil 26).



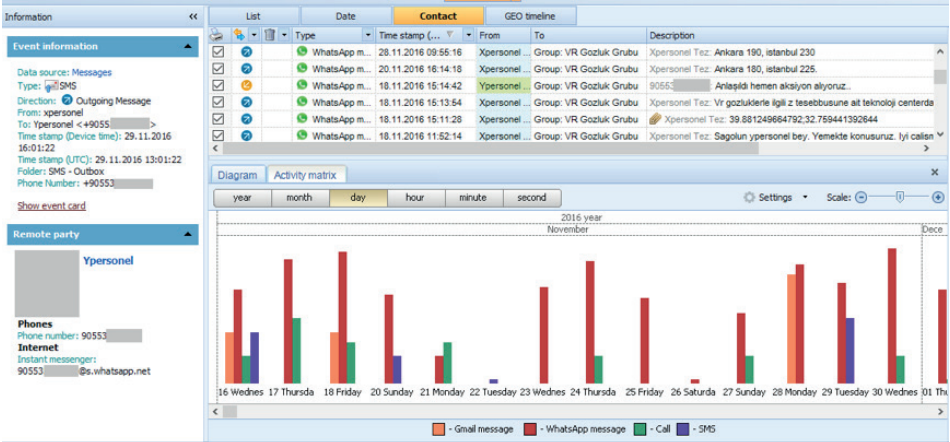
Şekil 26: *OFD* İletişim İstatistikleri Analiz Ekranı

Cihazdan elde edilen konum bilgilerine ek olarak, konum bilgisinin üretildiği uygulama bilgisi ve varsa paylaşılan iletişim kayıtlarına harita görünümünde erişilebilmektedir (Bkz. Şekil 27). Bu ekran sayesinde teşebbüs çalışanlarının aralarında paylaştıkları konum bilgilerinin harita üzerinde analiz edilmesi mümkün hale gelmektedir.



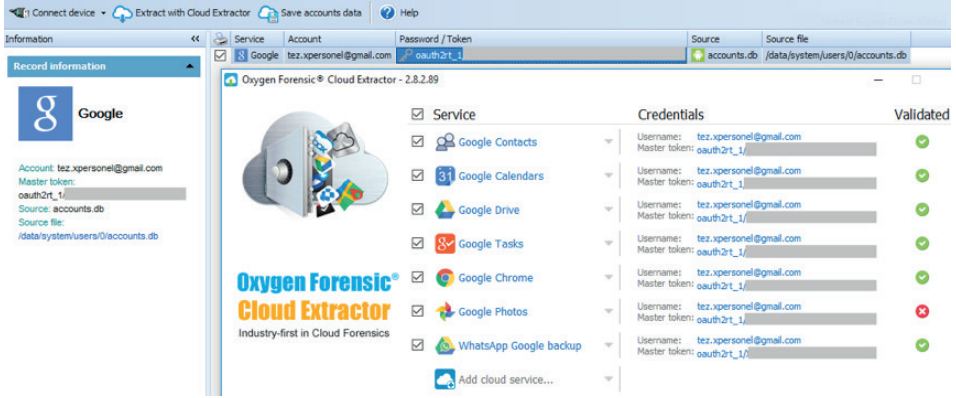
Şekil 27: OFD Konum Analiz Ekranı

İletişim kayıtlarının tespiti bakımından analiz edilebilmesi mümkün bir diğer unsur iletişim kayıtlarının tarihsel bazda ayrımıdır. Cihaz sahibinin hangi tarihler arasında kimlerle, hangi uygulamaları kullandığı hususunun tespiti için iletişim kayıtları aktivite grafiğinin kullanılması mümkündür (Bkz. Şekil 28).



Şekil 28: İletişim Kayıtları Analiz Ekranı

*Oxygen Forensics Cloud Extractor*⁶⁵, cihazdaki hesapların erişim bilgilerini kullanarak buluttaki verileri elde edebilmektedir (Bkz. Şekil 29). Buluttan elde edilen veriler, diğer dosyalarla birleştirilebilmekte ve derin veri analizi için *Analytics* araçlarıyla kullanılabilir. Teşebbüs çalışanının buluttaki hesaplarına erişilmesi için bahse konu aracın kullanımı mümkündür.



Şekil 29: Oxygen Forensics Cloud Extractor Ekranı

3.4. İNCELEMEDE KULLANILAN ADLİ BİLİŞİM ARAÇLARININ DEĞERLENDİRİLMESİ

3.4.1. Test Cihazından Elde Edilen Sonuçlar Kapsamında Değerlendirme

İncelenen adli bilişim araçlarından elde edilen sonuçlar ışığında, her bir adli bilişim aracının kullanımıyla rekabet ihlaline yönelik verilerin büyük çoğunluğuna ulaşıldığı görülmektedir. Bu çerçevede yapılan değerlendirmeler aşağıda özetlenmektedir:

- Cihazda yapılan değişiklikler bakımından, adli bilişim araçlarının *fiziksel* veri elde etme yöntemlerinde cihaza minimum düzeyde müdahale ettiği, *mantıksal* veri elde etme yöntemleri kullanıldığında müdahale sayısının arttığı görülmüştür.

⁶⁵ *Oxygen Forensics Cloud Extractor* kullanılarak *Google Drive*, *iCloud*, *OneDrive* ve *Dropbox* gibi 25'den fazla bulut depolama hizmetinden veri elde edilebilmektedir. <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/detective/cloud-data-extraction>, Erişim Tarihi: 18.12.2016.

- Her iki (*XRY* ve *UFED*) adli bilişim aracına da mobil cihazın kapalı olarak bağlanması nedeniyle *fiziksel* veri elde etme yönteminde ekran kilidinin geçilmesine gerek duyulmamıştır⁶⁶.
- Adli bilişim araçlarının kullanım kolaylıkları bakımından, yazılım arayüzlerinin gayet anlaşılır ve kolay kullanıma sahip olduğu sonucuna ulaşılmıştır.
- Elde edilen sonuçlar değerlendirildiğinde, Yİ'lerde *fiziksel* veri elde etme yönteminin (silinmiş ögeleri kurtarma, daha fazla veri elde etme vb.) öncelikli olarak kullanılmasının, *fiziksel* veri elde etme yönteminin kullanılmasının mümkün olmadığı durumlarda (cihazın *root* haklarına erişilememesi, adli bilişim aracının mobil cihazı desteklememesi vd.) *mantıksal* veri elde yöntemine geçilmesinin uygun olacağı sonucuna ulaşılmıştır.
- Test sonuçlarından yola çıkılarak incelemede kullanılan adli bilişim araçlarının birinin diğerine üstün olduğu şeklinde bir değerlendirme yapılamayacağı sonucuna ulaşılmıştır.

3.4.2. Bölüm Değerlendirmesi

Mobil adli bilişim saha çözümleri, veri elde edilmesi ve incelenmesi için kullanılacak taşınabilir araçlar olup, şirketlerin araç gamında yer alan saha serisi çözümlerle laboratuvar ortamına bağımlı kalınmaksızın sahada inceleme yapılabilmektedir. *Cellebrite UFED Field*, *MSAB Field*, *Paraben Mobile Field Kit* ve *AccessData nFIELD* gibi sahada kullanıma uygun araçların Yİ'lerde kullanımının inceleme sürecini hızlandırarak meslek personeline incelemelerde vakit tasarrufu sağlayacağı düşünülmektedir.

Yazma koruyucular (*write blockers*), veri elde edilecek cihazın diskini koruyarak üzerine veri yazılmasını engelleyen araçlardır (Nelson vd. 2015, 269). İncelenecek mobil cihazın delil bütünlüğünün korunması hususunda, donanımsal yazma koruyuculara sahip araçların kullanılması gerektiği değerlendirilmektedir.

⁶⁶ Ekran kilidi testinin daha çok mobil cihazla yapılması değerlendirmeyi daha doğru hale getirecektir.

Cihazdan *rootlama* veya *jailbreak* işlemlerine gerek kalmadan *fiziksel* veri elde edebilen adli bilişim araçlarının seçilmesinin önemli olduğu sonucuna ulaşılmaktadır. *Rootlama* veya *jailbreak* yapılmamasıyla, *fiziksel* veri elde edilmesi için meslek personelinin cihaza yaptığı müdahalenin sınırlı kalacağı ve *fiziksel* veri elde etme yönteminin meslek personeline daha aktif olarak kullanılmasının önünün açılacağı değerlendirilmektedir.

Adli bilişim araçlarının, piyasaya yeni sürülen mobil cihazları veri elde etme açısından hızlıca desteklemeleri (güncellenen işletim sistemleri ve uygulamalar da dâhil olmak üzere) ve yazılımlarını düzenli olarak güncelleştirmelerinin önemli bir ölçüt olduğu değerlendirilmektedir.

Teşebbüs çalışanlarının bulutta sakladıkları verilere ulaşılması için buluttan veri çekebilen adli bilişim araçlarının kullanılması bir diğer önemli husustur. Ayrıca teşebbüsten elde edilen verinin analizinin kolaylaştırılması adına, analiz modülü olan adli bilişim çözümlerinin, Yİ’lerde kullanılmak üzere Kurum envanterinde yer almasının uygun olacağı düşünülmektedir.

Mobil cihazlardan daha fazla veri elde etmek için incelemeyi yapan uzmanların kullandıkları adli bilişim araçlarının temel özelliklerine ve teknolojilerine hâkim olmalarının önemli bir husus olduğu ve inceleme boyunca sadece tek bir adli bilişim aracına bağımlı kalınmasının potansiyel dijital delillere erişimi sınırlayacağı değerlendirilmektedir (Tassone vd. 2013, 6).

Bu bağlamda, Kurum envanterinde birden fazla mobil adli bilişim aracının bulunmasının uygun olacağı, meslek personelinin adli bilişim araçlarının fonksiyonlarına tam olarak hâkim olması gerektiği, konuyla ilgili düzenli eğitimlerin alınmasının önemli olduğu sonuçlarına varılmaktadır.

