
GAZİ ÜNİVERSİTESİ
Gazi
1926

ANDROID AKILLI TELEFONLARIN ADLİ BİLİŞİM BAĞLAMINDA İNCELENMESİ: SÜREÇLER, YÖNTEMLER VE HUKUKİ BOYUTU

Tayfun YILDIRIM

YÜKSEK LİSANS TEZİ

ADLİ BİLİŞİM ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

ŞUBAT 2023

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Tayfun YILDIRIM

09/02/2023

ANDROID AKILLI TELEFONLARIN ADLİ BİLİŞİM BAĞLAMINDA İNCELENMESİ: SÜREÇLER, YÖNTEMLER VE HUKUKİ BOYUTU

(Yüksek Lisans Tezi)

Tayfun YILDIRIM

Gazi Üniversitesi

Bilişim Enstitüsü

Şubat 2023

ÖZET

Adli bilişimde her somut olay için uygulanabilecek tek bir inceleme metodu bulunmamakta olup, inceleme yapılacak hedefler hem donanımsal hem de yazılımsal olarak binlerce farklı kombinasyonlardan oluşabilir. Nitekim günümüzde teknolojik cihaz üreticileri işlevsel bakımından birbirinden farklı cihazlar (kamera, telefon, bilgisayar, yazıcı, televizyon vb.) ürettiği gibi gerek aynı işleve sahip olan gerek de aynı amaca hizmet eden ancak muhtelif nitelikler bakımından birbirinden ayrılan cihazlar da üretmektedirler. Örneğin akıllı telefonlar temelde aynı amaca hizmet etmek için üretilmelerine karşın birbirlerinden donanımsal ve/veya yazılımsal olarak ayrılan özellikleri bulunmaktadır. Bu çalışmada Android akıllı telefonların adli bilişim bakımından incelenmesi ele alınmaktadır. Ancak belirtildiği üzere Android akıllı telefonların işletim sistemi versiyonları ve donanımsal olarak birçok çeşitliliği bulunmasıyla her geçen gün çeşitliliğin hızlı bir şekilde artmasından dolayı bu telefonları incelemek büyük zorluklar içermektedir. Bu nedenle hedef akıllı telefonun özellikleri dikkate alınarak inceleme yönteminin belirlenmesi gerekmektedir. Mevcut inceleme yöntemleri her akıllı telefon için uygun olmamakla beraber gelecekte üretilecek olacak akıllı telefonlar için de yetersiz kalabilecektir. Bu çalışmada, Android akıllı telefonların incelenmesinde kullanılabilecek birçok açık kaynak kodlu araç uygulamalı olarak denenerek adli bilişim pratiğine hizmet edecek sonuçlar elde edilmiş tüm adli bilişim süreçlerinde nasıl hareket edilmesi gerektiği ortaya konulmuştur. Nitekim açık kaynak kodlu araçların bizzat denenmesiyle hem hedef cihazın mantıksal veya fiziksel imajının alınması hem mantıksal yahut fiziksel imajların analizi hem de faillerin kullandığı karşı adli bilişim yöntemlerinin tespitine ilişkin açıklamalar yapılmıştır. Bilhassa işbu araçların açık kaynak kodlu olması sebebiyle bu çalışmadaki araçlarla adli bilişim incelemelerinin gerçekleştirilmesi halinde maliyetler oldukça azalacaktır.

Bilim Kodu : 92401

Anahtar Kelimeler : Android akıllı telefon adli bilişimi, adli bilişim süreçleri, Android akıllı telefon imajı, mantıksal imaj, fiziksel imaj, Android akıllı telefon veri analizi. Android mimarisi.

Sayfa Adedi : 96

Danışman : Doç. Dr. Nursel YALÇIN

ANALYSIS OF ANDROID SMARTPHONES IN THE CONTEXT OF DIGITAL FORENSICS: PROCESSES, METHODS AND THE LEGAL DIMENSION

(M. Sc. Thesis)

Tayfun YILDIRIM

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

February 2023

ABSTRACT

There is no single examination method that can be applied for every tangible incident in digital forensics, and the targets to be investigated can consist of thousands of different combinations, both hardware and software level. As a matter of fact, today, technological device manufacturers produce devices that differ from each other in terms of functionality (camera, telephone, computer, printer, television, etc.), as well as devices that have the same function and serve the same purpose, but differ from each other in terms of various qualities. For example, although smartphones are basically produced to serve the same purpose, they have features that differ from each other in terms of hardware and/or software level. In this study, the examination of Android smartphones in the context of digital forensics is also discussed. However, as mentioned, Android smartphones have many operating system versions and hardware diversity, and it is difficult to examine these phones because the variety is increasing day by day. For this reason, it is necessary to determine the examination method by taking into account the characteristics of the target smartphone. Thus, current inspection methods are not suitable for every smartphone or they may be insufficient for smartphones that will be produced in the future. In this study, many open source tools that can be used in the examination of Android smartphones have been tested in practice and the results that will serve the digital forensic practice have been obtained, and how to act in all digital forensic processes has been revealed. By testing open source tools, explanations have been made regarding both acquiring the logical or physical image of the target device, the analysis of logical or physical images, and the detection of anti-digital forensic methods used by the perpetrators. Especially since these tools are open source, the costs will be considerably reduced if digital forensic investigations are carried out with the tools in this study.

Science Code : 92401

Key Words : Android smartphone digital forensics, digital forensics processes, Android smartphone image, logical image, physical image, Android smartphone data analysis, Android Architecture.

Page Number : 96

Supervisor : Assoc. Prof. Dr. Nursel YALÇIN

TEŞEKKÜR

Tüm hayatım boyunca her zaman yanımda olan aileme, tez çalışmam boyunca devamlı desteği bulunan ve akademik çalışmalar yapmamda yardımını esirgemeyen danışman Hocam Doç. Dr. Nursel YALÇIN'a teşekkürlerimi arz ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim **Sayfa**

Resim **Sayfa**

Resim **Sayfa**

KISALTMALAR

Kısaltmalar	Açıklamalar
ACPO	Baş Polis Memurları Birliği (Association of Chief Police Officer)
ADB	Android debug bridge (Android hata ayıklama köprüsü)
AOSP	Android Açık Kaynak Projesi (Android Open Source Project)
AOT	Zamanın Ötesinde (Ahead of Time)
API	Uygulama programlama arayüzleri (Application Programming interface)
AVD	Android sanal cihaz (Android Virtual Device)
ART	Android runtime (Android çalıştırma ortamı)
CMK	Ceza Muhakemesi Kanunu
DVM	Dalvik virtual machine (Dalvik sanal makinesi)
IOCE	Bilgisayar Delilinin Uluslararası Organizasyonu (International Organization on Computer Evidence)
NAND	Ve ile bağlı olmayan flaş bellek (Not-And Flash Memory)
NOR	Veya ile bağlı olmayan flaş bellek (Not-Or Flash Memory)
OSAF	Açık kaynak kodlu adli bilişim (Open source android forensics)
PASM	Sistem seviyesinde veri ve bellek taşıma ile özel veri elde etme metodu (Private data Acquisition method based on System level data migration and Memory)
PIN	Kişisel Tanımlama Numarası (Personel identification number)
ROM	Read only memory (Sadece okunabilir bellek)
RAM	Random access memory (Geçici bellek)
SDK	Yazılım geliştirme araç takımı (Software development kit)

SWDGE	Dijital Delil üzerinde Standart Çalışma Grubu (Scientific Working Group on Digital Evidence)
USB	Evrensel seri veri yolu (Universal serial bus)

1. GİRİŞ

Adli bilişim, dijital cihazların toplanmasıyla üzerlerinde analiz yapılarak bunların mahkemeye rapor halinde sunulacak biçimde delilleştirilmesini sağlayan bir bilim dalıdır. Bu bilim dalı vasıtasıyla maddi gerçeğe ulaşılarak faillerin yakalanması, cezalandırılması veya masumların beraatine karar verilmesi yahut işlenmesi planlanan suçların önlenmesi mümkün olmaktadır (Kılıç, 2012).

Yine her ne kadar adli bilişim daha çok suç ile ilişkilendirilse de hukuki yargılamalardaki dijital delillerin doğruluğun saptanması için de adli bilişim incelemelerindeki yöntemlerin uygulanması söz konusu olabilir. Örneğin bir boşanma davasındaki aldatma olgusu kanıtlama amacıyla sunulan fotoğrafın gerçek olup olmadığı, adli bilişimin tetkik yöntemlerinin kullanılmasıyla saptanabilecektir.

Eoghan Casey yapmış olduğu birçok çalışmayla adli bilişim bilimine katkıda bulunup bu bilimin öncüsü olmuştur. Android akıllı telefonların adli bilişim incelemesi bağlamında ise, birçok konunun ele alındığı kapsamlı çalışmalar mevcuttur (Skulkin ve diğerleri, 2018) (Hogg, 2011). Yine Android akıllı telefonların geçici belleğinin elde edilmesi (Yang ve diğerleri, 2016), imaj analizinin yapılması (Ghosh ve diğerleri, 2016), karşı adli bilişim işlemlerine karşı araçların geliştirilmesi (Mirza ve diğerleri, 2020) gibi daha spesifik çalışmalar da mevcuttur.

Bu çalışmada adli bilişim süreçleri, farklı işletim sistemli akıllı telefon türleri, Android akıllı telefonların mimarisi, Android akıllı telefonların inceleme süreçleri, bu akıllı telefonlara el konulmasından elde edilen verilerin ve yapılan işlemlerin raporlanmasına kadar geçen sürede hukuka aykırılıklar oluşmaması için nasıl hareket edilmesi gerektiği ele alınarak Android akıllı telefonların kapsamlı bir şekilde adli bilişim incelemesinin nasıl gerçekleştirileceği ortaya konulmuştur.

Bu bağlamda ilk olarak adli bilişim ve süreçleri, farklı işletim sistemli akıllı telefon türleri ele alınacak sonrasında Android akıllı telefonların mimarisi açıklanacak olup son olarak da bu akıllı telefonlara el konulmasından elde edilen verilerin ve yapılan işlemlerin raporlanmasına kadar geçen sürede yazılım araçlarının da uygulanmasıyla beraber hukuka aykırılıklar oluşmaması için nasıl hareket edilmesi gerektiği anlatılacaktır.

Böylelikle bu çalışmayla Android akıllı telefonların adli bilişim incelemesinin tüm süreçlerde nasıl yapılabileceğini, bilhassa açık kaynak kodlu araçların kullanılması suretiyle somut örneklerle açıklayarak, adli bilişim biliminin pratiğine de yardımcı olmak amaçlanmıştır.

Android akıllı telefonlardan veri elde edilmesi sırasında root yetkisinin ne denli önemli olduğu, root yetkisinin kazanılması için hangi yolların izlenmesi gerektiği, root yetkisinin kazanılması sırasında yaşanabilecek güçlükler ve root yetkisi kazanmanın cihazın bütünlüğünü bozduğundan bu işlemin yapılmasının dijital delilin mahkemelerce kabulünü engelleyip engellemeyeceği hususları açıklanmıştır.

Android cihazlardan mantıksal ve fiziksel imajının alınabilmesine ilişkin yöntemler açıklanmış, muhtelif açık kaynak kodlu araçların kullanılmasıyla somut örneklerle anlatılmıştır. Yine bu şekilde elde edilen verilerin muhtelif açık kaynak kodlu araçlar suretiyle nasıl analiz edilebileceği somutlaştırılmıştır. Raporlamanın tüm adli bilişim süreçlerinde yapılan işlemleri kapsamasının önemine dikkat çekerek hangi bilgileri içermesi gerektiği belirtilmiştir.

Bu çalışmanın "ADLİ BİLİŞİM" bölüm başlığında genel olarak adli bilişim hakkında bilgiler verilip adli bilişim aşamaları; "AKILLI TELEFONLARDA GÜNÜMÜZE KADAR KULLANILAN BAŞLICA İŞLETİM SİSTEMLERİ" bölüm başlığında farklı işletim sistemleriyle çalışan akıllı telefonlar hakkında bilgiler; "ANDROID İŞLETİM SİSTEMİNİN MİMARİSİ" bölüm başlığında Android işletim sisteminin hangi katmanlardan oluştuğu, katmanların birbirleriyle ilişkisi, hangi çekirdek üzerine kurulduğu, uygulamaların anatomisi; "ANDROID AKILLI TELEFONLARIN ADLİ BİLİŞİM BAKIMINDAN İNCELENMESİ" bölüm başlığında, olay yerine gitmeden önce yapılacak hazırlıklar, Android akıllı telefonların tanımlanması, Android akıllı telefonların açık kaynak kodlu araçlarla mantıksal ve fiziksel imajlarının alınması, yine açık kaynak kodlu araçlarla alınan imajların analiz edilmesi, raporlamanın yapılması ve Android akıllı telefonların incelenmesinde hukuki olarak dikkate alınması gereken konular ele alınmıştır.

2. ADLİ BİLİŞİM

Özellikle internet ağları vasıtasıyla suç işleyen faillerin kendilerini çeşitli araç ve yöntemlerle gizleyebilmeleri, nasıl olsa kimliklerinin tespit edilemeyeceğini düşünerek suç işlemelerini kolaylaştırmaktadır. Bununla beraber failler, kullandıkları dijital cihazlara yapay kullanıcı verisi yükleyerek üzerlerine suç isnadını önleyebilecek adli bilişim karşıtı muhtelif metotlar da kullanabilmektedir. Akıllı telefonlar gibi dijital cihazların oldukça yaygınlaşıp kullanıcıların devamlı surette bu cihazlarla etkileşimi, bu cihazların suç işlemek saikiyle araç olarak kullanılması ve suçla ilişkili delil barındırması potansiyelini oldukça artırmaktadır. Mezkur dijital cihazlardaki verilerin sayısal biçimde cihazlarca saklanması, bu delillerin değerlendirilmesini zorlaştırabilmektedir. Bu nedenle adli bilişim bilimi vasıtasıyla bu dijital cihazlardaki verilerin analizi yapılarak daha sarih bir biçimdeki rapor halinde soruşturma dosyasına veya mahkemeye sunulması sağlanmaktadır. Böylelikle ceza yargılamasının süjelerinin ilgili dijital cihazla bağlantılı delilleri değerlendirip tartışarak maddi gerçeğe ulaşıp hakkaniyetli bir karar tesis etmeleri mümkün kılınmaktadır (Baştürk, 2014).

Adli Bilişim bilimi; maddi gerçeğe ulaşılabilmesi için bilimsel metotların uygulanarak, çeşitli niteliklerdeki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bütünlüğünün korunarak zarar görmeden anlaşılabilir bir şekilde yargılama makamlarına sunulmaya hazır hale getiren ve belirli bilimsel tekniklerin uygulandığı dijital delillerin incelenmesi aşamalarının bütünüdür (Ekizer, 2014).

Kriminolog Prof. Edmond Locard'ın "Locard'ın Değişim Prensibi" olarak bilinen teoriye göre, suç işleyen bir fail suç mahalinden ayrılmadan önce, ya orada kendisi ile alakalı bir iz bırakacak ya da oradan bir izi kendisi üzerinde taşıyacaktır. Bu deliller, somut delil niteliğinde olduğundan soyut tanık beyanlarıyla çürütülmesi de mümkün olmayacağından oldukça ehemmiyetlidirler. Değişim prensibi, fiziksel ortamda geçerliği olduğu gibi bilişim alanında da geçerlidir. Bu bakımdan nasıl ki fiziksel ortamda her davranış belirti bırakmakta ise bilişim sistemleri üzerinde de belirti bırakmadan hareket etmek çok zordur. Nitekim dijital cihazların kullanıcısı her ne kadar cihazda herhangi bir iz bırakmadığını düşünse de log kayıtlarında (sistemin sıralı kayıtları), izler mevcut olabilecektir. Önemli olan bu belirtileri doğru yöntemlerle ve hukuka uygun bir şekilde belirleyip neticeye ulaşmayı sağlayan bilgileri edinebilmektir. Bu işlemlerin doğru, hukuka uygun ve bilimsel olarak yürütülmesi amacıyla da adli bilişim bilimi meydana gelmiş ve inkişaf etmiştir. Bu

doğrultuda da adli bilişim metotlarının oluşturulmasında, ceza muhakemesinin yöntemleri ile paralel olacak şekilde hareket ederek hukuka uygun delillerin meydana getirilmesi amaçlanmıştır. Adli bilişim kavramı, dilimize "computer forensics" ifadesinden aktarılmıştır. Ancak adli bilişim kavramı, daha kapsamlı bir ifade olduğundan bu bilimi ifade etmek açısından daha yerindedir. Nitekim "computer forensics" kavramı, sadece bilgisayarları karşıladığından günümüzde bunun yerine "digital forensics" kavramının kullanılması tercih edilmeye başlamıştır (Başlar, 2019).

Failler, adli bilişim ve incelemelerinin kapasiteleri hakkında daha fazla bilince varıp, daha özel şekilde bilgisayarlar ve ağları kullanarak suçları işlemektedirler. Hatta bazıları, kendi aktivitelerini gizlemek ve dijital delilleri yok etmekle beraber genel olarak adli bilişim uzmanlarının incelemesini baltalamak için spesifik olarak karşı adli bilişim metotları ve araçları dahi geliştirmektedir. Ayrıca işletim sistemlerine güçlü kriptolamaların entegre edilmesi, adli bilişim uzmanları için zorluklar oluşturabilerek dijital cihazlarındaki verilerin elde edilmesini engelleyebilmektedir (Casey, 2009b: 2).

Her ne kadar adli bilişimde kullanılan yöntemler gelişse de sürekli yaşanan teknolojik gelişmeler ile işletim sistemleri ve uygulamaların versiyonlarının güncellenmesiyle daha önce geliştirilen adli bilişim metotları işlevsiz kalabilmektedir. Bu nedenle adli bilişim halen gelişmeye büyük ihtiyaç duyan ve üzerinde devamlı çalışma yapılması gereken bir bilimdir.

2.1. Adli Bilişim Süreçleri

Adli bilişimdeki bir delilin elde edilmesinden mahkemeye sunulmasına kadar geçen süre içerisinde delillerin bütünlüğünün ve hukukiliğinin korunabilmesi için dikkat ve özenli şekilde hareket edilmesi gerekmektedir. Adli bilişim süreçlerine ilişkin birçok farklı aşama modelleri bulunmaktadır. Kimi modellerde 5 aşama bulunacağı gibi kimi modellerde de 6 aşama ya da farklı sayıdaki aşama modelleri bulunabilmektedir (Casey, 2011c: 189). Adli bilişim süreçlerini bu çalışmada 6 aşamada gösterilecektir. Bu aşamalar şu şekildedir:

1. Hazırlık aşaması,
2. Dijital delillerin tanımlanması,
3. Dijital delillerin toplanması ve imaj alınması,
4. Dijital delillerin muhafazası,
5. Dijital delillerin analizi,
6. Dijital delillerin rapor haline getirilmesi.

Hazırlık aşamasından raporlama aşamasına kadar ilgili yargılama makamlarıyla farklı durumlarda nasıl hareket edilmesi gerektiği, 5.7 başlık numaralı “Hukuki Boyutu” isimli bölüm başlığında Şekil 5.2’de gösterilmiştir.

2.1.1. Hazırlık Aşaması

Olay yerini analiz etmek için olay yerine erişen bir adli bilişim uzmanı, maddi gerçeğe ulaşabilmek yönünde olay yerinde bulunan hangi cihazlardan hangi verileri elde etmesi gerektiğini tespit etmelidir. Nitekim olay yerinde farklı cihazlar bulunabileceğinden bu cihazlardan veri elde edilmesi noktasında farklı metotlar uygulanması gerekebilecektir. Zira elde edilmek istenen veriler kişisel bilgisayarda; akıllı telefon, tablet veya saatte; yazıcıda; fotoğraf makinesinde; tarayıcıda; e-kitap okuyucuda olabilir. Dolayısıyla adli bilişim uzmanının bu olasılıkları dikkate alarak yanında bu cihazlardan veri elde etmeye yarar araçlar ile olay yerine intikal etmesi yahut bu cihazlardan hangi tekniklerle hukuka uygun veri elde edebileceğini konusunda hazırlıklı olarak bulunması gerekmektedir. Yine adli bilişim uzmanının olay yerinde karşılaşabileceği güçlükleri de nazara alarak olay yerinde hızlı müdahale edilmesi gereken sorunları çözülmesini sağlayacak bilgi ve ekipman açısından donanımlı olması ehemmiyetlidir (Bucak, 2019). Nitekim bazı durumlarda hangi tekniğin uygulanacağı noktasında hızlı davranılmadığı takdirde kurtarılması mümkün olmayan veri kayıpları meydana gelebilecektir.

Etkin dijital araştırma gerçekleştirebilmek için plan oluşturulmalı ve destekleyici kaynak ve materyal elde edilmelidir (Casey, 2011c). Bu bağlamda potansiyel karşılaşılacak cihazların imajını almak ve cihazlardaki veriler ile izlerin değişime uğramasına önlemek adına, her yönden izolasyonunu sağlayabilmeye elverişli cihazlar hazır bulundurulmalıdır.

2.1.2. Dijital Delillerin Tanımlanması

Olay yerinde bulunan cihazların hangi türde olduğu, bunların marka ve modelleri, hangi işletim sistemi üzerinde çalıştığının tespiti yapılmalıdır. Bu bağlamda cihazın kişisel bilgisayar, akıllı telefon, fotoğraf makinesi, akıllı tablet, akıllı saat vb. türlerden hangisinin kapsamında olduğu, bu cihazın üreticisi, markası ve modelinin ne olduğu ve cihazın hangi işletim sistemi üzerinde çalıştığı tespit edilmelidir. Yine olay yerindeki cihazların çalışıp çalışmadığı, ekranının açık olup olmadığı hususları belirlenmelidir (Årnes, 2018: 18).

Nitekim her cihazın çalışma şekilleri ve mimarisi oldukça farklı olup olay yerinde tespit edilen cihazla hangi adli bilişim uzmanın daha yetkin bir şekilde teknik bilgiye sahip olduğu belirlenerek o adli bilişim uzmanının cihazla etkileşim halinde olmasına özen gösterilmelidir. Hedef cihazların özelliklerinin nazara alarak adli bilişim süreçlerine devam edilmesi, tüm adli bilişim süreçlerinin sağlıklı bir şekilde gerçekleştirilmesi açısından oldukça ehemmiyetlidir. Herhangi bir aşamada hatalı işlem yapılması halinde, telafisi mümkün olmayan veri kayıpları yahut hukuka aykırılıklar meydana gelebilir.

Resim 2. 1. Örnek bir olay yeri

Resim 2.1'de örnek bir olay yeri bulunmaktadır. Bu olay yerinde birçok cihaz bulunmakta olup yukarıda anlatıldığı şekilde derhal tanımlamaların yapılması, oldukça önemlidir.

2.1.3. Dijital Delillerin Toplanması ve İmaj Alınması

Dijital deliller toplanırken cihaza doğrudan çıplak elle temas edilmeyerek statik önleyici eldiven kullanılmalıdır. Nitekim doğrudan temas halinde, elektriklenme ile cihaz zarara uğrayabilir. Yine cihaz üzerindeki parmak izi de ayrı bir delil olduğundan parmak izi delilinin korunması da ehemmiyetlidir. Hedef cihazların bulunduğu olay yerine ilk gelindiği andan itibaren fotoğraflanma veya video kaydı alınarak işlemler gerçekleştirilmelidir. Bilhassa tüm işlemler sırasında video kaydının devam ettirilmesi, ileride dijital delillerin

değişikliğe uğradığı iddiasına karşı önlem oluşturacaktır. Hedef cihazların şarj cihazına veya başka bir dijital cihaza bağlı olması durumunda, olay yerindeki mevcut durumları korunarak fotoğraflanma yapılmalıdır. Olay yerinde sırasıyla yapılan işlemlere ilişkin tutanak tutularak hareket edilmeli ve bu tutanağı fotoğraf ile video kayıtları desteklemelidir (Saraydere, 2018).

Olay yerinde ekranı halen açık veya çalışmakta olan cihazlar bulunmakta ise, cihazların bu durumu muhafaza edilmelidir. Cihazların bu durumunun muhafaza edilmemesi halinde, bilhassa geçici bellekte bulunan verilerin kaybı yahut parola engelinin ortaya çıkması söz konusu olabilir. Nitekim bir kullanıcının dahi kişisel bilgisayarında bir kelime işlemcisi uygulamasıyla belge düzenlediği sırada, sistemin çökmesi ve tamamen yeniden başlatılması durumunda kalınması halinde dahi kullanıcının kendisi bile ilgili belgeyi kaybetme riski altında kalmaktadır (Årnes, 2018: 23). Yine ekranı açık bulunmakta olan cihazların ekranların mevcut durumuyla fotoğraflanması yapılmalıdır.

Olay yerinde cihazların imajlarının alınıp alınamayacağı, tespit edilmelidir. Bilhassa halen çalışmakta olan cihazların imajının alınmasına öncelik verilmelidir. Nitekim bu cihazların geçici belleğinde bulunan veriler, zaman geçtikçe hızlı bir şekilde değişikliğe uğrayabilir. Eğer cihazların imajlarının alınabilmesi mümkün değilse, bir sonraki "Dijital Delillerin Muhafazası" adlı başlıkta belirtilen şekilde cihazların dışarıyla bağlantısı kesilerek ve halihazırda çalışmakta olan cihazların kapanması önleyecek tedbirlerin alınmasıyla beraber laboratuvara götürülmelidir (Rick ve diğerleri, 2014).

2.1.4. Dijital Delillerin Muhafazası

Dijital cihazların muhafazası; ağ üzerindeki sistemi izole etme, ilgili log dosyalarını koruma ve sistem kapatıldığında kaybedilecek değişken veriyi toplayarak dijital delil üzerindeki değişikliği önlemektir. Bu süreç aslında elde edilenlerin toplanması aşaması ile başlamakta olup sonraki tüm aşamaları da kapsamaktadır.

Delillerin muhafazası, veri bütünlüğünün güvenliğini sağlayarak el konulan cihazlardaki verilerin değiştirilmesi yahut silinmesini engelleyecek şekilde cihazların zilyetliğinin meşru şekilde cihaza el koyan kurumda bulundurulmasıdır. Bu dijital delildeki verilerin kurtarılması noktasında alınacak ilk önlemdir. Muhafaza, dijital delillerin inceleme aşamalarının toplanmasından başlayarak devam eden tüm aşamaları içerir. Nitekim delil bütünlüğünün korunamaması halinde, yargılamada hukuka uygun delil olarak kullanılabilmesi yahut suçluların tespit edilebilmesi mümkün olmayabilir. Dolayısıyla ceza

yargılanmasındaki hem soruşturma evresinin hem de kovuşturma evresinin etkili bir şekilde yürütülerek maddi gerçeğe ulaşmada, yetersiz kalınabilir (Akalın, 2016).

2.1.5. Dijital Delillerin Analizi

Dijital delillerin analizi, delillerdeki bulguları araştırma ve yorumlamadır. Bazı süreç modelleri, inceleme ve analiz kelimelerini birbirinin alternatifi olarak kullanmaktadır (Casey, 2011c).

Delil inceleme aşamasında elde edilen veriler üzerinde; olay ile ilgisi olabilecek dosyaların içeriğinde barındıkları veriler, dosyaların ne zaman oluşturulduğu, dosyaya hangi tarih ve saatte erişildiği, dosyada hangi tarih ve saatte düzenleme yapıldığı, internet tarayıcısında ziyaret edilen internet siteleri veya oluşturulan yer imleri bilgileri, çeşitli uygulamalarla gönderilen e-posta yahut ileti bilgileri vb. incelenerek olay ile ilgisi olabilecek veriler tespit edilir.

Bilgisayarlarda yapılabilecek delil inceleme aşamasındaki işlemler;

1. Bilgisayardaki dosyaların erişilme, oluşturulma ve son yazılma tarih ve saatinin tespiti,
2. İnternet tarayıcısında ziyaret edilmiş olunan internet siteleri ile bu sitelerin hangi tarih ve saatte ziyaret edildiğinin tespiti,
3. Bilgisayara internet üzerinden indirilen dosyaların ve bu dosyalar üzerinde herhangi bir değişiklik yapılıp yapılmadığının tespiti,
4. Gizli veya dosya uzantısı değiştirilerek gizlenen dosyaların görüntülenmesi,
5. Bilgisayardan yazıcıya gönderilen belge dosyalarının görüntülenmesi,
6. Bilgisayardaki dosyalar içinde olay ile ilgili olabilecek kelimelerin aramasının yapılması,
7. Dosya türlerinin filtrelenerek taranması,
8. Şifre korumalı dosyaların içeriğinin görüntülenmeye çalışılması olarak sıralanabilir (Aydoğan, 2009).