BÖLÜM 4

AB ve TÜRKİYE REKABET HUKUKU UYGULAMASINDA MOBİL CİHAZLARIN İNCELENMESİ

4.1. AB UYGULAMASI

4.1.1. Yerinde İncelemelere İlişkin Açıklayıcı Not

1/2003⁶⁷ sayılı Komisyon Tüzüğü'nün 20. maddesinin birinci fıkrası Komisyon'un rekabet ihlalleriyle ilgili inceleme yetkilerini düzenlemektedir. Bahse konu maddenin ikinci fıkrasının (b) bendinde Komisyon'un, *nerede saklandığına bakılmaksızın* işle ilgili tüm kayıtların inceleme yetkisine haiz olduğu ve yine aynı maddenin dördüncü fıkrası kapsamında teşebbüs ve teşebbüs birliklerinin Komisyon'un inceleme kararı kapsamında yapılan incelemelere katılımlarının gerekli olduğu belirtilmektedir.

En son 11 Eylül 2015 tarihinde güncellenen “1/2003 Sayılı Tüzüğün 20. maddesinin 4. Fıkrası Kapsamında Gerçekleştirilen İncelemelerle İlgili Açıklayıcı Not⁶⁸” (Açıklayıcı Not) ile Komisyon'un Yİ'lerde sahip olduğu yetkiler ve bu yetkilerin kullanılmasında uygulanan metotlarla ilgili ayrıntılı bilgiler yayımlanmıştır. Çalışmanın bu bölümünde, *Açıklayıcı Not*'un mobil cihazlarla ilgili olduğu değerlendirilen hususlara ve diğer kavramlara değinen dört paragrafı üzerinde durulacaktır.

⁶⁷ Bkz. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0001:EN:HTML>, Erişim Tarihi: 06.11.2016.

⁶⁸ Çalışma kapsamında “*Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003*” notu *Açıklayıcı Not* olarak ifade edilecektir. *Açıklayıcı Not*'a erişmek için bkz. http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf, Erişim Tarihi: 06.11.2016.

4.1.2. Bring Your Own Device (BYOD) Kavramı

Açıklayıcı Not'un 10. paragrafında, Yİ'yi gerçekleştiren uzmanların sunucu, masaüstü bilgisayar, dizüstü bilgisayar, **tablet** ve diğer **mobil cihazlara** ek olarak saklama ortamlarında⁶⁹ da arama yapabilecekleri ifade edilmektedir. Ayrıca bu ifadeye ek olarak teşebbüs çalışanlarının iş yerlerinde bulundurdıkları ve iş için kullandıkları (*Bring Your Own Device – BYOD*⁷⁰) kişisel cihazlarının da bu kapsamda incelenebileceği üzerinde durulmaktadır. 10. paragraf kapsamında ifade edilen bir diğer konuyla, incelemelerde adli bilişim araçlarının kullanılabileceği hususudur.

BYOD, teşebbüslerin çalışanlarına, teşebbüse ait cihazlar yerine sahip oldukları **mobil cihazları** teşebbüsle ilgili bilgi veya uygulamalara erişmek amacıyla kullanmalarına yönelik uyguladıkları politika veya metoda verilen addır (Kuschewsky ve Geradin 2013, 18). *BYOD* ile teşebbüs çalışanları, çalışma prensiplerine daha fazla hâkim oldukları kendi cihazlarını iş yerlerinde kullanmakta ve bu kapsamda teşebbüsler de yüksek maliyetli cihazların masraflarından tasarruf etmektedir (Dhingra 2016, 179). Teşebbüsler *BYOD* ile esneklik, kolaylık ve taşınabilirliği sağlayarak, teşebbüs çalışanlarının verimliliğini ve motivasyonunu arttırmayı hedeflemektedir⁷¹ (French vd. 2014, 192).

ICN (2014, 30) tarafından *BYOD* politikası kapsamında birçok teşebbüsün, çalışanlarına iş yerlerinde kendi elektronik cihazlarını kullanmalarına izin verdiği ve bu cihazların **kişisel** ve **profesyonel** bilgilerin birer birleşimini içerdiği belirtilmektedir. *BYOD* politikasını uygulayan bir teşebbüste, mobil cihazını kendi imkânlarıyla satın alan ve cihazını teşebbüs ağına dâhil etmeyen bir teşebbüs çalışanının mobil cihazının incelenmesi konusu da *BYOD* kapsamında tartışılması gereken konulardan biridir (Kinsella 2015,1). Bu bağlamda hangi cihazların *BYOD* kapsamında değerlendirileceği konusu önem kazanmaktadır (Collinson vd. 2015, 1). *BYOD* politikasını uygulayan teşebbüslerde gerçekleştirilen incelemelerde,

⁶⁹ CD-ROM, DVD, USB bellek, harici sabit disk, yedekleme teypleri, bulut servisler vd.

⁷⁰ “Kendi cihazını getir” olarak Türkçe’ye çevrilebilecek olan *BYOD*, “Bring Your Own Technology (*BYOT*)” kavramının yerini almaya başlamıştır (Miller vd. 2012, 53).

⁷¹ *BYOD* politikası, teşebbüsler açısından faydanın yanısıra bazı uygulama zorluklarını ve güvenlik risklerini de beraberinde getirmektedir. *BYOD* ile gelen güvenlik riskleri arasında teşebbüs çalışanlarının kasıtlı veya kasıtlı olmadan veri sızdırmaları, teşebbüsün cihazlar üzerindeki kontrolü kaybetmeleri ve cihazların kaybolması olarak sıralanmaktadır (Dedeche 2013, 8).

teşebbüs çalışanına ait kişisel veriler ile teşebbüse ait verilerin açıkça ayrılması, *BYOD* ile ortaya çıkan diğer bir konudur (Kuschewsky ve Geradin 2013, 18).

4.1.3. Wipe Kavramı

Açıklayıcı Not'un 13. paragrafında, inceleme süresince Komisyon tarafından kullanılan tüm adli bilişim araçlarının *wipe*⁷² edilmesi gerektiği, fakat teşebbüsçe verilen donanımların *wipe* edilmeden teşebbüse iade edileceği ifade edilmektedir. Bu paragrafkapsamında uzmanlar, inceleme süresince veri taşıyıcılara kopyalanmış verileri, kurtarılamayacak şekilde veri taşıyıcısı üzerinden temizlemektedirler (Erps ve Doury 2013, 214). Teşebbüse ait ticari sır içeren veriler de dâhil olmak üzere, mobil cihazlardan elde edilen tüm bilgilerin kopyalandığı Komisyon'a ait veri taşıyıcıların *wipe* edilmesi işlemi, incelemenin son adımını oluşturmaktadır (Erps ve Doury 2013, 214).

4.1.4. Mühürlü Zarf Prosedürü

Açıklayıcı Not'un 14. paragrafı, mühürlü zarf prosedürü hakkındadır. İncelenmesi gereken cihaz veya cihazların, incelemenin sonlarına doğru tespit edilmesi, incelemede teknik sorunların yaşanması veya incelemenin teşebbüsün iş akışlarını aksatacak şekilde teşebbüse iş yükü oluşturması gibi istisnai durumlarda, devam eden inceleme⁷³ veya mühürlü zarf prosedürü uygulanmaktadır (Erps ve Doury 2013, 214).

Anılan maddede, Yİ'nin beklenen vakit aralığında bitirilememesi durumunda incelenmesi gereken verinin mühürlü zarfa konulabileceği ve bu verinin bir kopyasının teşebbüs tarafından talep edilebileceği ifade edilmektedir. Ayrıca aynı madde kapsamında, mühürlü zarfın açılması esnasında hazır bulunmaları amacıyla teşebbüs yetkililerinin Komisyon'a davet edilebileceği veya mühürlü zarfın açılmadan teşebbüse iade edilebileceği gibi konular açıklığa kavuşturulmaktadır.

⁷² *Wipe*, disk üzerindeki verilerin geri getirilemeyecek şekilde silinmesi işlemidir. *Wipe* işleminden sonra disk üzerinde yer alan verinin kurtarılması mümkün değildir (Poonia 2014, 1374).

⁷³ Devam eden inceleme prosedürü, kopyası alınan verinin mühürlü bir zarf içinde teşebbüse bırakılması ve incelemenin teşebbüste (teşebbüse haber verilerek) gerçekleştirilmesi veya mühürlü zarfın içindeki verinin incelenmesi işleminin Komisyon'da gerçekleştirilmesi prosedürüdür (Doury vd. 2015, 1).

Mühürlü zarf prosedürünün özellikle kartel dosyaları kapsamında olan ve birden fazla teşebbüste eş zamanlı olarak gerçekleştirilen Yİ’lerde, teşebbüs çalışanlarına ait mobil cihazlarda oluşan iletişim kayıtlarının ortaya çıkarılmasıyla ilgili analizlerde fayda sağlayacağı değerlendirilmektedir.