2.1.6. Dijital Delillerin Rapor Haline Getirilmesi

Raporlama, mahkemenin kararını rapora dayanarak kuracağından dolayı önemli bir aşamadır. Delilin elde edilmesinden incelenmesi kadar geçen sürede yapılan işlemlerin delilin muhafaza edilme biçimi de dahil olmak üzere raporlanmasında yarar bulunmaktadır. Raporda delil uygun bir şekilde doğrulanmamışsa, mahkemede yargılanan fail sanığın

beraatı veya masum sanığın cezalandırılması gündeme gelebilecektir. Rapor sunulduğu mahkemede, taraflarca tartışılacağı için elde edilen dijital delil bakımından birçok duruma cevap verebilecek nitelikte hazırlanmış olmalıdır. Bu nedenle rapor mahkemeye arz edilmeden önce tamamlanmış ve itina ile hazırlanmış olması gereklidir (Mosa, 2018).

2.2. Dijital Deliller

Eoghan Casey tarafından dijital delil, bir suçlamanın aksini ispatlamayı yahut şüphelinin kastı olup olmadığı veya suçun işlendiği sırada suç mahallinde bulunmaması gibi suçlamanın önemli unsurlarını ortaya koymayı sağlamakla birlikte bir bilgisayar sistemi kullanmak suretiyle depolanan veya iletilen herhangi bir veridir. Bu tanımlamada belirtilen veri esas olarak; yazı, resim, ses ve video gibi çeşitli tür bilgilerini temsil eden rakam kombinasyonlarıdır (Casey, 2011a).

Dijital delile ilişkin birçok farklı tanımlama bulunmaktadır. Eoghan Casey 2000 yılında ise dijital delili, *"Dijital delil daha öncesinde, suç işlendiğine ilişkin veya suç ile mağdur yahut suç ile fail arasında bağ kuran herhangi bir veri"* olarak tanımlamıştır. Dijital Delil üzerinde Standart Çalışma Grubu (SWDGE), *"kanıt değeri olan dijital formda saklanan veya iletilen herhangi bir bilgi"* şeklinde tanımlamıştır. Bilgisayar Delilinin Uluslararası Organizasyonu (IOCE) tarafından yapılan farklı bir tanımlama ise, *" ikili formatta depolanan ya da iletilen mahkemede karar verilirken esas alınabilecek bilgi"* şeklindedir. Baş Polis Memurları Birliği (ACPO) tarafından yapılan daha kapsamlı bir tanımlama, *"soruşturma değeri olan bilgisayar tarafından depolanan veya iletilen herhangi bir veri ya da bilgi"* şeklindedir. Brian Carrier tarafından ortaya koyulan daha da geniş bir tanımla ise, *"dijital olayları veya dijital verilerin durumunu destekleyen veya reddeden dijital delil"* şeklindedir (Casey, 2011a: 7).

Amerika Birleşik Devletleri'nde bir sorgu yargıcı, dijital delillerinin kabul edilebilirliği açısından ana hatlarıyla ilkeler belirlemiştir. Bunlar dijital delilin; yargılama konusu ile ilgili olması, doğruluğu, duyumsal olmaması, duyumsal olsa da kabul edilebilecek duyumsal delillerden olması, en iyi delillerden olması, haksız yere önyargı oluşturmamasıdır. Mahkemeler tarafından bir delilin kabul edilmesi engelleyen diğer durumlara örnek olarak ise, dijital delilin uygunsuz şekilde muhafaza edilerek doğruluğundan şüphelenilmesine sebebiyet verilmesi, arama kararı olmadan arama yapılması gibi hukuka aykırı şekilde arama ve el koyma neticesinde delillerin elde edilmesi verilebilir (Casey, 2011b: 57).

ABD yargılamasında kabul edilen bu kurallar, Türk Ceza Hukukunda da uygulanmaya elverişlidir.

3. AKILLI TELEFONLARDA GÜNÜMÜZE KADAR KULLANILAN BAŞLICA İŞLETİM SİSTEMLERİ

Akıllı telefonlar, başlıca anakart, flaş bellek, kamera, WiFi ve bluetooth bağlantıları, SIM kartı, SD kart gibi donanımlardan oluşmakta olup temelde iletişim kurmayı sağlamak için geliştirilmiştir. Ancak bu telefonların donanımları oldukça güçlü olup mesaj ve çağrıyla iletişim sağlamanın yanında internet sitelerini ziyaret etmek, sosyal medya uygulamalarını kullanmak, ses ve görüntü kaydı almak, birçok bankacılık işlemi gerçekleştirmek, belge görüntülemek ve oluşturmak gibi muhtelif birçok işlevi de bulunmaktadır. Bu işlevleri yerine getirmek için her ne kadar günümüzde akıllı telefon piyasasında Android ve iOS işletim sistemleri baskın olarak kullanılsa da günümüze kadar birçok farklı işletim sistemi kullanılmıştır. Bu bölümde akıllı telefonlarda başlıca kullanılan muhtelif işletim sistemleri hakkında bilgi verilmiştir.

3.1. Sybiam OS

Symbian, Symbian Şirketi tarafından cep telefonları ve normale göre daha küçük dizüstü bilgisayarlar gibi çeşitli taşınabilir cihazlar için geliştirilmiş ve 2000'li yıllarda yaygın olarak bu cihazlarda kullanılmış işletim sistemidir. Akıllı telefon endüstrisini kuran öncü Symbian Şirketi'nin bu işletim sistemi, 2010 yılına kadar akıllı telefonlar arasında en çok kullanılan işletim sistemi olmuştur. Ancak Android ve iOS bu yıldan sonra akıllı telefon piyasasında baskın bir şekilde yayılmıştır. Symbian işletim sistemi, şu anda geliştirilmeye devam edilmemektedir. Symbian; Nokia, Samsung, Motorola, Sony Ericsson gibi birçok büyük cep telefonu markası tarafından işletim sistemi olarak kullanılmıştır. Symbian, yayımlanmamış Intel x86 bağlantı noktasıyla uyumlu sürümünün bulunmasına karşılık başlıca ARM işlemcileri üzerinde çalışacak şekilde yayınlanmıştır (*Symbian*, 2022). Sybiam OS Series60, series80, Series90, UIQ vb. gibi farklı kullanıcı arayüzlerine sahiptir (Chao Wang ve diğerleri, 2011).

3.2. Windows Mobile

Windows Mobile, Microsoft şirketi tarafından Windows İşletim Sisteminin benzeri olacak şekilde, cep bilgisayarı olarak tanımlanan PDA gibi taşınabilir cihazlarda çalışması amacıyla geliştirilmiş bir işletim sistemidir. 2000'li yıllarda etkin olarak piyasada bulunsa da iOS ve Android işletim sistemlerinin piyasada yaygınlaşmasıyla popülerliğini kaybetmiştir. Şu anda desteklenmeye devam edilmiyor olup Microsoft Şirketi bu işletim sistemi yerine Android ve

iOS işletim sistemlerinde çalışacak uygulama veya entegre olabilecek yazılım geliştirmeye odaklanmış durumdadır (*Windows Mobile,* 2022).

3.3. BlackBerry

Blackberry, BlackBerry Ltd. isimli bir Kanada Şirketi tarafından geliştirilen işletim sistemidir. Şirket, işletim sistemiyle beraber kendi akıllı telefon cihazlarını da üretmiştir. Blackberry Haziran 2013 yılından itibaren geliştirilmesi devam edilmemiştir. Bu tarihten itibaren, BlackBerry yerine BlackBerry 10 isimli işletim sistemi geliştirilmeye devam edilmiştir. Ancak Şirket, daha sonrasında Android ve iOS işletim sistemlerinin piyasada baskınlığına dayanamayarak kendisi de Android işletim sistemli cihaz üreteceğini duyurmuştur. Şirket 2017 yılıyla beraber BlackBerry KeyOne isimli ilk ürettiği Android akıllı telefonunu piyasaya sürmüştür. Bu bağlamda, 4 Haziran 2022 tarihinde BlackBerry 10 isimli işletim sisteminin de geliştirilmesi durdurulmuştur (*BlackBerry OS,* 2022).

3.4. iOS

iOS, Apple Inc. şirketi tarafından salt olarak yine kendisinin üretmiş olduğu iPod, iPhone ve iPad cihazlarında çalışmak üzere tasarlanmıştır. Daha sonrasında iPad için ayrıca iPAD OS isimli işletim sistemi geliştirilerek 3 Haziran 2019 yılında yayınlanmıştır. iOS, akıllı telefonlarda Android'ten sonra piyasada en çok etkinliği bulunan işletim sistemidir. İşletim Sistemi'nin her yıl büyük bir güncellenme versiyonu yayınlanmaktadır. 12 Eylül 2022 tarihinde, en son büyük güncellemesiyle iOS 16 yayınlanmıştır. Her ne kadar muhtelif lisanslar kapsamında açık kaynak kodlu kısımları bulunsa da İşletim Sistemi büyük oranda kapalı kaynak kodludur (*IOS,* 2022).

3.5. WebOS

webOS, Linux çekirdek temelli bir işletim sistemidir. webOS sırasıyla Palm,Inc; HP ve LG Electronics şirketleri tarafından kullanılmıştır. HP Palm, Inc isimli Şirketi satın aldıktan sonra işbu İşletim Sistemi'ni açık kaynak kodlu yaparak isminin de Open webOS olarak değişmesini sağlamıştır. İşletim Sistemi Pre, Pxi ve Veer akıllı telefon modellerinin serilerinde kullanılmıştır. Daha sonrasında LG Electronics İşletim Sistemi'ni satın alınca başlıca akıllı televizyonlarda kullanılmaya devam edilmiştir (*WebOS,* 2022).

3.6. Maemo

Maemo, ilk başta Nokia tarafından geliştirilmeye başlanılmıştır. Açık kaynak kodlu ve Linux çekirdeği temellidir. Bu İşletim Sistemi ile Nokia, Android ve iOS işletim sistemleriyle rekabet etmeyi amaçlamıştır. Ancak muhtelif sebeplerden dolayı bu konuda başarılı olamamıştır. Nokia, İşletim Sistemini geliştirmeyi bıraktıktan sonra, bu İşletim Sistemi bir topluluk tarafından akıllı telefonlar ve tabletler için geliştirilmeye devam edilmektedir. Maemo, Nokia tarafından MeeGo isimli İşletim Sistemi'nin kaynak kodu olarak kullanılmıştır (*Maemo*, 2022).

3.7. MeeGo

MeeGo, Maemo İşletim Sistemi'nin kaynak kodunun kullanılmasıyla geliştirilen Linux çekirdek temelli bir işletim sistemidir. ARM ve Intel x86 işlemcilerinde çalışabilecek şekilde tasarlanmıştır. Nokia ile Intel ve Samsung ile Intel birliktelikleriyle geliştirilmek istense de her iki durumda da hedef değişikliğine gidilerek bu birliktelikler vasıtasıyla işletim sistemi geliştirilememiştir. Linux çekirdeği temelli ücretsiz ve açık kaynak kodlu mobil işletim sistemleri yapmayı amaçlayan Mer isimli Topluluk da MeeGo'nun bir kolunu oluşturmuştur. Daha sonrasında bu Topluluk'tan yararlanılarak Sailfish OS isimli işletim sistemi oluşturulmuştur (*MeeGo*, 2022).

3.8. LiMo

LiMo OS, Linux Mobile'ın kısaltmasından ismini almış olup taşınabilir cihazlar için geliştirilmiş Linux çekirdek temelli bir işletim sistemidir. LiMo, çok az akıllı telefonda kullanılmıştır. Bunlara örnek olarak Vodafone ve Samsung iş birliği ile geliştirilmiş 360 M1, 360 H1 ve 360 H2 verilebilir. LiMo İşletim Sistemi, 2011 yılı Eylül ayında Tizen işletim sistemi kapsamında geliştirilmeye devam edilmiştir (*LiMo OS*, 2022).

3.9. Ubuntu Touch

Ubuntu Touch, masaüstü veya dizüstü bilgisayarlar için geliştirilen Ubuntu işletim sisteminin de geliştiricisi olan Canonical Ltd. ve Ubuntu Topluluğu tarafından akıllı telefon ve tabletler için geliştirilmiş bir işletim sistemidir. 5 Nisan 2017 tarihinde, Ubuntu Touch projesine geliştirilmeyeceği duyurulmuştur. Ubuntu Touch; BQ, Meizi gibi akıllı telefon serilerinde kullanılmıştır.

3.10. Tizen

Tizen, Samsung tarafından akıllı telefonların yanında tablet, akıllı televizyon, araç multimedya sistemleri gibi cihazlarda da çalıştırılmak üzere geliştirilmiş Linux tabanlı bir işletim sistemidir. Samsung daha sonraları, bu İşletim Sistemini Bada ile birleştirerek daha çok giyilebilir cihazlar veya akıllı televizyonlar üzerinde kullanmıştır. 2021 Mayıs'ta Google, Samsung ile ortak olarak Android giyilebilir cihazlarda Tizen'ın özelliklerinin entegre edilebileceğini duyurmuştur. Bu durum da Tizen'ı asıl olarak Samsung Akıllı Televizyonlarda kullanılmak üzere geliştirilmesine devam edilmesine neden olmuştur (*Tizen*, 2022).

3.11. Sailfish

Sailfish OS, MeeGo işletim sisteminde muhtelif değişiklikler yapılarak meydana getirilen bir işletim sistemidir. Jolla isimli Finlandiyalı Şirket, Mer Topluluğu'nun geliştirmiş olduğu Linux temelli sistemden baz alarak Sailfish OS İşletim Sistemini tasarlamıştır. Jolla Phone isimli bir akıllı telefonla ilk defa piyasaya 2013 yılında sürülmüştür.

3.12. Firefox OS

Firefox OS; akıllı telefonlar, tablet bilgisayarlar, akıllı televizyonlar ve Matchstick TV gibi dijital cihazlar için Mozilla ve diğer işbirlikçilerle meydana getirilmiştir. Firefox internet tarayıcısı hizmet servisi ve Mozilla tarafından geliştirilmiş Gecko isimli tarayıcı motoru ile Linux çekirdeğine temellendirilmiştir. Piyasaya 2014 yılında sürülmüştür. En son sürümü, 29 Nisan 2015 yılında yayınlanmıştır. Şu anda geliştirilmeye devam edilmemektedir (*Firefox OS*, 2022).

3.13. Bada

Bada, Samsung Şirketi tarafından orta ve yüksek kalitedeki akıllı telefon ve tabletler için meydana getirilmiş ancak geliştirilmeye devam edilmeyen bir işletim sistemidir. Samsung Android işletim sistemli olarak ürettiği akıllı telefonları Galaxy serisi ile model isimlendirdiği gibi Bada işletim sistemli telefonları da Wave serisiyle model isimlendirmiştir. Bada işletim sistemli ilk telefon, Samsung Wave 8500 2010 yılının Mayıs ayında piyasaya sürülmüştür. 25 Şubat 2013 tarihinde Samsung, Bada İşletim Sistemini geliştirmeyi durdurarak onun yerine Tizen İşletim Sistemini geliştirmeye odaklanacağı duyurulmuştur (*Bada*, 2022).

3.14. Android

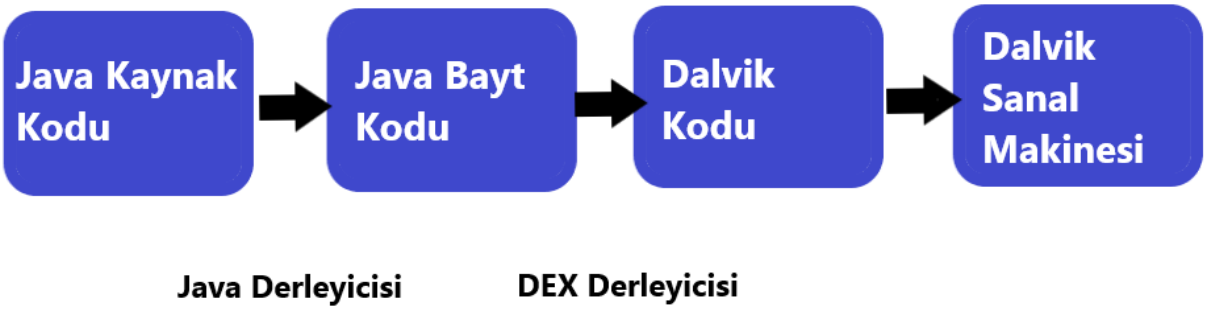
Android; Google ve Open Handset Alliance tarafından, mobil cihazlar için geliştirilmekte olan, Linux tabanlı özgür ve ücretsiz bir işletim sistemidir. Sistem açık kaynak kodlu olsa da kodlarının ufak ama çok önemli bir kısmı Google tarafından kapalı tutulmaktadır. Bu çalışmanın temel konusunu oluşturan mezkur işletim sistemi hakkında, Android İşletim Sisteminin Mimarisi başlığı altında detaylı açıklamalar bulunmaktadır.

4. ANDROID İŞLETİM SİSTEMİNİN MİMARİSİ

Akıllı telefon ve tabletler daha da popülerleştikçe, bu cihazlara ilişkin işletim sistemi de oldukça önem kazanmaya başlamıştır. Android, GPS (Küresel Konumlama Sistemi), kameralar, ışık ve yön sensörleri, WiFi ve 4.5 G (LTE) sinyal bağlantısı ve dokunmantik ekran özelliklerine sahip olan düşük donanım seviyeli cihazlar üzerinde çalışabilen bir sistemdir. Tüm işletim sistemleri gibi Android de uygulamaların donanım özelliklerini soyutlama yoluyla kullanmasını etkinleştirmekte ve uygulamalara tanımlanmış bir ortam sunmaktadır (Brahler, 2010). Her ne kadar Android ilk başta dizüstü ve masaüstü bilgisayarlara göre daha düşük donanım seviyesine ait cihazlar için geliştirilmişse de artık Android ile çalışan özellikle akıllı telefon ve tabletler, bir dizüstü veya masaüstü bilgisayara yakın güçte donanım seviyesine sahip olabilmektedir.

Apple' ın iOS işletim sistemi Palm'ın webOS işletim sistemi veya Symbian gibi diğer mobil sistemlerin aksine, Android uygulamaları Java üzerinden yazılmış olup Android 5.0 öncesi sanal makineler üzerinde çalışmaktaydı. Bu amaç için Android 5.0 sürümü öncesinde, kendi bayt kodunu uygulayan Dalvik sanal makinesini sunmaktaydı. Android 4.4 "Kitkat" ve önceki sürümlerinde Dalvik temel bileşen olup, Android kullanıcı uygulamalarının tamamı ve uygulama çerçevesi Java tarafından yazılarak Dalvik tarafından çalıştırılmaktadır. Şekil 4.1'de Dalvik Sanal Makinesi ile Java kaynak kodunun çalıştırılma süreci gösterilmiştir. Diğer platformlardaki gibi, Android uygulamalara da Google Play isimli merkezi yerden erişilebilir. Platform, Google tarafından satın alınan Android Inc. tarafından oluşturulmuş ve Android Açık Kaynak Projesi (AOSP) olarak 2007 yılında yayınlanmıştır (Brahler, 2010).

Android Linux çekirdek temelli olarak geliştirilmiş bir işletim sistemidir. Sistemin başlatılması ve çalıştırılması için farklı dosya formatları kullanılmaktadır. Bu dosya formatları sırasıyla rootfs, tmpfs, cgroup, proc, sysfs, devpts, ext3, yaffs2 ve vfat şeklinde sayılabilir. Cihazın başlatıldığı sırada, Linux çekirdeği rootfs dosya sistemine dönüştürülmektedir. Daha sonrasında da dosya sistemleri yukarıda verilmiş olan sırada oluşturulmaktadır (Ghosh ve diğerleri, 2021).



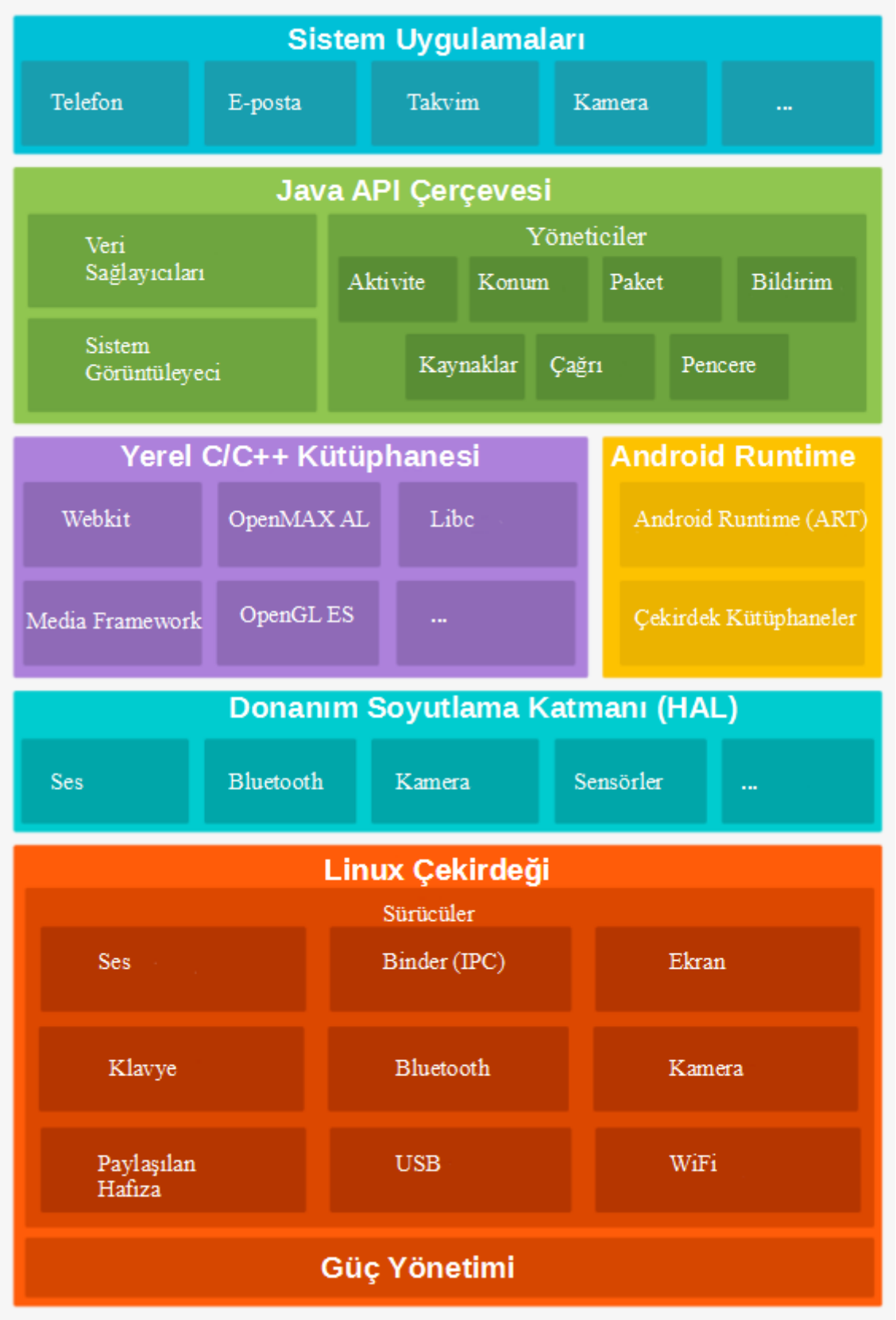
Şekil 4. 1. Java Kaynaklı Kodların Dalvik Sanal Makinesiyle Dönüştürülmesi (*What Are the Differences between Dalvik and ART?*, 2019)

Andoid 5.0 ile Dalvik Sanal Makinesi (DVM) yerine ART (Android Runtime) kullanılmaya başlanmasıyla, Android uygulamaları artık DVM gibi bir emülatöre gerek kalmadan cihazın makine dili ile doğrudan etkileşim kurabilir duruma gelmiştir (Küçükyılmaz, 2015).

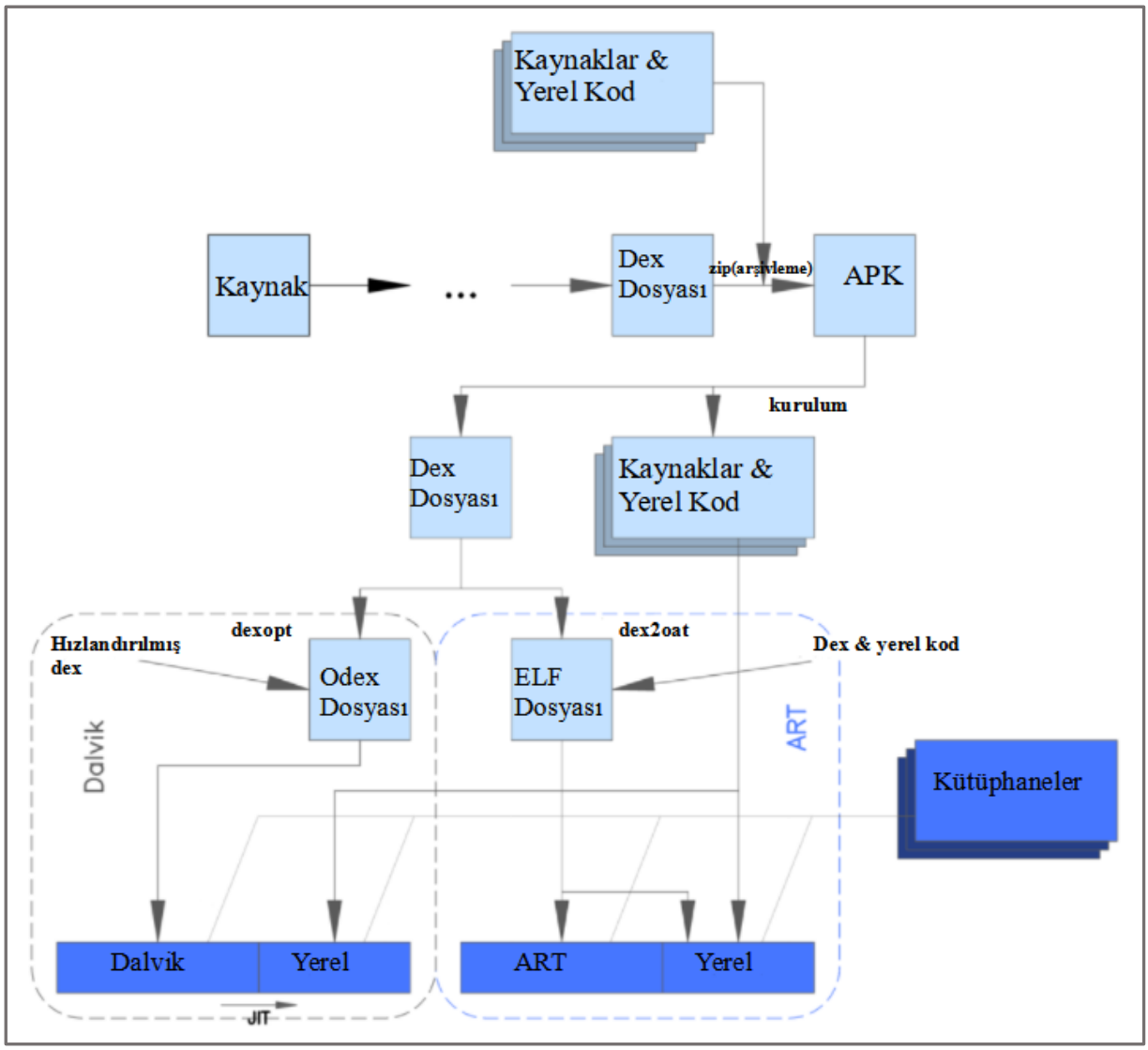
ART (Android Runtime) AOT (Ahead of Time) kullanmaktadır. AOT ile, uygulamanın cihaza indirildikten sonra kurulması sırasında tüm yüksek seviye kodlamaları makine seviyesi kodlamasına dönüştürülmekte ya da makine seviyesi kodlaması oluşturulmaktadır. Böylelikle uygulamanın çalıştırılması sırasında dinamik olarak dönüştürülme (Dalvik'te olduğu gibi) yapılmamaktadır. Tüm kodlamanın uygulamanın kurulması sırasında tek defada oluşturulması nedeniyle uygulama, Android cihazda çalışırken sürekli kodlamaların dönüştürülmesine gerek duymamaktadır. Ancak uygulama cihaza kurulduğunda, makine dili kodlarını da içermesi sebebiyle uygulamanın boyutu artmaktadır (*What Are the Differences between Dalvik and ART?*, 2019). Bununla beraber uygulama çalıştırıldığında artık bir emülatöre ve yüksek seviyedeki kodları makine diline çevirme gerekliliği bulunmadığından uygulama çok daha hızlı ve stabil şekilde çalışmaktadır.