4.1.5. Kişisel Verilerin Korunması

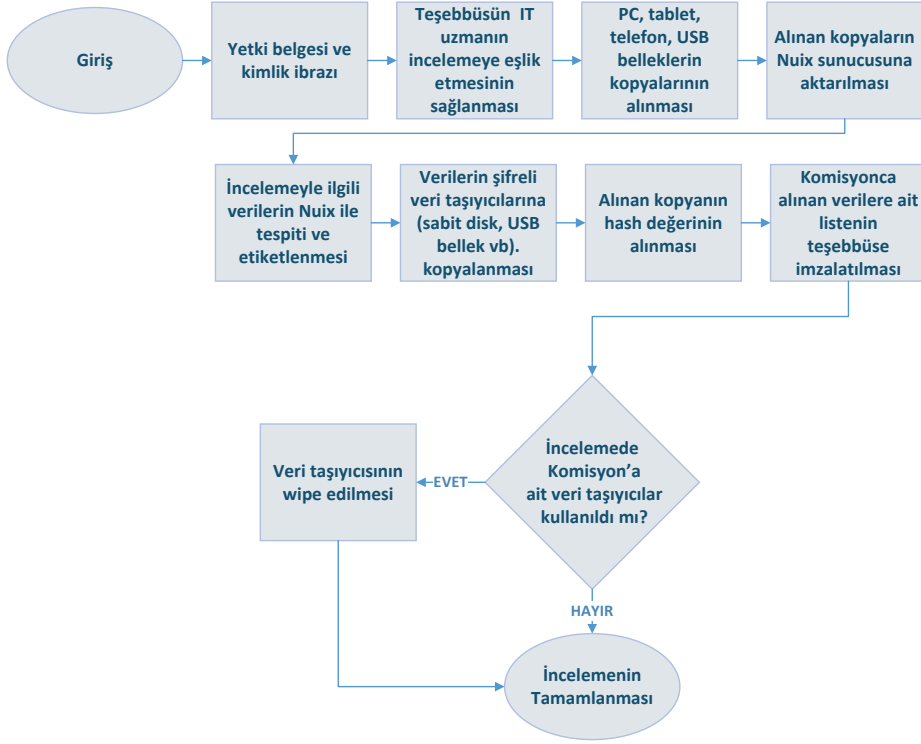
Açıklayıcı Not’un 20. ve 21. paragrafı, 45/2001⁷⁴ sayılı Avrupa Parlamentosu ve Konsey Tüzüğü kapsamında kişisel verilerin korunmasıyla ilgilidir. Teşebbüs çalışanlarına ait kişisel verilerin Komisyon tarafından yürütülen incelemelerin kapsamında olmadığı ve AB antitröst kanunlarının sadece teşebbüslere uygulanabileceği ifade edilmektedir. Aynı maddede, teşebbüs çalışanlarına ait bazı kişisel verilerin (isim, telefon numarası, e-posta adresi vb.) inceleme kapsamında elde edilen veriler kapsamında yer alabileceği; dolayısıyla bu verilerin de kopyalarının alınmış olabileceği belirtilmektedir. Ancak 21. paragrafta, söz konusu kişisel verilerin sadece 45/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü’ne uygun olarak kullanılabileceği vurgulanmaktadır.

4.1.6. Mobil Cihazların İncelenme Süreci

Açıklayıcı Not’un 10. paragrafında, Komisyon tarafından gerçekleştirilen incelemelerin kapsamında tablet ve mobil cihazlara ek olarak kişisel cihaz ve medyaların da dâhil olduğu (BYOD) belirtilmekte ve incelemelerde adli bilişim yazılım ve donanımlarının kopyalama, arama ve verilerin kurtarılması amacıyla kullanılabileceği ifade edilmektedir. Komisyon, teşebbüslere ait cihazlardaki verilerin kopyalarını aldıktan sonra inceleme işlemini *Nuix*⁷⁵ adli bilişim aracını kullanarak teşebbüste gerçekleştirmektedir (Erps ve Doury 2013, 213). Komisyon’un mobil cihazları da kapsayan inceleme yönergesi aşağıdaki şekilde yer almaktadır (Bkz. Şekil 30).

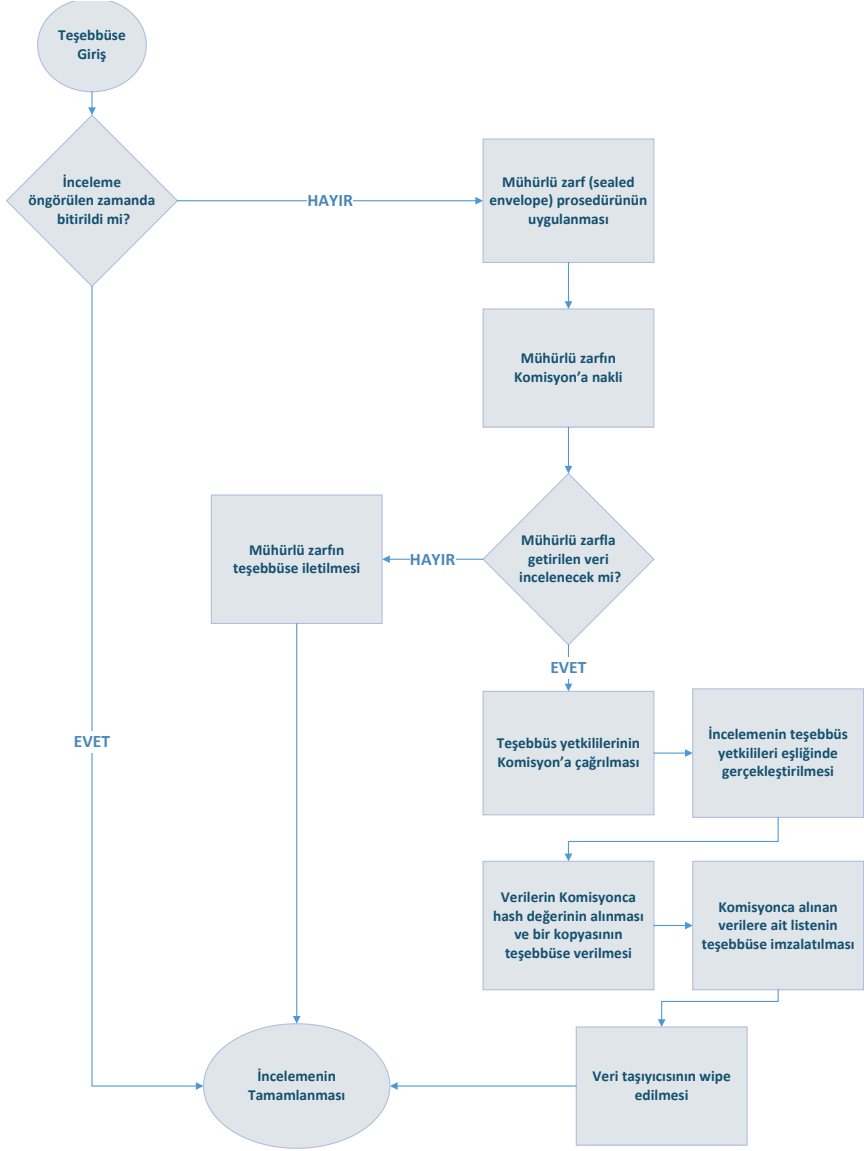
⁷⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=O:L:2001:008:0001:0022:en:PDF>, Erişim Tarihi: 06.11.2016.

⁷⁵ *Nuix*, 60’ dan fazla ülkede kamu kurumları ve özel sektörde faaliyet gösteren şirketlerce kullanılan genel bir adli bilişim aracı çözümüdür. (Nuix 2016a). *Nuix* mobil cihazlarda, mobil cihaz dosya sistemlerine ek olarak, *Cellebrite*, *Micro Systemation XRY* ve *Oxygen Forensic* imajlarında da inceleme yapılmasına olanak sağlamaktadır (Nuix 2016b). *Nuix* ve *Cellebrite* şirketlerinin teknoloji ortaklıkları bulunmaktadır (Nuix 2016c).



Şekil 30: Komisyon'un İnceleme Yönergesi İşığında İnceleme Süreci
(Erps ve Doury 2013, 213-214)

İncelemenin zamanında bitirilememesi durumunda, Komisyon mühürlü zarf veya devam eden inceleme prosedürünü uygulamaktadır (Erps ve Doury 2013, 214). Teşebbüse ait cihazlardan elde edilen kopyalar hash değerleri hesaplandıktan sonra bir veri taşıyıcısına kopyalanmakta ve mühürlü bir zarf içine konularak Komisyon'un merkezi olan Brüksel'e götürülmektedir. Mühürlü zarf içinde yer alan kopyaların incelenmesine karar verildiği durumda, mühürlü zarf teşebbüs temsilcileri eşliğinde açılmakta ve inceleme Komisyon'a ait birimde teşebbüs temsilcilerinin nezaretinde gerçekleştirilmektedir. Mühürlü zarftaki veri taşıyıcısının incelenmesinin gerekli görülmediği durumlarda uygulanan prosedürse, zarf içinde yer alan kopyanın teşebbüse geri gönderilmesidir. Mühürlü zarf prosedürü kapsamındaki verinin Komisyon'da incelendiği yönerge aşağıda yer almaktadır (Bkz. Şekil 31).



Şekil 31: Mühürlü Zarf Prosedürü Kapsamındaki Verinin Komisyon'da İncelendiği Usul

Komisyon tarafından yürütülen inceleme sürecinin aktarılmasından sonra Komisyon'un rekabet ihlalleri açısından mobil cihazlara yaklaşımının *Asansör*⁷⁶ kararıyla birlikte açıklanmasında fayda görülmektedir. Komisyon'un ilgili kararında kartellerin mobil cihaz kullanımıyla ilgili ifadeleri dikkat çekmektedir. Belçika, Almanya, Lüksemburg ve Hollanda'da asansör kurma ve bakım alanlarında faaliyet gösteren şirketlerin kurdukları kartel, 1995 ve 2004 yılları arasında fiyat sabitleme, pazar paylaşımı, önemli ve gizli ticari sırların değişimi gibi rekabet ihlaline sebebiyet verecek eylemlerde bulunmuş ve Komisyon kartele yaklaşık 992 milyon euro para cezası vermiştir. Komisyon tarafından yapılan basın açıklamasında, *"(...)genellikle barlarda ve lokantalarda buluşmuşlar; kırsal alanlara hatta yurtdışına seyahat etmişler ve takip edilmekten kaçınmak için ön ödemeli cep telefonu kartları kullanmışlardır."* ifadeleri yer almaktadır.

Komisyon'un mobil cihazlarla ilgili dikkat çeken bir diğer incelemesi telekomünikasyon şirketlerine gerçekleştirilen Yİ'lerdir. Komisyon tarafından 9 Temmuz 2013 tarihinde üye devletlerde internet bağlantı hizmetleri alanında faaliyet gösteren telekomünikasyon teşebbüslerinde Yİ'ler gerçekleştirilmiştir⁷⁷. Farklı teşebbüslerde gerçekleştirilen Yİ'ler kapsamında, Genel Müdür'ün cep telefonu da dâhil olmak üzere teşebbüslerin üst düzey çalışanlarının mobil cihazları da incelenmiştir⁷⁸. Komisyon tarafından rekabet ihlaline yönelik bir karar verilmediği için inceleme sonlandırılarak sektörün izlenmesine devam edilmesi kararı alınmıştır⁷⁹.

⁷⁶ 21.02.2007 ve *Case COMP/E-1/38.823 - PO/Elevators and Escalators*.

⁷⁷ Bkz. http://europa.eu/rapid/press-release_MEMO-13-681_en.htm, Erişim Tarihi: 26.12.2016.