Şekil 4. 2. Dalvik sanal makinesi ile çalışan Android sistem mimarisi. Yeşil nesneler C/C++ dili ile yazılmış olup, mavi nesneler Java ile yazılmış ve Dalvik sanal makinesi ile çalışmaktadırlar (Brahler, 2010).

Şekil 4.2'de Dalvik sanal makinesiyle Şekil 4.3.'te ise, Android Runtime ile çalışan Android sistem mimarisi gösterilmiştir.



Şekil 4. 3. ART ile çalışan Andoid sistem mimarisi (*Platform Architecture*, 2021)



Şekil 4. 4. Dalvik ile ART (Android Runtime) karşılaştırılması (*Android Runtime*, 2022).

Şekil 4.4'te Dalvik sanal makinesi ile Android Runtime ile çalışan Android sistemleri karşılaştırılmıştır.

Android 2011 yılında beri akıllı telefonlarda ve 2013 yılından itibaren tabletlerde dünya çapında en çok satılan işletim sistemi olmuştur. Mayıs 2017 tarihiyle, iki milyardan fazla aktif aylık kullanıcıya sahip olmakla beraber 2021 Ocak tarihi itibariyle ise, Google Play Store 3 milyondan fazla uygulama sunmaktadır. Güncel kararlı versiyonu 15 Ağustos tarihinde yayınlanan Android 13'dür (*Android (Operating System)*, 2022).

4.1. Uygulama katmanı

En üstte yalnızca Java veya Kotlin ile yazılan uygulama katmanı bulunmaktadır. Telefon, Kişiler, Galeri, Takvim gibi Android ile beraber gelen varsayılan uygulamalar ve kullanıcıların Google Play Store'dan indirebildiği tüm uygulamalar bu katmanın bir parçasıdır. Bu uygulamalar Android 5.0'dan önce Dalvik sanal makinesi ile çalışırken, şu an Android Runtime ile çalıştırılmaktadır.

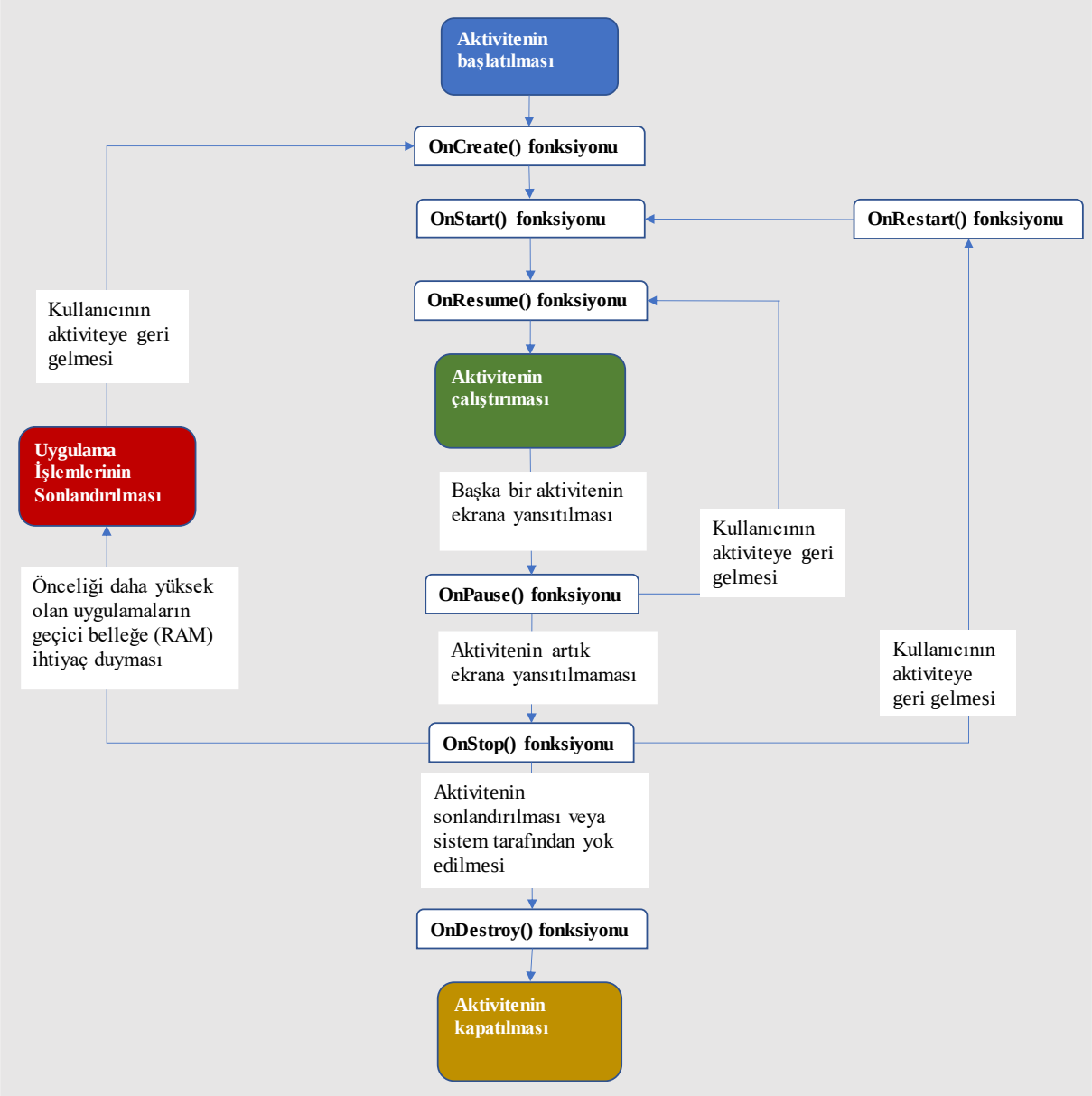
4.2.Uygulama Anatomisi

Manifest.xml dosyası, Android işletim sistemine yüklenen uygulamanın birçok özelliğini barındırmaktadır.

Her uygulama kök dizininde, manifest.xml dosyasını barındırmalıdır. Bu dosyada; uygulamanın ismi, ikonu, uygulama gereksinim ayarları gibi spesifik bilgiler bulunmaktadır. İşletim sisteminin güvenliği için oldukça önemli olan hangi izinlerin uygulamaya verilip verilmediği manifest.xml dosyasında, String sınıfı olarak tanımlanmaktadır (Ayed, 2015).

4.2.1. Aktivite

Aktivite, kullanıcının kişiler veya gelen SMS mesajları gibi ilgili uygulamanın bir ekranıdır. Aktivitenin içerisine, aktivite ile benzer şekilde çalışan fragmanlar yerleştirilebilir. Böylelikle birden fazla aktiviteyle yapılabilecek işlemler, fragmanlar vasıtasıyla aynı ekranda kullanıcıya gösterilebilir. Kullanıcı arabirimi, bileşenini göstererek sistem veya kullanıcıca başlatılan aksiyona tepki vermektedir. Aktivite kodu, aktivite kullanıcı arayüzü ekranda mevcutken ve hedefi varken çalışmaktadır. Bir uygulama kapatılasıya kadar, başlatılan aktivitelerin çoğunu ihtiva etmekte ve "geçmiş yığını" oluşturmakta, geçmiş yığınında oluşan aktiviteler geri planda tutulmaya devam edilmekte böylelikle ortaya çıkartılan tüm aktiveler "geri plan yığını" oluşturmaktadır. Bu geçmiş yığınını muhafaza etmek, kullanıcı bir önceki ekrana dönmek istediğinde ekranda halihazırdaki aktiviteyi hızlı bir şekilde ortadan kaldırarak bir önceki aktiviteyi ekranda görüntülemeyi sağlamaktadır (Pandiyan & Paranjape, 2012).



Şekil 4. 5. Aktivitenin yaşam döngüsü (*Activity*, 2022)

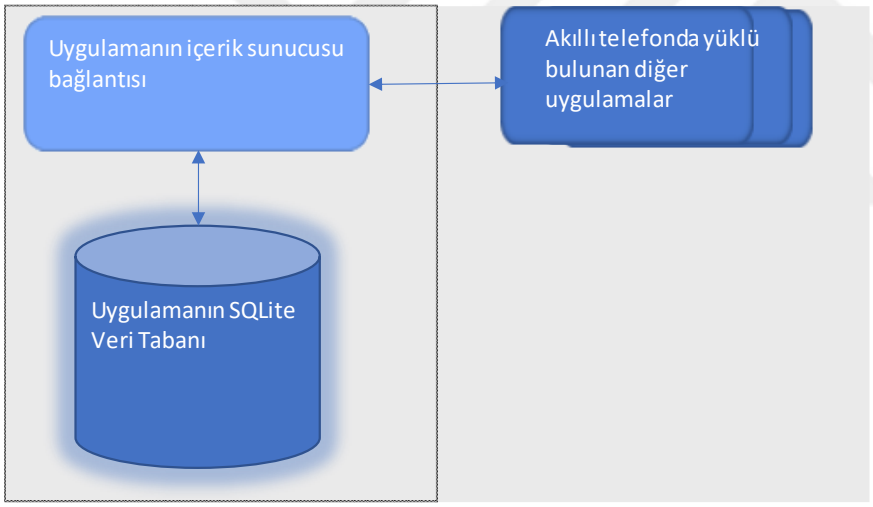
Şekil 4.5'te hangi fonksiyonların aktiviteyi nasıl etkilediği sunularak aktivitenin yaşam döngüsü gösterilmiştir. Bu fonksiyonların aktivitenin yaşam döngüsünü nasıl etkilediğini dikkate almak özellikle Android uygulamaların geliştirilmesi sırasında büyük önem arz etmektedir. Örneğin uygulamanın kapatılmasıyla beraber herhangi bir verinin silinmesi gerekiyorsa, verinin silinmesine ilişkin kod bloğu onDestroy() fonksiyonu içerisine yerleştirilmelidir.

4.2.2. Hizmetler

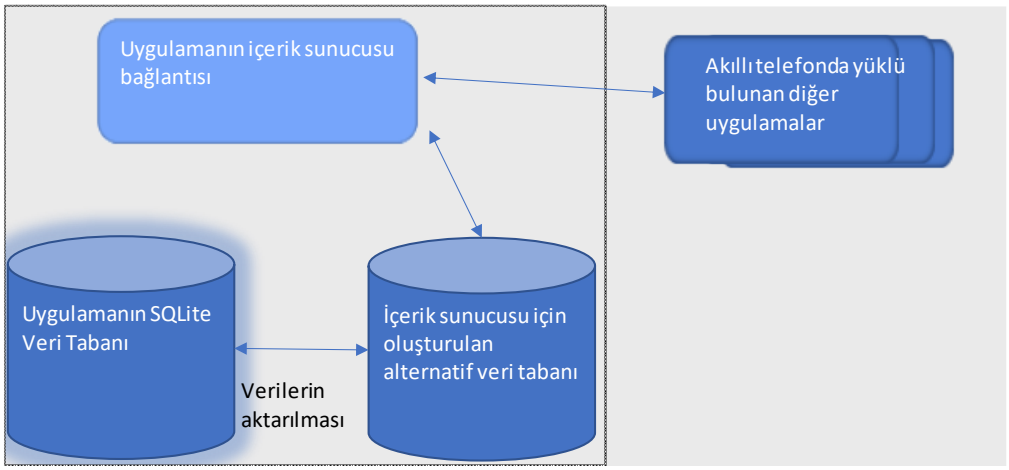
Hizmet, bir uygulama bileşeni olup, uzun süre çalışan görevleri arka planda devamlı çalıştırmayı sağlar. Bu kod kullanıcı etkileşimine ihtiyaç duyulduğunda çalışır. Kullanıcı farklı bir uygulamayı kullanmaya başlandığında dahi hizmetler çalışmaya devam edebilir. Örnek olarak ana ekrana gidildiğinde, bir tarayıcının dosya indirme işlemi devam eder.

4.2.3. İçerik Sunucu

Uygulamalardaki verilerin depolanması ve çağrılması içerik sunucusu üzerinden yerine getirilir. İçerik sunucusu, sistem ile uygulamalar ve uygulamalar arası veri aktarımını sağlar. Yine içerik sunucu sayesinde, uygulamanın verilere ulaşma ve değiştirme izinleri kontrol edilir. İçerik sunucusu bağlantısı, uygulamanın veri tabanı ile doğrudan sağlanabileceği gibi oluşturulan alternatif bir veri tabanı ile de sağlanabilir. Şekil 4.6 ve Şekil 4.7'de bu iki farklı durum gösterilmiştir (*Content Providers*, 2022).



Şekil 4. 6. İçerik sunucusunun veri tabanıyla doğrudan etkileşim halinde olması (*Content Providers*, 2022)



Şekil 4. 7. İçerik sunucusu için oluşturulan alternatif veri tabanıyla etkileşim halinde olması (*Content Providers*, 2022)

4.2.4. Yayın Alıcısı

Cihazın şarjının az kalması veya şarja takılması, cihaza uygulamaların ilgisini çekebilecek yeni bir verinin indirilmesi, uçak modunun açılıp kapatılması, Bluetooth'un açılıp kapatılması gibi durumlarda sistemle uygulamalar arasında bilgi akışının sağlanmasına yardımcı olur. Uygulamalar geliştirilirken sistemdeki hangi bilgi akışlarının uygulama için önem arz ettiği belirlenerek bu bilgi akışlarının uygulamalar tarafından yakalanması mümkün kılınabilir (*Broadcast Overview*, 2022).

4.3. Java Uygulama Programlama Arayüzü Çerçevesi (Java API Framework)

Android işletim sisteminin birçok özelliği, Java dilinde yazılan programlama arayüzlerinde mevcuttur. Android uygulamaları, bu programlama arayüzleri kapsamında geliştirilmektedir. Bu kapsamda uygulamaların kullanıcıya sunulan çeşitli buton, listeleri ve yazı kutuları gibi görüntü desenlerini düzenlenmesine yardımcı olan View System (Nimodia & Deshmukh, 2012); uygulama geliştirme dilindeki kodlarla ilgisi bulunmayan grafikler ve yerleşik dosyalar gibi verileri sağlayan Kaynak Yöneticisi; kullanıcıya bir iletişim uygulamasından mesaj geldiğinin bildirilmesi gibi uygulamaların kullanıcılara bildirim gönderebilmesini sağlayan Bildirim Yöneticisi; aktiviteleri başlatmaya, geri plana almaya ve kullanıcın yeniden aktiviteye ulaşmasını sağlayan Aktivite Yöneticisi; bir banka uygulamasındaki IBAN bilgisinin mesajlar uygulamasıyla paylaşılması gibi uygulamalar arası veya uygulamalarla sistem arası veri akışını sağlayan İçerik Sunucusu gibi uygulama programları arayüzleri (API) mevcuttur (*Platform Architecture*, 2021).

Uygulama Çerçevesini oluşturulan uygulama programlama arayüzü (API), Android işletim sisteminde büyük önem arz etmektedir. Bu çekirdek kütüphaneler Java yazılım dilinde oluşturulmuş olup Android Runtime üzerinde çalışan birçok çekirdek kütüphaneyi meydana getirirler. Bu çekirdek kütüphaneler; libc, libssl ve Freetype gibi optimize edilmiş yerel sistem kütüphanelerini kapsayarak işlevsel hale getirir. Her yeni Android sürümü, daha yüksek seviyedeki API'leri destekler (Brahler, 2010). Android işletim sistemi için geliştirilen uygulamalar, belirli bir API seviyesi ve üstü için tasarlanmış olabilir. Böyle bir durumda, daha düşük düzeydeki API seviyesinde kalan Android işletim sistemi sürümüne sahip cihazlar, mezkur uygulamayı çalıştıramayacaktır.

4.4. Donanım Soyutlama Katmanı (HAL)

Donanım soyutlama katmanında çeşitli sürücülerle Android cihazdaki donanımların, detaylı donanım seviyesine göre daha genel veya soyut seviyede kullanılarak daha işlevsel şekilde donanımlardan yararlanılması sağlanmaktadır (Huang & Wu, 2018).

Donanım soyutlama katmanı, ilgili kütüphane modülleriyle beraber akıllı telefonun çeşitli donanımların işletim sistemi tarafından kullanılmasına, imkan sağlamaktadır. Bu sayede ilgili uygulama; telefonun kamerası, bluetooth'u, WiFi bağlantısı, operatör sinyal alıcı anteni, kamera flaşı gibi donanımlara ulaşmak istediğinde işletim sistemi o donanıma ilişkin kütüphane modüllerini yükleyerek uygulamanın donanımın özelliklerini kullanmasına, imkan tanır (*Platform Architecture*, 2021).

4.5. Yerel C/C++ Kütüphaneleri

Android Run Time ve Donanım Soyutlama Katmanı gibi birçok Android sistem bileşeni, C veya C++ dilleriyle yazılmış yerel kütüphanelerden oluşmaktadır. Dolayısıyla bu yerel kütüphaneler, Android işletim sisteminin mimarisinde önemli bir konuma sahiptir (*Platform Architecture,* 2021).

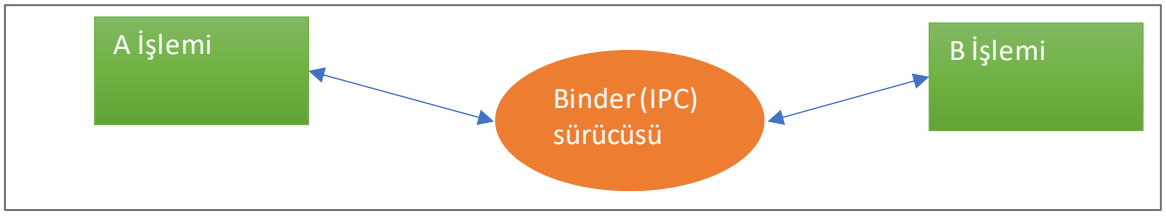
Surface Manager, pencere yöneticisi şeklinde çalışarak uygulama pencerelerinin doğrudan ekrana yansıtmaz. En son pencereyi ekrana yansıtarak diğer pencerelerin ekran dışı arabellekte muhafaza edilmesini sağlar. Media Framework (Medya çerçevesi), medyalara ilişkin kod çözücüler barındırarak farklı medyaların kaydedilmesini ve oynatılmasını sağlar. Android, SQLite'ı veri tabanı motoru olarak kullanır. Webkit, HTML içerikleri görüntülemek için kullanılır. OpenGL, iki boyutlu veya üç boyutlu grafik verilerini ekranda görüntülemek üzere kullanılır (Khan & Shahzad, 2015).

Media Framework (Medya Çerçevesi); OpenCORE, vorbis ve sonivox gibi medya kütüphanelerin üzerine yapılandırılmıştır. Android Media Framework, kütüphanelerin altında bulunan tüm hizmetler için devamlı şekilde arayüz oluşturarak kullanıcılara sunmayı amaçlar (Song ve diğerleri, 2010).

4.6. Linux Kernel

Linux Çekirdeğinin modifikasyon yapılmış halini, Android işletim sistemi kullanmaktadır. Her ne kadar bazı durumlar için donanım sürücülerin yeniden oluşturulması gerekse de Linux çekirdeği, birçok donanım mekanizmasını desteklemektedir (Khan & Shahzad, 2015).

Android; cihaz sürücüleri, hafıza yönetimi, işlem yönetimi, dosya sistemi ve ağ yönetimi için açık kaynak kodlu Linux çekirdeği kullanmaktadır. Android çekirdeği, temel Linux çekirdeğine bazı özellikler eklenerek veya çıkarılarak oluşturulmuştur. Binder (IPC) sürücüsü, Şekil 4.8'te gösterildiği gibi işletim sistemindeki çalışan işlemler arasında veri alışverişini gerçekleştirerek bunlar arasındaki iletişimi sağlar. IPC Binder, bu aktarmayı yaparken performansı artırmak için paylaşılan hafızayı kullanır. IPC için kullanılan Binder sürücüsü; geçici belleğin alanın daralması halinde işlemleri sonlandırmak üzere etkinleşen düşük geçici bellek (RAM) sonlandırıcısı, tek bir şarj dolumu ile daha uzun batarya ömrü sunmayı amaçlayan güç yönetimi, kayıt defterci ve ashmem (bilinmeyen paylaşılan hafıza) ile birlikte kernel'i de içermektedir (Brahler, 2010) (Aneeshya Rose K. M., 2020).



Şekil 4. 8. Binder (IPC) sürücüsünün işletim sistemindeki devam eden işlemler arasında argümanların aktarılması (Aneeshya Rose K. M., 2020).

5. ANDROID AKILLI TELEFONLARIN ADLİ BİLİŞİM BAKIMINDAN İNCELENMESİ

İlk mobil telefonların depolama kapasiteleri oldukça kısıtlı olduğundan cihaz üzerinde yapılan adli bilişim incelemeleri de oldukça kısıtlı olmakta ve daha çok servis sağlayıcıda bulunan gelen ve giden arama ve mesajlara ilişkin bilgiler üzerinden soruşturmalar yürütülmekteydi. Ancak mobil telefonların depolama alanlarının ve işlemci güçlerinin gelişmesiyle beraber bu cihazlar başlı başına, adli bakımından büyük bir delil değerine sahip olmuşlardır (Ahmed & Dharaskar, 2008).

2000'li yıllarda dahi mobil telefonlardaki deliller sayesinde birçok failin yargılamasının yapılarak cezalandırılması mümkün olmuştur (Baggili ve diğerleri, 2007). Günümüzde ise mobil telefonlar oldukça gelişerek akıllı telefonlar olarak adlandırılmaya başlanmış, depolama kapasiteleri ve işlemci güçleri oldukça gelişmiştir. Bunun doğal sonucu olarak da işlenen suçlara ilişkin delil barındırma potansiyelleri yüksek boyutta artmıştır.

Android ilk seferinde 2007 yılında başlıca tablet veya akıllı telefonlarda kullanılmak üzere yayınlanmış işletim sistemidir. İlk olarak 2008 yılı Ekim ayında Android akıllı telefonu piyasaya sürülmüştür. Android işletim sistemi açık kaynak kodlu olup Google yılda bir kere işletim sisteminin büyük bir geliştirilmiş versiyonunu yayınlanmaktadır (Rick ve diğerleri, 2014).

2016 yılının Aralık ayında piyasada en yaygın Windows işletim sistemi ile Android işletim sisteminin piyasa etkinlikleri eşitlenmiş olup devam eden yıllarda ise, Android işletim sisteminin yaygınlığı devamlı artarak piyasada baskın işletim sistemi haline gelmiştir. 2022 yılının Kasım ayında ise, tüm işletim sistemleri arasında Android %43,47 piyasa payıyla cihazlarda en yaygın kullanılan işletim sistemi durumundadır (StatCounter, 2022).

Akıllı telefonların nispeten kişisel bilgisayarlara göre daha uygun fiyatlarda olması nedeniyle, bu cihazlara ulaşmak çok daha kolay olabilmektedir. Yine düşük gelir grubundaki bulunan ve suç işlemeye yatkın insanların akıllı telefonlardan başkaca bir cihaz kullanmayarak yaşamlarını temel olarak akıllı telefonlarındaki yaptıkları işlemler ile sürdürebilmeleri mümkündür (Petraityte ve diğerleri, 2017: 79-89). Bu durum, akıllı telefonların işlenen suçlarda büyük bir delil potansiyeline sahip olmasına sebebiyet vermektedir.

Akıllı telefonlar, birçok bakımından işlenen suçla bağlantılı olabilir. Nitekim suçun işlenme aşamalarında iletişim vasıtası veya doğrudan suçun işlenme aracı olarak kullanılma, içerdiği verilerle suçu aydınlatma, mağdurun bilgilerini içerme özelliklerine sahip olabilir (Lutes & Mislan, 2008).

Telefon adli bilişimi, telefon sektörünün hızla büyümesiyle, en hızlı büyüyen ve değişen adli bilişim disiplini olduğu tartışılabilir. Bu durum belirli fırsatlar sağlamakla birlikte çeşitli zorluklar da meydana getirmektedir. Günümüzde akıllı telefon olarak bilinen cihazların ortaya çıkması, telefon endüstrisinin gelişmesinde yeni bir dönem oluşturmuştur. Geleneksel telefonların aksine, akıllı telefonlar kullanıcılara birçok veri ile etkileşim sağlamasına yardımcı olan işletim sistemleri ve birçok uygulama ile donatılmıştır (Alamin & Mustafa, 2015).

Akıllı telefonlar bilgisayar gibi diğer potansiyel dijital delillere göre, sahiplerince genellikle fiziksel olarak kendilerine daha yakın tutularak devamlı surette sahiplerinin beraberinde taşınırlar. Nitekim bu cihazların cepte taşınabilecek boyutta olması, devamlı surette insanların bu cihazları yanında taşımasını büyük oranda kolaylaştırmaktadır. Kullanıcısın gün içerisinde sürekli bu cihazlarla etkileşim halinde bulunması kuvvetle muhtemel olması sebebiyle cihazların suçun işlendiği alana götürülmüş olması; olay yerinde akıllı telefonu kullanmak suretiyle kişilerle iletişime geçinilmiş bulunması halinde konum bilgisinin oluşması; akıllı telefonla olay yerinde ses, video kaydı veya fotoğrafın çekilmesi; akıllı telefonda suça ilişkin mesajlaşma kayıtlarının bulunması ihtimalleriyle bu cihazların delil potansiyeli oldukça artmaktadır. Kaldı ki bu cihazların doğrudan araç olarak kullanılması suretiyle de suçların işlenmesi mümkündür. Nitekim akıllı telefonların günümüzde oldukça güçlü donanımlara ve işlevlere sahip olmasıyla beraber kişisel bilgisayarla eşdeğer biçimde zengin veri türleri barındırabilirler (Walnycky ve diğerleri, 2015). Akıllı telefonlar, birçok soruşturmada, en kritik ve önemli delil haline gelmiş bulunmaktadır (Kim & Lee, 2020).

Günümüzde yazılım sistemlerinin parçası olan Android akıllı telefonlar oldukça yayılarak, temel çağrı yapma ve yanıtlamanın yahut SMS göndermenin yanında ses veya video kaydı yapılmasını; fotoğraf çekilmesini; internet sitelerini ziyaret etmeyi, ziyaret edilen internet sitelerinden verileri kaydetmeyi; doküman, fotoğraf, video veya ses kaydı dahil olmak üzere birçok farklı dosya türünü görüntülemeyi veya oynatmayı; bu dosyaları başka kişilere transfer etmeyi; banka uygulamalarıyla para göndermeyi veya emtia, döviz alım satım işlemlerini gerçekleştirmeyi; sosyal medya uygulamalarıyla kişisel paylaşımlar yapmayı, diğer kişilerin paylaşımlarını görüntüleyebilmeyi veya bu uygulamalar üzerinden haberleri

takip edebilmeyi; çevrimiçi mesajlaşma; sesli veya görüntülü görüşme gerçekleştirmeyi sağlamaktadır. Bu denli farklı işlevleri bulunan akıllı telefonların oldukça kişisel olması ve her akıllı telefonun farklı kişilerce kullanımı neticesinde bu akıllı telefonlarda oluşan verileri çok büyük oranda özgün kıldığı aşikardır (Roy ve diğerleri, 2016). Hatta zoraki bir yaklaşımla, akıllı telefonların kullanılması sonucu oluşan verilerin neredeyse biyometrik boyutta olduğu söylenebilir. Bu verilerin bazıları çeşitli bulut sistemlerinde veya servis sağlayıcıların altyapısında yahut ağında saklanabilmektedir (Androulidakis, 2012: 75-99). Bu durum sebebiyle akıllı telefonlar, adli bilişim açısından çok önemli bir delil değeri taşır.