⁷⁸ Bkz. <https://www.bloomberg.com/news/articles/2013-10-16/orange-ceo-s-iphone-seized-as-eu-antitrust-raiders-go-high-tech>, Erişim Tarihi: 26.10.2016.

⁷⁹ Bkz. http://europa.eu/rapid/press-release_IP-14-1089_en.htm, Erişim Tarihi: 26.12.2016.

4.2. MOBİL CİHAZLARIN İNCELENMESİNE İLİŞKİN AB ÜYESİ ÜLKE UYGULAMALARINDAN ÖRNEKLER

4.2.1. İspanya Uygulaması

İspanya’da rekabet ihlalleriyle ilgili incelemeler, İspanya Rekabet Otoritesi (CNMC⁸⁰) tarafından 3/2013 Sayılı Kanun kapsamında gerçekleştirilmektedir. Anılan kanunun 27. maddesinin ikinci fıkrasında, mobil cihazlarla ilgili açık bir düzenleme yer almamakla birlikte, bahse konu maddenin (b) ve (c) bentleri, CNMC’ye ticari faaliyetlerle ilgili kayıtların ne şekilde saklanıldığına bakılmaksızın tetkik edebilme ve kayıtların herhangi bir şekilde kopyalarını alabilme veya elde edebilme yetkilerini vermektedir.

Bu çerçevede CNMC, 3/2013 Sayılı Kanun’un 27. maddesinden aldığı yetkiyle tabletlerde ve mobil cihazlarda inceleme yetkisine sahiptir (OECD 2013, 3). CNMC tarafından gerçekleştirilen Yİ’lerde ağırlıklı olarak yazılı belgelere odaklanılmakta ve teşebbüslerin e-posta, *SMS* ve *WhatsApp* mesajlaşmaları gibi yazışmaları da toplanan deliller arasında yer almaktadır (OECD 2013, 3).

Durantez ve Contreras (2016, 1), CNMC’nin *WhatsApp* mesajlarına önem atfettiğini belirterek, CNMC’nin mobil mesajlaşma sistemlerine bakış açısını:

CNMC’ye göre mobil mesajlaşma sistemleri rakiplere rekabete hassas bilgilerin hızlıca değişimini sağladığı için bu mesajlaşma sistemleri rekabet otoriteleri için özellikle önemlidir.

şeklinde ifade etmektedirler. 2013 yılında CNMC tarafından gerçekleştirilen incelemede koz helvası üretimi yapan Almendra y Miel, S.A. (AyM) teşebbüsünde Yİ yapılmış, teşebbüsün diğer teşebbüsle olan *WhatsApp* yazışmaları elde edilmiş ve yazışmalarda teşebbüslerin beyaz etiketli koz helvası alıcılarından biriyle olan ilişkilerde ortak bir tavır takınılması gerekliliğinden bahsedildiği tespit edilmiştir. AyM’den elde edilen *WhatsApp* yazışmaları, CNMC’nin verdiği kararda⁸¹ delil olarak kullanılmış ve İspanya’daki beyaz etiketli koz helvası dağıtıcıları arasındaki pazar paylaşımı anlaşması yapmaları nedeniyle ihlale sebebiyet veren AyM ve diğer koz helvası üreticilerine 11,6 milyon euro para cezası uygulanmıştır (Durantez ve Contreras 2016, 2).

⁸⁰ CNMC: Comisión Nacional de los Mercados y la Competencia.

⁸¹ Bkz. CNMC’nin 07.04.2016 tarihli ve Case /DC/0503/14 *Fabricantes de Turrón* kararı.

4.2.2. Macaristan Uygulaması

Macaristan’da rekabet ihlalleriyle ilgili incelemeler, Macaristan Rekabet Otoritesi (GVH⁸²) tarafından 1996 yılında yürürlüğe giren Macaristan Rekabet Kanunu kapsamında gerçekleştirilmektedir. İlgili kanunun 65. maddesinin birinci paragrafı kapsamında teşebbüsler, bir bilgi işlem sisteminde veya bir dijital veri saklama cihazında kaydettikleri verileri, okuma ve kopyalamaya uygun formatta ilgili otoriteye sunmakla yükümlü kılınmışlardır. GVH tarafından gerçekleştirilen Yİ’lerde uygulanan kanunun ilgili maddesi kapsamında adli bilişim araçları da kullanılmaktadır. Turi (2014, 1) ilgili otorite tarafından gerçekleştirilen Yİ’lerde tablet ve cep telefonlarının da inceleme kapsamına girebileceğini belirtmektedir.

2011 yılında Budapeşte Belediyesi tarafından 12 hastane için gerçekleştirilecek ilaç temini ihalesi kapsamında iki farklı şirketten ihale kapsamında danışmanlık hizmeti alınmış, bahse konu danışman şirketler kartelin diğer ayağını oluşturan üç teşebbüsün ihaleyi alması adına şartnameyi kartel adına uygun hale getirmişlerdir. 9 Nisan 2013 tarihinde Macaristan Rekabet Otoritesi tarafından gerçekleştirilen Yİ’lerde kartel üyelerinden PharmAudit adlı teşebbüsün temsilcisinin cep telefonunda inceleme gerçekleştirilmiş ve GVH tarafından cep telefonundan ve arama kayıtlarından elde edilen deliller dosya kapsamında kullanılmıştır (Petrányi vd. 2015, 1). İlgili otoritenin 14.09.2015 tarihli kararında⁸³ devam eden tek bir ihlal ve rekabeti kısıtlayıcı etkilerden dolayı karteli oluşturan şirketlere yaklaşık 8 milyon euro paza cezası uygulanmıştır⁸⁴.

4.2.3. Hollanda Uygulaması

Hollanda’da rekabet ihlalleriyle ilgili incelemeler, Hollanda Rekabet Otoritesi (ACM⁸⁵) tarafından Hollanda Genel İdari Usul Kanunu’nun 5:17. maddesinin verdiği yetki kapsamında gerçekleştirilmektedir. Anılan maddede, rekabet incelemesini gerçekleştiren uzmanların bilgi ve belgelerin kopyasını almaya yetkili oldukları ifade edilmektedir. İlgili otorite tarafından dijital verilerin incelenmesiyle ilgili prosedür de yayımlanmıştır. ACM, ofis ve endüstriyel

⁸² GVH: Gazdasági Versenyhivatal.

⁸³ Dosya Numarası: Vj-28/2013/506 ve Karar Tarihi: 14 Eylül 2015.

⁸⁴ http://www.gvh.hu/en//data/cms1033603/Vj028_2013_a_sz.pdf, Erişim Tarihi: 26.12.2016.

⁸⁵ <https://www.acm.nl/en/publications/publication/15446/Dutch-General-Administrative-Law-Act/>, Erişim Tarihi: 31.01.2017.

aynı *Hazır Beton* kararında ikincil deliller kapsamında yer alan delillerin en sık rastlanılan örnekleri:

(...) telefon görüşmesi kayıtları, teşebbüslerin ortak bir varış noktasına seyahat ettiklerini gösteren kayıtlar, belirli bir toplantı veya etkinliğe katılımı gösteren deliller, konaklama veya toplantı salonu kiralanmasına ilişkin faturalar ile rakiplerle ticari sır niteliğindeki hususların görüşüldüğüne ilişkin bilgi içeren ancak uzlaşmanın sağlandığını tek başına ispatlayamayan toplantı notları ve iç yazışmalarıdır.

olarak gösterilmektedir.

Yİ’lerde elde edilen delillerin fiziksel veya dijital ortamda elde edilip edilmediğinden ziyade elde edilen delillerin içeriğinin önemli olduğundan hareketle, mobil cihazlardan elde edilen dijital delillerin birincil ve ikincil delil kapsamında değerlendirilmesinin mümkün olduğu düşünülmektedir. Ayrıca mobil cihaz kullanım oranlarının artmasıyla birlikte iletişimin büyük ölçüde bu cihazlarla gerçekleştirilmesi, birincil ve ikincil delillerin mobil cihazlarda bulunma olasılığını da arttırmaktadır. İspat gücü yüksek delillerin elde edilmesinin istisnai hale geldiği (Can 2012, 18) bu süreçte, teşebbüslere ait mobil cihazların incelenmesiyle elde edilecek olan birincil ve ikincil delil kapsamındaki dijital delillerin, ispat faaliyetini önemli ölçüde kolaylaştıracağı öngörülmektedir.

4.3.2. 4054 Sayılı Kanun’un Yİ’lerde Kuruma Verdiği Yetki

Kanun’un (4054 Sayılı Rekabetin Korunması Hakkında Kanun) 15. maddesinin birinci fıkrasında,

Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin:

a) Defterlerini, her türlü evrak ve belgelerini inceleyebilir ve gerekirse suretlerini alabilir,

ifadeleri yer almaktadır. Bu bağlamda Kurul’un, 15. maddeden aldığı yetkiyle bilgisayar ve bilgisayar sistemlerinde inceleme gerçekleştirebildiği ve örneğin

*Araç Lastiği*⁸⁷, *Sinema*⁸⁸, *3M*⁸⁹, *Turkcell*⁹⁰ ve *Bankacılık*⁹¹, gibi birçok kararda dijital delillerden yararlandığı anlaşılmaktadır.

Bu noktada, elektronik ortamda yer alan verilerle ilgili olarak “*Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Tasarısı’nın*” 15. maddesinin birinci fıkrasındaki düzenlemeye değinilmesinin önemli olduğu değerlendirilmektedir.

Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin ve bunların yöneticilerinin ve çalışanlarının:

a) Defterlerini veya **her türlü ortamda tutulan veri** ve belgelerini inceleyebilir, bunların **her türlü kopya ve çıktılarını** alabilir.

Bahse konu Kanun tasarısının ilgili maddesinin gerekçesindeyse şu ifadelere yer verilmektedir:

(...) yerinde incelemelerde; defterlerin veya her türlü ortamda tutulan verilerin, bilgi ve belgelerin incelenebilmesi, bunların bulunduğu **elektronik ortamların imajlarının alınması dâhil her türlü kopya ve çıktılarının alınabilmesi** yetkisi (...) tanımlanmıştır.

Kanun’un 15. maddesi kapsamında teşebbüs veya teşebbüs birliklerinde gerçekleştirilen Yİ’lerde, incelemeler sadece teşebbüse ait istemci⁹² ve sunucularda⁹³ gerçekleştirilmekte olup, mobil cihazların⁹⁴ Yİ uygulamalarında *BYOD* uygulaması gözetmeksizin meslek personeline inceleme konusu yapılmadığı görülmektedir. Bununla birlikte, Yİ’lerde herhangi bir adli bilişim aracı da kullanılmamaktadır.

⁸⁷ 16.12.2015 tarihli ve 15-44/731-266 sayılı Kurul kararı (*Araç Lastiği*).

⁸⁸ 20.11.2015 tarihli ve 15-41/682-243 sayılı Kurul kararı (*Sinema*).

⁸⁹ 25.06.2014 tarihli ve 14-22/461-203 sayılı Kurul kararı (*3M*).

⁹⁰ 01.10.2014 tarihli ve 14-37/702-310 sayılı Kurul kararı (*Turkcell*).

⁹¹ 08.03.2013 tarihli ve 13-13/198-100 sayılı Kurul kararı (*Bankacılık*).

⁹² *Windows, Mac OS X* vb. işletim sistemine sahip, teşebbüse ait masaüstü veya dizüstü bilgisayarlar.

⁹³ *Windows Server* versiyonlarını veya *Linux* sunucu dağıtımlarını kullanan sabit teşebbüs sunucuları.

⁹⁴ *Android, iOS, Windows Phone OS* vb. gibi işletim sistemlerine sahip akıllı telefonlar, tabletler veya temel özelliklere sahip cep telefonları.

4.3.3. Mevzuatta Yer Alan Diğer Düzenlemeler

Kanun'un 15. maddesinin mobil cihazların Yİ'lerde incelenmesi konusunda meslek personeline yetki verip vermediğinin tespiti amacıyla yürürlükte bulunan mevzuattaki düzenlemelere yer verilmesinin uygun olacağı değerlendirilmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesinin birinci fıkrasında:

Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı **bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına**, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

hükümleri yer almaktadır⁹⁵.

CMK'nin 134. maddesinin diğer fıkraları da incelendiğinde mobil cihazlarla ilgili herhangi bir ifadenin yer almadığı görülmektedir. Özen ve Özocak (2015, 71) bilgisayara benzer özellikleri nedeniyle cep telefonlarının da bilgisayarlarla aynı düzenlemeye tabi kılınması gerektiğini ifade etmektedirler. Bahse konu maddede cep telefonu veya akıllı telefon kavramları geçmemesine rağmen adli kolluk kuvvetlerinin suçu aydınlatma noktasında mobil cihazlara el koyma ve el koyulan cihazlarda adli bilişim incelemeleri yapma yetkilerine sahip oldukları ve uygulamada bunu gerçekleştirdikleri bilinmektedir.

6362 Sayılı Sermaye Piyasası Kanunu'nun 89. maddesinin birinci fıkrasında denetimle görevlendirilen personelin denetim yetkilerinin bir kısmı,

(...) **elektronik ortamda tutulanlar dâhil tüm kayıtlar** ve sair bilgi ihtiva eden vasıtaları, bilgi sistemlerini incelemeye, bunlara erişimin sağlanmasını istemeye ve **bunların örneklerini almaya**, ...

ifadeleriyle belirtilirken, 5411 Sayılı Bankacılık Kanunu'nun 95. maddesinde denetim yapmaya yetkili meslek personelinin incelemeyle ilgili yetkilerinin bir kısmı,

⁹⁵ Aynı hükümler Adli Ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde de yer almaktadır.

(...) **tüm bilgi işlem sistemini** denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, verilerin güvenliğini sağlamakla ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin **mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını** ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle...

ifadeleriyle sıralanmaktadır.

4.3.4. Mobil Cihazlarda Adli Bilişim Araçlarının Kullanılmasına İlişkin Yetki Tartışması

Kurul'un uyguladığı mevzuatla birlikte farklı mevzuat incelendiğinde, diğer kanunlarda;

- “(...) bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına⁹⁶ (...), ,
- (...) bilgisayar kayıtlarından kopya çıkarılmasına⁹⁷ (...),
- (...) elektronik ortamda tutulanlar dâhil⁹⁸ (...),
- (...) tüm bilgi işlem sistemini, mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını⁹⁹ (...)”

gibi açık ifadeler yer almasına rağmen Kanun'da dijital ortamdaki verilerle ilgili açık bir ifade yer almamakta, fakat Kanun'un 15. maddesinde geçen “*Defterlerini, her türlü evrak ve belgelerini inceleyebilir ve gerekirse suretlerini alabilir,*” ifadesi bulunmaktadır. Bu bağlamda mobil cihazların Yİ'lerde incelenmesi konusunda mevcut Kanun'un incelemeye yetki verip vermediğinin tespitinin hukuksal anlamda tartışılması gerektiği düşünülmektedir.

Bu noktada, Kurul'un Yİ'lerde mobil cihazların incelenmesi konusundaki yetkilerinin geniş mi yoksa dar mı yorumlanacağı konusu önem kazanmaktadır.

⁹⁶ 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi.

⁹⁷ Adli Ve Önleme Aramaları Yönetmeliği'nin 17. maddesi.

⁹⁸ 6362 Sayılı Sermaye Piyasası Kanunu'nun 89. maddesi.

⁹⁹ 5411 Sayılı Bankacılık Kanunu'nun 95. maddesi.

Anayasa Mahkemesi yetkisizliğin kural, yetkili olmanın istisna olduğunu belirttiği kararında¹⁰⁰ şu ifadeler yer almaktadır:

İdare Hukukunda “yetki”, idareye Anayasa ve yasalarla tanınmış olan karar alma gücünü ifade eder ve idari işlemlerin en temel ögesini oluşturur. Bir kamu düzeni sorunu olan yetki, yasa koyucu tarafından hangi makam veya merciye verilmiş ise, ancak o makam veya merci tarafından kullanılabilir. Bu bakımdan, yasanın açık izni olmadıkça yetkili makam veya mercinin yetkisini devretmesi olanaklı değildir. Aktarılan nitelikleri gereği, idare hukukunda **yetkisizlik kural, yetkili olmak istisnadır**. Bu itibarla, yetki hükümlerinin sınır ve çerçevesinin yasayla **açıkça** çizilmesi gerekir **ve genişletici yoruma tabi tutulamaz**.

Akıllıoğlu (1978, 73) yönetimin kullandığı yetkilerin kapsamlarının belirlenmesinin önemini belirterek, yetki kullanımı konusunu şu şekilde ifade etmektedir:

Yetki konusunun dar biçimde yorumlanması yönetimin işleyişini engelleyici, geniş biçimde yorumlanması da yönetilenlerin davranışlarını hukuka aykırı biçimde kısıtlayıcı sonuçlara yol açabilir.

Kekevi (2008, 119), kartellerle etkin bir şekilde mücadele edilmesi için Yİ yetkisinin rekabet otoritelerine verilmesine dair genel bir kabul olduğunu belirtmektedir. Yİ’lerin sınırları Devrim (2009, 59) tarafından, Kurul’un verdiği yetki belgesinde **incelemenin konusunun ve amacının** yer aldığını ve bu kapsamda incelemelerin sınırlarının çizilerek, teşebbüslerde keşif aramasının yapılmadığı şeklinde ifade edilmektedir.

Gündüz (2009, 18), Yİ’lerin rekabet otoritelerinin en önemli delil toplama yöntemlerinden biri olduğunu ve bu bağlamda rekabet otoritelerine **geniş yetkiler tanımlandığını** belirterek, yetkilerin kullanımında teşebbüs yönetici ve çalışanlarının özel hayatın ve haberleşmenin gizliliği gibi haklarına müdahalelerin söz konusu olabileceğine değinmektedir¹⁰¹. Coşgun (2009, 65) yönetici ve çalışanlara ait kişisel bilgisayarların imajlarının alındığı durumlarda özel hayatın gizliliğin korunmasının da önem kazanacağını ve bu durumun “temel haklara

¹⁰⁰ Anayasa Mahkemesi, 08.11.2012, E: 2012/27, K: 2012/173, RG 28.03.2013, S:28601, <http://www.resmigazete.gov.tr/eskiler/2013/03/20130328-9.htm>, Erişim Tarihi: 31.01.2017.

¹⁰¹ Bu durumla birlikte Kekevi (2008, 120), başta ABD ve AB olmak üzere farklı rekabet otoritelerinin konutlarda da Yİ yapabildiğini fakat Kurum’un konutlarda Yİ yetkisinin olmadığını ve konunun Kanun’da değişiklikle çözüme kavuşturulması gerektiğini belirtmektedir.

saygı gösterilmesi zorunluluğu açısından da” değerlendirilmesi gerektiğini ifade etmektedir.

Bu bilgiler ışığında Kanun’un mevcut hükümlerinin geniş biçimde yorumlanması durumunda,

- Teşebbüs tarafından çalışanlarına sağlanan, aylık faturası teşebbüs tarafından ödenen ve dolayısıyla satın alma faturaları muhasebe kayıtlarında yer almış mobil cihazların,
- Teşebbüsün *BYOD* politikası kapsamında yer alan cihazların,
- Teşebbüs çalışanlarının mesai saatleri içinde iş amaçlı kullandıkları cihazların (teşebbüse ait kurumsal e-postaların ve teşebbüsün elektronik iş akışlarıyla ilgili mobil uygulamaların kurulu bulunduğu),

Yİ’lerde incelenebileceği değerlendirilmektedir. Kanun’un geniş biçimde yorumlanması durumunda mobil cihazlardan *fiziksel* veri elde etme yöntemiyle veri elde edilmesinden ziyade *manuel* veya *mantıksal* veri elde etme yöntemlerinin kullanılabileceği düşünülmektedir.