Akıllı telefonların geniş kullanımı, hem ceza hukuku hem de diğer hukuk dalları bakımından adli bilişime önünde sonunda kaynaklık etmektedir. Mobil Adli Bilişimi, yasal perspektif bakımından hukuki olarak kabul edilen adli bilişimsel yöntemleri kullanmak suretiyle elde edildikten sonra doğru bir şekilde muhafaza edilmiş mobil cihazdan imaj alınması ve imajın analiziyle dijital delil elde etmektir. Telefon üreticilerin çok hızlı büyümesi ve işlemci (CPU) mimarisi ve işletim sistemlerinin çeşitliliği nedeniyle zorluklar da oldukça artmıştır. Nitekim her geçen gün yeni bir telefon üreticisi piyasaya giriş yapmakta, Android işletim sistemini kullanmak suretiyle kendi donanım modelleri ve kullanıcı arayüzleriyle farklı kombinasyonlar oluşturacak şekilde akıllı telefonlar üretmektedirler. Her ne kadar Android işletim sistemi açık kaynak kodlu olsa da Android akıllı telefon üreticileri sistem dosya yapılarını (ROM) kendileri özgü olacak şekilde tasarlamakta ve bunlar kapalı kaynak kodlu olmaktadır. Dolayısıyla adli bilişim araçları ve ekipmanları, bazı Android akıllı telefonlarda etkili olabilirken bazı akıllı telefonlarda ise başarısız olabilmektedir (Rick ve diğerleri, 2014) (Roy ve diğerleri, 2016).

Akıllı telefonlardaki oldukça hızlı donanımsal ile yazılımsal gelişme ve güncellemeler de adli bilişim araç ve ekipmanların, yeni akıllı telefonlar veya işletim sistemleri versiyonlarında etkisiz kalabilmelerine sebebiyet verebilmektedir (Ahmed & Dharaskar, 2008). Zira adli bilişim, hedef akıllı telefonların belirli açıklarından yararlanmak suretiyle de gerçekleştirilebildiğinden her yeni işletim sistemi güncellemesiyle akıllı telefonların güvenliği artırılmakta ve güvenlik açıklıkları kapatılmaya çalışılmaktadır. Yine hedef akıllı telefonun donanımsal zarara uğramış olması ve yazılımsal hatalar barındırması da adli bilişim açısından güçlükler meydana getirmektedir. Bununla beraber akıllı telefonlarda, aynı amaca hizmet eden birçok farklı uygulama bulunmaktadır. Örneğin internet sitelerini ziyaret etmek için Chrome, Firefox, Opera, Brave gibi internet tarayıcı uygulamaları bulunduğu gibi her üreticinin kendi akıllı telefonu için geliştirdiği yerleşik internet tarayıcısı da

bulunmaktadır. Benzer şekilde kişiler arası iletişimi sağlamak amacıyla Whatsapp, Telegram, Skype, Viber vb. birçok farklı uygulama bulunmaktadır. Bu uygulamaların çalışma ve veri depolama biçimleri farklılık gösterebilir. Kaldı ki bu uygulamaların devamlı güncellenmesi nedeniyle eski sürüm çalışan araç ve ekipmanlar, yeni sürümlerde başarısız olabilecektir. Bu denli uygulama çeşitliliği de adli bilişim pratiğinin zorluklarından birisini oluşturmaktadır. Standart yazılım ve donanımın bulunmaması, mobil adli bilişimi için ileriki aşamalarda da zorluklar oluşturmaktadır. Yine bazen analiz için getirilen veya kurtarılan depolama donanımı hasarlı, bozuk olabilir ve o depolama cihazından veri elde etmek oldukça zor gerçekleştirilebilir. Yine adli bilişimindeki bir zorluk da her yeni piyasaya sürülen cihazdaki depolama alanın ve işlemci gücünün geliştirilmiş olması nedeniyle elde edilen ve analiz edilecek verilerin artmasıdır (Roy ve diğerleri, 2016) (Kim & Lee, 2020).

Kaldı ki Android akıllı telefonlar parola, desen, parmak izi, yüz tanıma vb. yöntemlerle yahut verilerin kriptografik şifrelenmesi yöntemleriyle korunabilir. Bu durumlar da adli bilişim analizleri için oldukça büyük güçlükler meydana getirmektedir (Umale ve diğerleri, 2014).

Mobil adli bilişimin popüler olmasına, Android akıllı telefonların teknolojilerinin ve güvenlik sistemlerinin hızlı bir şekilde gelişmesine ve büyük kademe kaydetmesine karşın; halen mobil adli bilişim ilk gelişim safhalarında kalmıştır. Mobil adli bilişimi, akıllı telefonların yazılım ve donanımsal gelişimlerinin çok gerisinde kalmış bulunmaktadır. Bu nedenle mobil adli bilişimden etkili sonuçlar elde etmek git gide güçleşmektedir. Yakın gelecekte de mobil telefonların adli bilişim analizin yapılmasını tek başına sağlayabilecek bir araç veya ekipmanın geliştirilmesi, oldukça zor görünmektedir (Tayeb & Varol, 2019).

5.1. Hazırlık Aşaması

Android akıllı telefonların bulunabileceği bir olay mahaline gitmeden önce, hangi yazılım araçları ve ekipmanların kullanılacağının önceden belirlenmesi oldukça önemlidir. Olay yerinde bulunacak adli bilişim uzmanların yeterli teknik bilgiye sahip olmaları gereklidir. Nitekim adli bilişim aşamalarından en başından sonuna kadar titiz bir şekilde süreçlerin yönetilmesi gereklidir. Herhangi bir aşamada yapılacak hata, soruşturma ehemmiyeti yüksek bir delilin kaybedilmesine sebebiyet verebilecektir. Bu bağlamda kullanılabilecek ticari yazılımlar olduğu gibi açık kaynak kodlu yazılımlar da bulunmaktadır. Tek bir ticari yazılım aracı, adli bilişim süreçlerinin çoğunu karşılamak üzere tasarlanmaya çalışılsa da genelde tek bir araçla adli bilişim süreçlerinin tamamının gerçekleştirilmesi güçtür. Nitekim "Android Akıllı Telefonların Adli Bilişim Bakımından İncelenmesi" Başlığının altında bu

akıllı telefonların adli bilişimsel analizi açısından birçok güçlük barındırdığı belirtilmiştir. Açık kaynak kodlu yazılımlar ise, daha çok adli bilişim süreçlerin birisini yahut bir sürecinin parçasını yerine getirmek üzere tasarlanmıştır. O yüzden ticari de açık kaynak kodlu da olsa adli bilişim yazılım araçlarının kombine bir şekilde kullanılması daha etkili neticeler verecektir (Umale ve diğerleri, 2014) (MRKAIĆ, 2016).

Akıllı telefon teknolojisi o denli hızlı gelişmektedir ki en iyi araçların kullanılması, tek başına başarılı işlemlerin yapılmasını sağlayamamaktadır. Bu yüzden adli bilişim alanında çalışacak inceleyici ve analizciler, devamlı surette eğitilmeli ve kendilerini yeni gelişmelere karşı güncel tutmalıdırlar (Androulidakis, 2012: 75-99).

Akıllı telefonların model ve işletim sistemlerinin çok çeşitli olması nedeniyle telefonların markaları, modelleri, işletim sistemleri, işletim sistemi versiyonları vb. hakkında özelliklerine göre hangi ekipmanların, yazılımların veya araçların etkili olabileceğine ilişkin dokümantasyonlar yapılarak adli bilişim analizlerinin geliştirilmesi gerekmektedir(Baggili ve diğerleri, 2007) .

Adli bilişim uzmanları, olay yerine gitmeden önce asgari ekipman olarak yanlarında uygun şarj cihazı ve hedef cihazın kablosuz bağlantılarını kesecek bir çanta taşımalıdırlar (Induruwa, 2009). İmaj alma ve imaj alındıktan sonra imajın analizin yapılması işlemleri için birden fazla farklı araç veya ekipmanların hazır bulundurulması gereklidir. Nitekim bazı araçlar ile bu işlemlerin gerçekleştirilmesinin başarısız olması halinde, farklı yazılım araçları veya ekipmanları ile gerçekleştirilecek işlemlerde başarılı olma ihtimali bulunmaktadır (Rick ve diğerleri, 2014).

Analiz yapılırken kullanılacak yazılımlar elverişli ve denenmiş olmalıdır (Androulidakis, 2012: 75-99). Nitekim daha önceden denenmemiş yazılımların doğrudan hedef cihazın analizinde kullanılması halinde, cihazdaki verilerin değişmesi ve veri kaybı yaşanması söz konusu olabilir.

Akıllı telefonların işlenmiş olan suçla bağlantısı bu denli yüksekken, aynı zamanda kendisinin de doğrudan tehlike oluşturulabileceği durumlar da bulunmaktadır. Nitekim bu duruma, alacağı bir çağrıyla kendini infilak ettirebilecek akıllı telefonlar örnek olarak verilebilir (Androulidakis, 2012: 75-99).

5.2. Android Akıllı Telefonların Tanımlanması

Olay yerine gelen kolluk görevlileri yahut inceleyiciler hedef cihaza doğrudan temas etmemelidir. Zira hedef cihaz üzerinde parmak izi gibi biyometrik verilerin bulunması mümkün olup eldiven vb. kullanılmadan cihaza müdahale edilmesi bu delillerin bozulmasına veya yok olmasına sebebiyet verebilecektir. Bununla beraber olay yerine ilk temas eden bu kişiler, dijital delillerin yanında bulunabilecek silah, uyuşturucu madde, biyometrik kalıntı ihtiva edebilecek eşyalar vb. delillerin de elde edilmesine hazırlıklı olmalı ve muhafazasını sağlamalıdır. Nitekim olay yerinde ele geçirilen diğer deliller de hedef cihazdan elde edilecek verileri destekleyebilir, maddi gerçeğe ulaşmada büyük rol oynayabilir (Androulidakis, 2012: 75-99).

Potansiyel dijital delil barındıran bir yerde bulunulduğunda inceleyiciler, ilk olarak video kaydıyla beraber gözlemde bulunarak incelemeye başlamalı ve dijital delil barındıran cihazların ilk durumuyla ilgili doğrudan belgelendirme yapmalıdır (Induruwa, 2009).

Olay yerindeki tüm görünen bilgiler hakkında rapor tutulmalıdır. Tüm dijital cihazlar, kablolarıyla, şarj cihazı, çıkarılabilir ortamları vb. ile fotoğraflanmalıdır. Fotoğraflanma işlemi yapılırken cihazlara dokunmamaya özen gösterilerek direkt bulunduğu yerdeki durumu ile fotoğraflanmalıdır. Cihazların ekranı açık durumda ise, cihazın ekranının video kaydı alınmalı ya da en azından cihaz ekranı o durumda fotoğraflanmalıdır (Rick ve diğerleri, 2014).

Hedef cihazda adli bilişim incelemecileri tarafından dikkate alınması gereken bazı özelleştirmeler yapılmış olabilir. Örneğin parola korumasına ek olarak inşa edilmiş cihazın kendini kitlemesi veya üzerindeki tüm verileri silmesi, adli bilişim analizin yapılmasını engelleyecek veya analiz araçlarına zarar verecek kötü amaçlı yazılımlar, donanım tuşlarına çeşitli kombinasyonlarda basılması halinde etkinleşen cihazı koruyucu yazılımlar, cihazın farklı konumda bulunduğunun algılanması halinde cihazdaki tüm verilerin silinmesi, cihazla ilişkili patlayıcılar veya bubi tuzakları, cihazdaki verilerin silinmesini tetikleyebilecek alarm sistemleri söz konusu olabilir (Rick ve diğerleri, 2014).

Adli bilişim uzmanları, olay yerindeki akıllı telefona patlayıcı veya bubi tuzağı gibi herhangi bir düzenek kurulup kurulmadığını, güvenlik önlemlerini almak suretiyle kontrol etmelidirler.

Olay yerinde birçok farklı Android akıllı telefon bulunabilir. Bu akıllı telefonların hangi üretici tarafından oluşturulduğu, marka ve modeli, hangi Android işletim sistemi sürümünde

çalıştığının tespit edilmesi gerekmektedir. Ayrıca cihazın halen çalışmakta yahut ekranın açık olup olmadığının da belirlenmesi gereklidir. Nitekim adli bilişimin ileriki süreçleri için kullanılacak yazılım araçları veya ekipmanların belirlenmesi, Android akıllı telefonunun mezkur özelliklerin tespit edilmesiyle gerçekleştirilecektir. Bu tespitin olay yerine ulaşıldığında derhal yapılmasının zaman ve veri kaybı yaşanmaması açısından önemi bulunmaktadır.

Birçok akıllı telefon marka ve modeli bulunduğundan ilk bakışta uzmanların dahi hedef akıllı telefonun marka ve modelini belirlemekte zorluk yaşaması mümkündür (Lutes & Mislan, 2008).

Hedef akıllı telefonun tanımlanması sırasında, birebir aynı telefon marka modeline ilişkin kılavuzun baz alınarak uygun kablo, şarj cihazı vb. ekipmanların kullanılması sağlanılmalıdır (Androulidakis, 2012: 75-99).

Cihazın açık durumda olması halinde iki farklı prosedür izlenmesi gereklidir. İlk olarak, cihazın herhangi bir bağlantıyla başka cihazlarla etkileşeme geçmesi engellenmelidir. Bu bakımdan özellikle cihazın internet bağlantısı kesilmelidir. Nitekim internet bağlantısının devam etmesi halinde, cihaza veri gönderilerek inceleyiciler tarafından cihazın elde edildiği sıradaki durumu değiştirilebilir. Cihazın internet bağlantısına erişememesi veya herhangi bir şekilde çağrı yahut SMS almaması için Faraday çantası kullanılarak cihazın dışarıyla tamamen bağlantısı kesilebilir. İkinci yapılması gereken ise, cihazın bataryasının bitmesini önleyerek cihazın açık durumda olması halinin muhafaza edilmesidir. Dolayısıyla cihazın bataryasının bitme ihtimali varsa, şarj cihazına bağlanarak kapanmasının engellenmesi gereklidir (Induruwa, 2009).

5.3. Delillerin Toplanması ve İmaj Alınması

Hedef akıllı telefon elde edildiği andan itibaren Faraday çantasına konulmak, uçak modunun açılması gibi önlemlerle ağ bağlantısına erişiminin ve servis sağlayıcısından sinyal alabilmesi engellenmelidir. Nitekim bu gelen bir SMS, çağrı veya internet bağlantısı erişimi hedef cihazın verileri değiştirilebilir, silinebilir yahut tamamen yok edilebilir. Cihazın bu bağlantıların kesilmesini sağlamak amacıyla asla gücü kapatılmamalıdır. Aksi halde yeniden açılması sırasında parolanın girilmesini isteyebilecektir (Androulidakis, 2012: 75-99) (Lin, 2018: 338).