Yİ’lerde mobil cihazlardan *rootlama* veya *jailbreak* ile *fiziksel* veri elde yöntemiyle veri elde edilmesi gerektiğinde, Kanun’un ne şekilde yorumlanacağını tartışılması gereken bir başka konu olduğu değerlendirilmektedir. Çalışmanın önceki bölümlerinde değinildiği gibi bazı adli bilişim araçları mobil cihazlardan *fiziksel* olarak veri elde etmek için *rootlama* veya *jailbreak* tekniklerini kullanmaktadır. Her ne kadar *rootlama* veya *jailbreak* teknikleri teşebbüs çalışanın mobil cihazındaki kişisel verileri etkilememekte ve yapılan işlem sistem dosyaları düzeyinde kalsa da teşebbüs çalışanın mobil cihazına adli bilişim teknikleriyle müdahale edilmesi durumu söz konusudur.

Kurul’un mevcut uygulamasında, Yİ’lerde adli bilişim araçları kullanılmamakta ve mobil cihazlarla ilgili bir işlem yapılmamaktadır. Bu durumdan yola çıkarak, Kurum’un Yİ’lerde adli bilişim tekniklerinden yararlanmaması nedeniyle incelemelerin etkinliğinin giderek azaldığı gözlemlenmektedir. Dolayısıyla orta veya uzun vadede Yİ’lerin inceleme vasfını kaybedeceği ve incelemelerin teşebbüslere yapılan rutin kontrollere dönüşeceği öngörülen bir

farklı durum olarak ortaya çıkmaktadır. Yİ'lerin vasfını giderek kaybetmesi nedeniyle Kurum'un teşebbüsler üzerindeki caydırıcılığının giderek azalması durumunun, göz önünde bulundurulması gereken bir diğer önemli husus olduğu değerlendirilmektedir.

Sonuç olarak, mobil cihazlar gibi kişisel veri yoğun cihazların incelenmesinde hem meslek personelinin yetki sınırlarını bilmesi hem de teşebbüs çalışanlarının temel hak ve özgürlüklerinin kısıtlanmaması için yasal altyapının tüm sorulara cevap verecek şekilde revize edilmesinin en uygun çözüm olacağı kanaatine varılmaktadır.

SONUÇ

Kartellerin faaliyetlerini gizlemek amacıyla dolaylı yöntemler kullanması ve rakipler arasındaki iletişimde açık bilgilerin yer almaması nedeniyle birincil delillere erişim gün geçtikçe daha da güç hale gelmektedir (Can 2012, 23). Bu duruma ek olarak, Kurum'un Yİ'lerde delil elde etme yöntemleri gelişim göstermezken teşebbüsler işledikleri rekabet ihlallerini gizlemek amacıyla teknolojinin tüm imkanlarını kullanmaktadır. Yİ'lerde hiçbir adli bilişim aracının kullanılmamasıyla birlikte mobil cihazların da inceleme konusu yapılmamasının Kurum'un rekabet ihlallerini ortaya çıkarma ve caydırma noktasındaki etkinliğini azalttığı da yadsınamaz bir gerçektir. Teşebbüslerin çalışanlarına akıllı telefon ve tablet gibi birden fazla mobil cihaz sağlayabildiği günümüz dünyasında, meslek personelinin Yİ'lere ayrılan süreyi teşebbüs çalışanlarının sadece masaüstü ve dizüstü bilgisayarlarındaki e-posta ve belgeleri inceleyerek geçirmelerinin rekabet ihlallerinin tespiti noktasında etkinsizliğe sebebiyet verdiği açıktır.

Yİ'lerde mobil cihaz incelemeleri, dijital verinin korunması, elde edilmesi, incelenmesi ve raporlanması gibi bir takım adli bilişim süreçlerini de kapsayacak şekilde gerçekleştirilmelidir. Bu süreçler kapsamında dijital veri elde edilirken kullanılacak olan adli bilişim araçlarının, farklı otoritelerce yapılan testleri geçmesi ve adli bilişim dünyasında kabul edilen standartları karşılaması gerekmektedir (Baggili vd. 2007, 2). Ayrıca meslek personelinin Yİ'lerde mobil cihazlardan veri elde etmesi için adli bilişim disiplininin gereklerine hâkim olması da oldukça önemlidir.

Çalışmada, Yİ'lerin Kurumla teşebbüsler arasındaki bir silahlanma yarışına sahne olduğundan hareketle, bu yarışta Yİ'lerde mobil cihazların incelenmesinin Kurum'a ne tür faydalar sağlayacağı araştırılmıştır. Bu kapsamda mobil cihaz ve mobil cihazlarda adli bilişim kavramları hakkında bilgi aktarılmış,

sonrasında adli bilişim araçları kullanılarak örnek olay kapsamında rekabet ihlaline yönelik delil incelemesi gerçekleştirilmiştir. Örnek ülke uygulamalarıyla ilgili bilgiler aktarıldıktan sonra Yİ’lerde mobil cihazların incelenmesi bakımından ülkemizdeki durumla ilgili yetki tartışmasıyla çalışma sonlandırılmıştır. Çalışmada, Yİ’lerde mobil cihazların incelenmemesinin, teşebbüslerin rekabeti ihlal etme motivasyonlarını arttırdığı, Kurum’un Yİ’lerde mobil cihazları inceleme kapasitesine sahip olduğu fakat bu kapasitenin kullanılması için sahip olunması gereken yetkiye ait tartışmanın hukukçulara bırakılması gerektiği sonucuna ulaşılmıştır.

Son olarak, Kanun’un mobil cihazlarda adli bilişimi de içerek şekilde düzenlenmesinin ve Yİ’lerde adli bilişim araçlarının kullanılması yetkisinin açıkça meslek personeline verilmesinin, serbest piyasa düzeninin korunması ve Kurum’un rekabet ihlalleri açısından caydırıcılığının artırılması hususunda ülkemizin menfaatine olacağı değerlendirilmektedir.

ABSTRACT

It is clear that mobile devices are essential part of daily and business life. Many undertakings provide smartphones or tablets to their employees to make them mobilized. EU Commission and many EU member states investigate mobile phones at dawn raids. Investigating mobile devices at dawn raids is a new position. Mobile forensics can improve evidence quality for authorities. Turkish Competition Authority (TCA) has the ability but not a clear legal power to use mobile forensic techniques like other EU member states. For instance, using forensic tools at dawnraids is not applicable in the existing procedure of the TCA related to dawnraids.

This paper especially focuses on mostly technical part of mobile forensics rather than legal aspects of law issues. Furthermore, paper includes a sample mobile device investigation related to a fiction cartel case. Main goal of this paper is to examine mobile devices, mobile forensics, digital evidence related to mobile devices and procedures to be followed by TCA during dawnraids and the urgent need for legal regulations to give the Authority exact power to carry out computer and mobile forensic investigations.

KAYNAKÇA

AGARWAL, A., M. GUPTA, S. GUPTA ve S. C. GUPTA (2011), “Systematic Digital Forensic Investigation Model”, *International Journal of Computer Science and Security (IJCSS)*, Vol:5, Is:1, s.118-131.

AISWARYA, P. S. (2016), “A Study on Existing Trends for Forensic Examination of Social Networking Applications on Android Phones”, *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, Vol:3, Is:5, s.98-104.

AKILLIOĞLU (1978), “Saklı Yetki Kavramı”, *Amme İdaresi Dergisi*, Cilt II, Sayı 3, Eylül 1978, s.73-83, http://www.todaie.edu.tr/resimler/ekler/05f50528627af5b_ek.pdf?dergi=Amme%20Idaresi%20Dergisi, Erişim Tarihi: 13.11.2016.

ALGHAFI, K. A., A. JONES ve T. A. MARTIN (2011), “Guidelines for the Digital Forensic Processing of Smartphones”, *Australian Digital Forensics Conference*, s.1-8, <http://ro.ecu.edu.au/adf/90/>, Erişim Tarihi: 30.10.2016.

AL-HADADI ve M., A. ALSHIDHANI, (2013), “Smartphone Forensics Analysis: A Case Study”, *International Journal of Computer and Electrical Engineering*, Vol:5, No:6, s.576-580, <http://ijcee.org/papers/776-S0005.pdf>, Erişim Tarihi: 19.10.2016.

ANOBAN, M., S. SALEEM ve O. POPOV (2014), “Testing Framework for Mobile Device Forensics Tools”, *The Journal of Digital Forensics, Security and Law: JDFSL*, Vol:9, Is:2, s.221-234, <http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/281/226>, Erişim Tarihi: 10.10.2016.

AYERS, R., S. BROTHERS ve W. JANSEN (2014), “Guidelines on Mobile Device Forensics”, National Institute of Standards and Technology, Special Publication 800-101, Rev:1, s.1-75, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>, Erişim Tarihi: 30.10.2016.

BADER, M. ve I. BAGGILI (2010), “iPhone 3GS Forensics: Logical Analysis Using Apple iTunes Backup Utility”, *Small Scale Digital Device Forensics Journal*, Vol. 4, No.1, s.1-15.

- BAGGILI, I. M., R. MISLAN, M. ROGERS (2007), “Mobile Phone Forensics Tool Testing: A Database Driven Approach”, *International Journal of Digital Evidence*, Vol:6, Is:2, s.1-11.
- BATTY, P. ve A. SCOTT (2016), “SQLite Visualiser: Building A Tool to Visualise the SQLite File Format and Log All Changes”, http://www.lancaster.ac.uk/undergrad/battyp/docs/battyp_sqlite_visualiser_report.pdf Erişim Tarihi: 28.11.2016.
- BHOSALE, S. T., T. PATIL ve P. PATIL (2015), ”SQLite: Light Database System”, *International Journal of Computer Science and Mobile Computing*, Vol:4, Is:4, s.882-885, <http://ijcsmc.com/docs/papers/April2015/V4I4201599a35.pdf>, Erişim Tarihi: 28.11.2016.
- BOLAT Y. (2015), “Memory Forensics”, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Ve Teknoloji Hukuku Yüksek Lisans Tezi.
- BROTHERS, S. (2014), “NIST Mobile Forensics Workshop and Webcast, Mobile Device Forensics: A - Z”, https://www.nist.gov/sites/default/files/document/s/forensics/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf, Erişim Tarihi: 28.01.2017.
- CAN, B. (2012), “Rekabet Hukukunda Kartellere İlişkin İspat Standardı”, Rekabet Kurumu Uzmanlık Tezleri Serisi, No:123, Ankara.
- CARRIER, B. (2003), “Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers”, *International Journal of Digital Evidence*, Vol:1, Is:4, s.1-12, http://www.digital-evidence.org/papers/ijde_define.pdf, Erişim Tarihi: 10.10.2016.
- CASEY E. ve TURNBULL B. (2011), “Digital Evidence on Mobile Devices”, http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf, Erişim Tarihi: 28.01.2017.
- CHANG, Y. T., K. C. TENG, Y. C. TSO ve S. J. WANG (2015). “Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence”, *Journal of Computers*, Vol:26, No:2, s.19-33, <http://csroc.org.tw/journal/JOC26-2/JOC26-2-4.pdf>, Erişim Tarihi: 01.10.2016.
- COLLINSON A., C. PÉREZ-ABAD ve D. ROSKIS (2015), “Pushing the (Sealed) Envelope? The European Commission’s Revised Explanatory Note on Dawn Raids”, <http://www.lexology.com/library/detail.aspx?g=d06712db-aa70-4f62-9dc7-087662d245ea>, Erişim Tarihi: 31.12.2016.
- COŞGUN, H. (2009), “ABD, AB ve Türk Otoritelerinin Bilgi Edinme Yetkileri

ve Bilgi Kaynağı olarak Fonksiyonları”, Rekabet Kurumu Uzmanlık Tezleri Serisi No.107, Ankara.

CROFT, N. J. ve M. S. OLIVIER (2006), “Sequenced Release of Privacy Accurate Call Data Record Information in a GSM Forensic Investigation”, *ISSA*, s.1-14.

ÇAKIR H. (2014), “Mobil Cihazların İncelenmesi”, ÇAKIR H. ve S. KILIÇ (der.), *Adli Bilişim ve Elektronik Deliller* içinde, Seçkin Yayıncılık, Ankara, s.373-409.

DAS, S. K. (2016), “*Mobile Terminal Receiver Design, LTE and LTE – Advanced*”, Wiley, Hindistan.

DASHTI M., L. ROOHI ve R. MOIENI (2013), “Mobile Forensics Opportunities and Challenges in Data Preservation”, *IOSR Journal of Engineering (IOSRJEN)*, Vol:3, Is:8, s.23-29.

DAVYDOV O. (2014), “Mobile Phone Forensics Challenges”, <https://www.forensicmag.com/article/2013/02/6-persistent-challenges-smartphone-forensics>, Erişim Tarihi: 28.01.2017.

DEDECHE, A., F. LIU, M. LE ve S. LAJAMI (2013). “Emergent BYOD Security Challenges and Mitigation Strategy, The University of Melbourne, https://minerva-access.unimelb.edu.au/bitstream/handle/11343/33340/300297_2013_Lajami_Strategy.pdf?sequence=1, Erişim Tarihi: 07.11.2016.

DETHMERS F., F. MULLER ve C. CHANCE (2016), “Restrains of trade and dominance in the Netherlands: Overview”, <http://uk.practicallaw.com/3-573-8205?q=&qp=&qo=&qe=>, Erişim Tarihi: 31.01.2017.

DEVİRİM, F. (2009), “İdare Hukunda ve Ceza Hukukunda Kartellerle Mücadelede Kullanılan Soruşturma Yöntemleri”, Rekabet Kurumu Uzmanlık Tezleri Serisi No. 102, Ankara.

DHINGRA, M. (2016), “Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)”, *Procedia Computer Science*, Vol:78 s.179-184.

DIXIT, P. K. (2014), “*Android*”, Vikas Publishing House Pvt. Ltd., India.

DOURY N. J., J. ELLISON, J. P. SCHMIDT ve D. M. HARRISON, “EU Dawn Raids: the Updated Inspection Explanatory Note Sends a Clear Message” <https://www.mayerbrown.com/EU-Dawn-Raids-the-Updated-Inspection-Explanatory-Note-Sends-a-Clear-Message-10-01-2015/>, Erişim Tarihi: 29.01.2017.

DUBEY A. Ve A. MISRA (2013), “*Android Security: Attacks and Defenses*”, CRC Press, FL.

DURANTEZ H. G. ve M. CONTRERAS (2016), ““WhatsApp” and Mobile

Phones: The Spanish Antitrust Regulator Bolsters Its Powers to Uncover Cartels”, <http://www.lexology.com/library/detail.aspx?g=079974c4-0c4d-4dec-b050-f051ec82e52f>, Erişim Tarihi: 20.11.2016.

ENGLER R. ve C. M. MILLER (2013), “6 Persistent Challenges with Smartphone Forensics”, <https://www.forensictmag.com/article/2013/02/6-persistent-challenges-smartphone-forensics>, Erişim Tarihi: 28.01.2017.

EPIFANIM. ve P. STIRPARO (2015), “*Learning iOS Forensics*”, Packt Publishing Ltd, Birmingham – Mumbai.

ERPS, D. V. ve N. J. DOURY (2013), “Digital Evidence Gathering: An Up-Date”, *Concurrences*, No:2-2013, s.213-219.

FARJAMFAR A., M. T. ABDULLAH, R. MAHMOD ve N. I. UDZIR (2014), “A Review On Mobile Device’s Digital Forensic Process Models”, *Research Journal of Applied Sciences, Engineering and Technology* Vol:8, No:3, s.358-366.

FRENCH, A. M., C. GUO ve J. P. SHIM (2014), “Current Status, Issues, and Future of Bring Your Own Device (BYOD)”, *Communications of the Association for Information Systems*, Vol:35, Article: 10, s.192-19.

GONZALEZ J., J. HUNG ve S. FRIEDBERG (2011), “Mobile Device Forensics: A Brave New World, Bloomberg Law Reports”, http://files.dorsey.com/files/upload/NYC12_BillionDollarMobileDeviceForensics.pdf, Erişim Tarihi: 18.10.2016.

GOVINDARAJ, J., R. VERMA, R. A. MATA ve G. GUPTA (2014), “Poster: iSecureRing: Forensic Ready Secure iOS Apps for Jailbroken iPhones”, *35th IEEE Symposium on Security and Privacy*, <http://www.ieee-security.org/TC/SP2014/posters/GOVIN.pdf>, Erişim Tarihi: 01.10.2016.

GÜNDÜZ, H. (2009), “Avrupa İnsan Hakları Sözleşmesi’nin Rekabet Hukuku Uygulamasına Etkisi”, Rekabet Kurumu Uzmanlık Tezleri Serisi No. 99, Ankara.

HAARTSEN, J. C. (2000). “The Bluetooth Radio System”, *IEEE Personal Communications*, Vol:7 No:1, s.28-36.

HAYES, D. R. (2015), “*A Practical Guide to Computer Forensics Investigations*”, Pearson, Amerika Birleşik Devletleri.

HEBERT M, K. PANG, W. WENG, R. SOU ve R. KADIYALA (2008), “3G Telecommunications: Innovative Designs of Cellular Phones, SHAHI, G. Ve J. GRECO (der.), *Financing Technology Innovation* içinde, CSEM ve GBI Books, Amerika Birleşik Devletleri, s.19-28.

HENKOĞLU, T. (2014), *Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi*,

Pusula Yayınları Güncellenmiş 2. Baskı, Ankara.

HOLT, T. J., A. M. BOSSLER ve K. C. SEIGFRIED-SPELLAR (2015), “*Cybercrime and Digital Forensics: An Introduction*”, Routledge, Oxon.

HOOG A. ve K. STRZEMPKA (2011), “*iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*”, Elsevier, Amerika Birleşik Devletleri.

HOSMER, C. (2017), “*Integrating Python with Leading Computer Forensics Platforms*”, Syngress, India.

HUDDLESTON R. (2012), “*Android Fully Loaded Second Edition*”, Wiley Publishing, Amerika Birleşik Devletleri.

ICN (2014), “Anti-Cartel Enforcement Manual Cartel Working Group Subgroup 2: Enforcement Techniques, Chapter Digital Evidence Gathering”, <http://www.internationalcompetitionnetwork.org/uploads/library/doc1006.pdf>, Erişim Tarihi: 23.10.2016.

JAMES, J. I., A. F. SHOSHA ve P. GLADYSHEV (2012), “Digital Forensic Investigation and Cloud Computing”, RUAN, K. (der.), *Cybercrime and Cloud Forensics: Applications for Investigation Processes* içinde, Information Science Reference, Amerika Birleşik Devletleri, s.1-41.

JAMES, K. L. (2012), “*Linux: Learning the Essentials*”, PHI Learning Private Limited, Haryana.

JONES, A., ve C. VALLI (2008), “*Building a Digital Forensic Laboratory 1st Edition Establishing and Managing a Successful Facility*”, Syngress, Burlington, MA.

JOSHI, R. C. ve E. S. PILLI (2016), “*Fundamentals of Network Forensics, A Research Perspective*”, Springer, Birleşik Krallık.

KEKEVİ, H. G. (2008), “ABD, AB ve Türk Rekabet Hukukunda Kartellerle Mücadele”, Rekabet Kurumu Lisansüstü Tez Serisi, No. 15, Rekabet Kurumu, Ankara.

KINSELLA, S. (2015), “Call My Bluff”, <http://kluwercompetitionlawblog.com/2015/10/20/call-my-bluff/>, Erişim Tarihi: 29.01.2017.

KUSCHEWSKY, M. ve D. GERADIN (2013), “Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges. *Tilburg Law School Research Paper*, 2013, 020”, <http://awards.concurrences.com/IMG/pdf/data.pdf>, Erişim Tarihi: 07.11.2016.

LESSARD, J. ve G. C. KESSLER (2010), “Android Forensics: Simplyfing Cell Phone Examinations”, *Small Scale Digital Device Forensics Journal*, Vol:4, No:1, s.1-12.

LONE, A. H., F .A. BADROO, R. C. KHAIRAJ ve A. KHALIQUE (2015), “Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications”, *International Journal of Computer Applications*, Vol:128 No:12 s.26-33.

MAHALIK, H., R. TAMMA ve S. BOMMISETY (2016), “*Practical Mobile Forensics Second Edition*”, Packt Publishing, Birmingham - Mumbai.

MARAS, M. H. (2015), “*Computer Forensics, Cybercriminals, Laws, and Evidence*”, Jones & Bartlett Learning, Amerika Birleşik Devletleri.

MARCELLA, A. J. ve D. MENENDEZ (2007), “*Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition*”, Auerbach Publications, FL.

MILLER, K. W., J. VOAS ve G. F. HURLBURT (2012), “BYOD: Security and Privacy Considerations”, *IT Professional*, Vol:14, s.53-55.

MURPHY, C. A. (2009), “Developing Process for Mobile Device Forensics”. <https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf>, Erişim Tarihi: 27.09.2016.

NELSON B., A. PHILLIPS, C. STEUART (2015), “*Guide to Computer Forensics and Investigations Processing Digital Evidence, Fifth Edition*”, Cengage Learning, Boston.
OECD (1998), “Recommendation of the Council Concerning Effective Action Against Hard Core Cartels”, <https://www.oecd.org/daf/competition/2350130.pdf>, Erişim Tarihi: 27.12.2016.

OECD (2006), “Policy Roundtables: Prosecuting Cartels without Direct Evidence”, <http://www.oecd.org/dataoecd/19/49/37391162.pdf>, Erişim Tarihi: 24.10.2016.

OECD (2013), “Latin American Competition Forum Session III: Unannounced Inspections in Antitrust Investigations, Contribution from Spain (CNC)”, [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF\(2013\)16&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2013)16&docLanguage=En), Erişim Tarihi: 20.11.2016.

ÖZBEK, M. (2013), “Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları”, *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, s.255-262.

ÖZEN, M. ve G. ÖZOCAK (2015), “Adli Bilişim, Elektronik Deliller ve

Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", *Ankara Barosu Dergileri*, Vol:73, Is:1, s.41-77.

ÖZTÜRKÇİ H. (2014), "Adli Bilişim İncelemelerinde Sabit Disk İmajları – Giriş", <http://halilozturkci.com/adli-bilisim-incelemelerinde-sabit-disk-imajlari/>, Erişim Tarihi: 28.01.2017.

PANCHAL, E. P. (2013), "Extraction of Persistence and Volatile Forensics Evidences from Computer System", *International Journal of Computer Trends and Technology (IJCTT)*, Vol:4, Is:5, s.964-968.

PETRÁNYI, D., V. KOVÁCS ve N. JEKKELE (2015), "Pharma Cartel Fined by the Hungarian Competition Office", <http://www.lexology.com/library/detail.aspx?g=dedb3366-6883-4c8d-b8a9-c07d2bb03426>, Erişim Tarihi: 26.12.2016.

POONIA, A. S. (2014), "Data Wiping and Anti Forensic Techniques", *Compusoft, An International Journal of Advanced Computer Technology*, Vol:3, Is:12, s.1374-1376.

PUNJA, S. G. ve R. P. MISLAN (2008). "Mobile Device Analysis", *Small Scale Digital Device Forensics Journal*, Vol:2, No:1, s.1-16.

QUICK, D., B. MARTINI ve K. R. CHOO (2013), "Cloud Storage Forensics", Syngress, Amerika Birleşik Devletleri.

RAGGI, E., K. THOMAS ve S. V. VUGT (2011), "Beginning Ubuntu Linux Natty Narwhal Edition", Apress The Expert's Voice in Linux Sixth Edition.

RAY, D. ve E. RAY (2015), "Unix and Linux Fifth Edition", Peachpit Press, Amerika Birleşik Devletleri.

REIBER, L. (2016), "Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation 1st Edition", McGraw-Hill Education.

SAHU, I. ve I. CHAKRABORTY (2013), "Understanding Location Manager in Android and Implementing an Optimal Image Geotagging Application", *International Journal of Computer Trends and Technology (IJCTT)*, Vol:4, Is:6, s.1682-1686.

SCHWAMM, R. ve N. C. ROWE (2014), "Effects of the Factory Reset on Mobile Devices", *Journal of Digital Forensics, Security and Law*, Vol:9, Is:2, s.205-219.

SIDHU, B., H. SINGH ve A. CHHABRA (2007), "Emerging Wireless Standards-WiFi, Zigbee and Wimax", *World Academy of Science, Engineering and Technology*, Vol:1, No:1, s.43-48.

SIMON, L. ve R. ANDERSON (2015), "Security Analysis of Android Factory

- Resets”, 4th Mobile Security Technologies Workshop (MoST), http://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf, Erişim Tarihi: 13.10.2016.
- SINDHU, K. K ve B. B. MESHRAM (2012),” Digital Forensics and Cyber Crime Datamining”. *Journal of Information Security*, Vol:3, s.196-201.
- SOPER, M. E. (2015), “*The PC and Gadget Help Desk, A Do-It-Yourself Guide to Troubleshooting and Repairing*”, QUE, Indianapolis, Indiana.
- SUN, S., A. CUADROS ve K. BEZNOSOV (2015), “Android Rooting: Methods, Detection, and Evasion”, *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, s.3-14.
- TAL, A. (2002), “Two Flash Technologies Compared: NOR vs NAND. White Paper of M-SYstems”, <https://focus.ti.com/pdfs/omap/diskonchipvsnor.pdf>, Erişim Tarihi: 20.10.2016.
- TAMMA, R. ve D. TINDALL (2015), “*Learning Android Forensics*”, Packt Publishing, Birmingham - Mumbai.
- TASSONE, C., B. MARTINI, K. K. R. CHOO ve J. SLAY (2013), “Mobile Device Forensics: A snapshot. Trends and Issues in Crime and Criminal Justice, (460), 1.” http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi460.pdf, Erişim Tarihi: 11.10.2016.
- TOMLIN, W. (2016), “How Mobile Has Changed the World”, <http://mobilebusinessinsights.com/2016/05/how-mobile-has-changed-the-world/>, Erişim Tarihi: 28.01.2017.
- TURI, A. (2014), “Hungary: Hungary & EU : What Would You Do If The Competition Authority Greeted You In Your Office?”, <http://www.mondaq.com/x/447358/Antitrust+Competition/d+You+Do+If+The+Competition+Authority+Greeted+You+In+Your+Office>, Erişim Tarihi 26.12.2016.
- WILLASSEN, S. Y. (2003), “Forensics and the GSM Mobile Telephone System”, *International Journal of Digital Evidence*, Vol:2, Is:1, s.1-17.
- WILS, W. P. J. (2006), “Optimal Antitrust Fines: Theory and Practice”, *World Competition*, Vol: 29, No: 2, June 2006.
- XU, W. ve Y. FU (2015), “Own Your android! Yet Another Universal Root, 9th USENIX Workshop on Offensive Technologies (WOOT 15)”, <https://www.blackhat.com/docs/us-15/materials/us-15-Xu-Ah-Universal-Android-Rooting-Is-Back-wp.pdf>, Erişim Tarihi: 1.11.2016.
- ZAREEN, A. ve S. BAIG (2010), “Mobile Phone Forensics: Challenges, Analysis

and Tools Classification”, *Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering*, s.47-55.

Diğer Kaynaklar

Bilişim Teknolojileri ve İletişim Kurumu (BTK) (2016), “Üç Aylık Pazar verileri Raporu, 2016 Yılı 2. Çeyrek Nisan – Mayıs -Haziran”, <http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fPazarVerileri%2f2016-Q2.pdf>, Erişim Tarihi: 29.09.2016.

Cisco (2017), “Global Mobile Data Traffic Forecast Update, 2016-2021”, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf>, Erişim Tarihi: 05.03.2017.

NUIX (2016a), “Nuix History”, <http://www.nuix.com/nuix-history>, Erişim Tarihi: 17.11.2016.

NUIX (2016a), “Nuix History”, <http://www.nuix.com/nuix-history>, Erişim Tarihi: 17.11.2016.

NUIX (2016b), “Nuix and Cellebrite Partner to Leverage Complementary Strengths in Mobile Device Forensics, Investigation and eDiscovery”, <https://www.nuix.com/media-releases/nuix-and-cellebrite-partner>, Erişim Tarihi: 17.11.2016.

NUIX (2016b), “Nuix Investigator Lab”, <https://www.nuix.com/products/nuix-investigator-lab>, Erişim Tarihi: 17.11.2016.

STATCOUNTER (2016), “Mobile and Tablet Internet Usage Exceeds Desktop for First Time Worldwide”, <http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide>, Erişim Tarihi: 02.02.2017.

SWGDE (2013), SWGDE Best Practices for Mobile Phone Forensics, <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics>, Erişim Tarihi: 28.01.2017.

The Radicati Group (2015), “Mobile Statistics Report, 2015-2019”, <http://www.radicati.com/wp/wp-content/uploads/2015/02/Mobile-Statistics-Report-2015-2019-Executive-Summary.pdf>, Erişim Tarihi: 27.09.2016.

Anayasa Mahkemesi Kararı

08.11.2012 tarihli ve E. 2012/27, K. 2012/173 sayılı karar, RG 28.03.2013, S. 28601.

Avrupa Komisyonu Kararları

21.02.2007 ve Case COMP/E-1/38.823 - PO/Elevators and Escalators.

İspanya Ulusal Piyasalar ve Rekabet Komisyonu Kararı (CNMC)

07.04.2016 tarihli ve Case /DC/0503/14.

Rekabet Kurulu Kararları

16.12.2015 tarihli ve 15-44/731-266 sayılı Kurul kararı (*Araç Lastiği*).

06.10.2015 tarihli ve 15-37/585-204 sayılı Kurul kararı (*Hazır beton*).

20.11.2015 tarihli ve 15-41/682-243 sayılı Kurul kararı (*Sinema*).

25.06.2014 tarihli ve 14-22/461-203 sayılı Kurul kararı (*3M*).

01.10.2014 tarihli ve 14-37/702-310 sayılı Kurul kararı (*Turkcell*).

08.03.2013 tarihli ve 13-13/198-100 sayılı Kurul kararı (*Bankacılık*).

Macaristan Rekabet Kurumu Kararı (GVH)

14.09.2015 tarihli ve Dosya Numarası: Vj-28/2013/506.



Üniversiteler Mahallesi
1597. Cadde No: 9
06800 Bilkent - Çankaya /ANKARA
[http:// www.rekabet.gov.tr](http://www.rekabet.gov.tr)