Faraday çantasına veya benzer bir sinyal kesici çantaya cihazın konulması halinde, aynı zamanda çantanın içerisinde bataryanın şarj edilmesi de sağlanmalıdır. Nitekim cihazın sürekli sinyal almak için çabalaması, daha hızlı bir şekilde bataryasının tükenmesine neden olacaktır (Androulidakis, 2012: 75-99).

Hedef cihazdaki tarih ve saat doğru olmayabileceğinden cihazın elde edilmesi sırasında tarih ve saat ile cihazdaki tarih ve saat not edilerek uyumsuzluk bulunup bulunmadığı ve uyumsuzluk nispeti karşılaştırılmalıdır (Rick ve diğerleri, 2014).

Android akıllı telefonlardan elde edilebilecek verilere örnek olarak şunlar verilebilir: telefon kayıt defteri ve kişiler; gelen, giden ve cevapsız çağrılar; gelen ve giden SMS ve MMS; ses kayıtları, sesli notlar ve çağrı sesleri; fotoğraflar, videolar, grafikler ve çalışma alanları; takvime kayıtlı etkinlikler, alarm saatleri ve hatırlatıcıları, yapılacaklar listesi; yazılı notlar; e-postalar; akıllı telefonla ziyaret edilen internet siteleri; dokümanlar; PIN gibi kullanıcı tanımlayıcıları ile IMEI gibi cihaz tanımlayıcıları; kaydedilen kablosuz internet ağları; GPS konum bilgileri; kullanıcının sıklıkla klavyede yazdığı kelimelere göre kayıtlı sözcük tahminleri; GPRS, WAP ve internet ayarlarına ilişkin veriler. Akıllı telefonlarda suçla bağlantılı veriler, cihazın dahili veya harici hafızasında yahut SIM kartında bulunabilir. Yine aynı zamanda failin bir bulut sistemi vasıtasıyla akıllı telefonu senkronize ediyor olması halinde, kişisel bilgisayarında da bulanabileceği unutulmamalıdır (Androulidakis, 2012: 75-99).

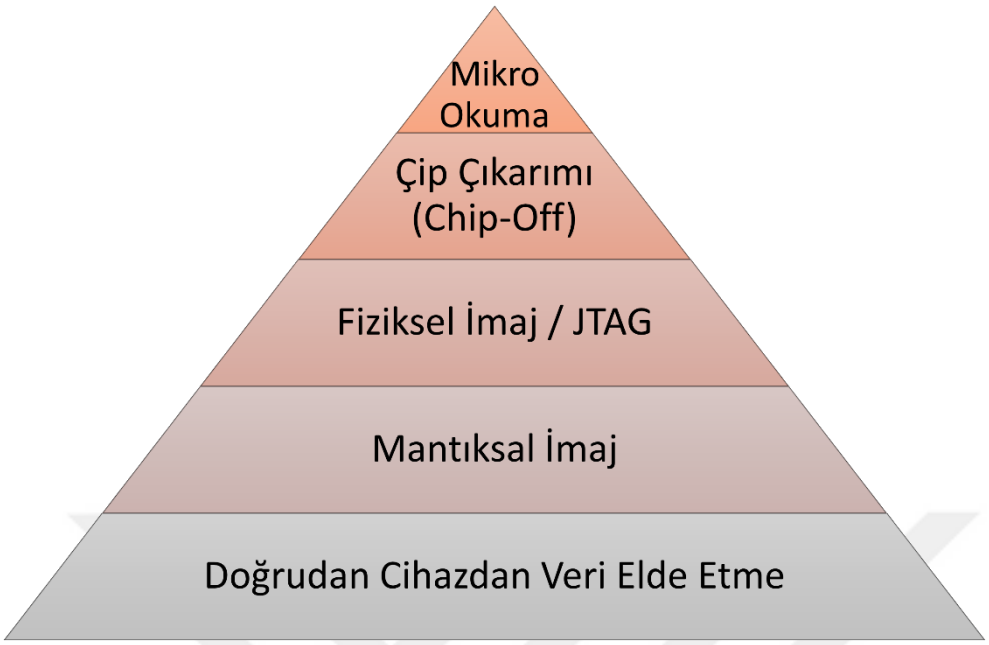
Eğer cihaz parola, PIN veya daha farklı tanımlama mekanizmaları ile korunmaktaysa; cihaz sahibinden parola, PIN vb. vermesi istenebilir. Cihaz sahibinin parolayı vermeye rızasının mevcut olması halinde, parolayla cihaza erişim sağlanabilir. Ancak cihazın parolayla kilidinin açılması için sahibinin eline kesinlikle verilmemesi gereklidir. Nitekim eline aldığı sırada, cihazda mevcut olan verileri yok etmesi yahut değiştirmesi mümkün olabilecektir (Androulidakis, 2012: 75-99). Cihaz sahibinin bu bilgileri sunmaması ya da sunmasının mümkün olmaması hallerinde, hedef cihazın çevresinde bulunan materyaller incelenebilir. Nitekim bir kağıt parçasına, cihazının PIN veya parolanın yazılmış olması mümkündür. Zira servis sağlayıcısı SIM kartı ile beraber PIN ve PUK kodlarını bir kağıt parçasında ya da SIM kartının muhafaza edildiği materyal üzerinde paylaşabilmektedir. Yine PIN kodunun, bu yöntemlerle elde edilememesi halinde servis sağlayıcısı ile iletişime geçilerek PIN kodunun aşılması sağlanabilir (Rick ve diğerleri, 2014).

Brute force attack gibi yöntemlerle cihazın parola veya PIN'inin aşılması mümkünse de belirli parola deneme girişimlerinden sonra cihazdaki tüm verilerin silinmesi, yıkıcı uygulamaların etkinleşmesi mümkündür. SIM kartında ise, belirli deneme girişim sayısından sonra tamamen SIM kartı kullanılmaz hale gelebilir (Rick ve diğerleri, 2014).

Olay yerinde bulunan hedef cihazla ilişkili olabilecek SIM kart, SD kart, kişisel bilgisayar vb. cihazlar da değerli bilgiler muhteva edebilirler. Hasarlı cihazlardan çeşitli yöntemlerle veri elde edilebileceğinden daha ayrıntılı inceleme için laboratuvara götürülmesi gerekmektedir (Rick ve diğerleri, 2014).

Akıllı telefonlarda bulunan SIM kartları da küçük boyutta da olsa veri depolayabilmektedir. SIM kartlarının PIN koduyla korunuyor olması halinde, yanlış girilen PIN ve PUK kodlarıyla SIM kartının tamamen işlevsiz hale gelmesi mümkündür. SIM kartlarının imajının alınması mümkün olmadığından dolayı incelemenin doğrudan orijinal SIM kartının üzerinden yapılması gerekmektedir. Bu nedenle SIM kartını inceleyecek analizcilerin oldukça dikkatli olmaları gerekmektedir. Ele geçirilen akıllı telefonun gücünün kapalı olması, SIM kartında PIN kodu bulunması, sahibinin bu kodu sunmaması hallerinde servis sağlayıcısı ile iletişime geçilerek akıllı telefon SIM kart kilidinin geçilmesi sağlanabilir. Ancak servis sağlayıcısı yardımıyla telefon SIM kart kilidinin geçilmesi, aylar sürebilir (Androulidakis, 2012: 75-99).

5.3.1. İmaj Alma Yöntemleri



Şekil 5. 1. Cihazdan veri elde edilmesine ilişkin aşamaların uygulanabilirliğini korumak açısından sırasıyla takip edilmesi gereken aşamalar (Rick ve diğerleri, 2014)

Şekil 5.1'de hedef cihazdan veri elde edilmesini uygulanabilecek yöntemler gösterilmiştir. Hedef cihazdan veri elde etmek için tüm yöntemlerin sırasıyla kullanılması gerekmemektedir. Ancak piramitte üst basamakta bulunan herhangi bir yöntem kullanıldıktan sonra, alt basamaktaki yöntemin uygulanabilirlik imkanının ortadan kalkabileceği göz önüne alınmalıdır. Örneğin cihazın chip-off vasıtasıyla belleğinin cihazdan ayrılması yöntemiyle imajının alınması durumunda, cihazın mantıksal imajının alınması mümkün olmayacaktır (Rick ve diğerleri, 2014).

Cihazın geçici belleğinin (RAM) imajı alınacaksa, ilk başta bu işlemin yapılması ehemmiyetlidir. Nitekim geçici bellekteki veriler, devamlı surette değişmekte ve cihazın gücünün kapanması halinde bu verilere ulaşmak mümkün olmayabilecektir (Rick ve diğerleri, 2014).

Hedef cihazdan veri elde edildikten sonra, analiz işlemine geçmeden önce, veri kirliliğinin azaltılması, önemli verilerin ayırt edilerek bu veriler üzerinde analiz yapılması; zaman, maliyet ve soruşturmanın etkinliğini artırmak açısından önemlidir (Marturana ve diğerleri, 2011).

Her ne kadar geleneksel adli bilişim yaklaşımları hedef cihazın elde edildiği sırada cihazdaki verilerin değiştirilmemesi gerektiğini belirtse de Android akıllı telefonlarda root yetkisini kazanmak, birçok adli bilişim aşaması için zorunluluktur. Dolayısıyla cihazdaki verilerin elde edilmesi için root yetkisini kazanmak; kazanma işlemi sırasında gerçekleştirilen uygulamaların tümünü raporlamak, imaj alma işlemi tamamlandıktan sonra root yetkisi kazanma işleminin geri alınması koşullarının sağlanmasıyla gerçekleştirilebilir. Zira yapılan bir çalışmada (Almehmadi & Batarfi, 2019) root yetkisinin kazanılmasının cihazdaki diğer verilerin bütünlüğünü bozmadığı ve bu yöntemle elde edilen verilerin güvenilirliği bulunduğu sonucuna ulaşılmıştır.

Depolama alanında silinmiş olan bir veri, her ne kadar kullanıcı tarafından tamamen silindiği düşünülebilse de silinen verinin bulunduğu kısmın üstüne yeni bir veri yazılasıya kadar silinen verinin kurtarılması mümkün olabilecektir (Androulidakis, 2012: 75-99).

Android akıllı telelefonların mantıksal veya fiziksel imajının yazılım araçları vasıtasıyla elde edilebilmesi için cihazın USB debug modunun açılması gerekmektedir. Kilitli Android akıllı telefonların USB debug modunun açılabilmesini sağlayan araçlar olsa da bu araçlar oldukça kısıtlı sayıdaki Android akıllı telefonlarda çalışmaktadır (Rick ve diğerleri, 2014).

Yine WireShark ve Networkminer gibi araçlarla da hedef Android akıllı telefonun internet ağı izlenilmesi yoluyla gönderilen ve alınan paket detaylarından da veri elde edilebilir. Bir çalışmada, Android akıllı telefon üzerinden gönderilen e-postalara ilişkin e-posta sunucusu, kullanıcı adı ve parola, e-postanın gönderilme tarih ve saati, kaynak ve hedef sunucuların ip adresleri vb. birçok bilgi edinmeleri mümkün olmuştur (Umar ve diğerleri, 2019).

5.3.1.1. İmaj Almadan Önce Cihazın Root Yetkisinin Kazanılması ve Önemi

Root yetkisi kazanılmadan Android akıllı telefonların adli bilişim bakımından incelenebilmesi mümkün olsa da yapılacak inceleme ve elde edilecek bulgular oldukça sınırlı olacaktır. Yapılan bir çalışmada (Boueiz, 2020), Android akıllı telefonların root yetkisini kazanmanın hedef cihazdan elde edilecek bulguları ne denli artıracağı belirtilmiş ve Android akıllı telefonların son sürümlerinin incelenebilmesi bağlamında bu cihazların root yetkisinin kazanılması sağlayacak araç ve yazılımların geliştirilmesi gerektiği açıklanmıştır.

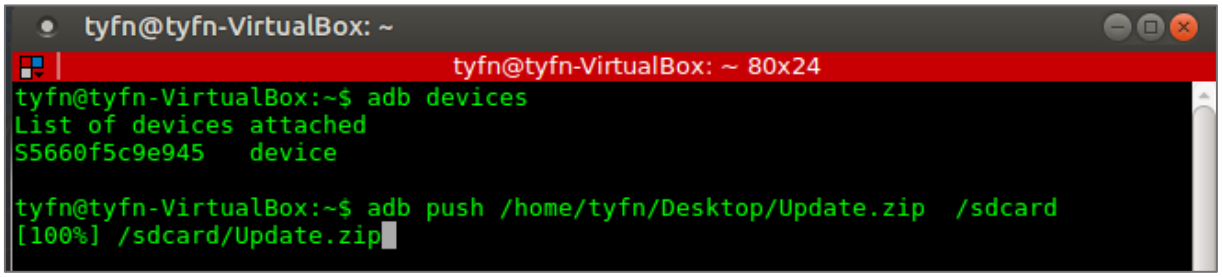
Root yetkisine sahip olunulmadan önemli kullanıcı verileri barındıran */data* ve */system* dizinlerine erişmek mümkün değildir. Root yetkisini kazanmak, Android cihazın

başlamasına engel olabilecek şekilde çökmesine, üretici garantisinin kaybedilmesine, güvenlik zaaflarına neden olabilir. Yine cihaz üzerindeki verilerin değişmesine de kaçınılmaz olarak sebep verir (Skulkin ve diğerleri, 2018: 62).

Ancak root yetkisinin kazanılması sırasında, salt sistem verisinin değiştirildiğini soruşturmayla ilgili olabilecek herhangi bir kullanıcı verisinin değiştirilmediği raporlanarak hedef cihazda yapılan değişiklik yasal zemine oturtulabilir. Root yetkisini kazanmadan hedef cihazın incelenmesi halinde, soruşturmaya katkı sağlayabilecek birçok veriden mahrum kalınacaktır. Fakat Android 5 veya üzeri sürüme sahip akıllı telefonların root yektisinin kazanabilmesi bootloader sisteminin kilidinin açılması ve bootloader sisteminin değiştirilmesi suretiyle gerçekleştirilebilmektedir. Bazı Android akıllı telefonların "*fastboot oem unlock"* komutuyla bootloader kilidi açılabilir. Ancak bootloader kilidinin açılabilmesi için akıllı telefon üzerinde bulunan tüm verilerin silinmesi gerekmektedir (Skulkin ve diğerleri, 2018: 66).

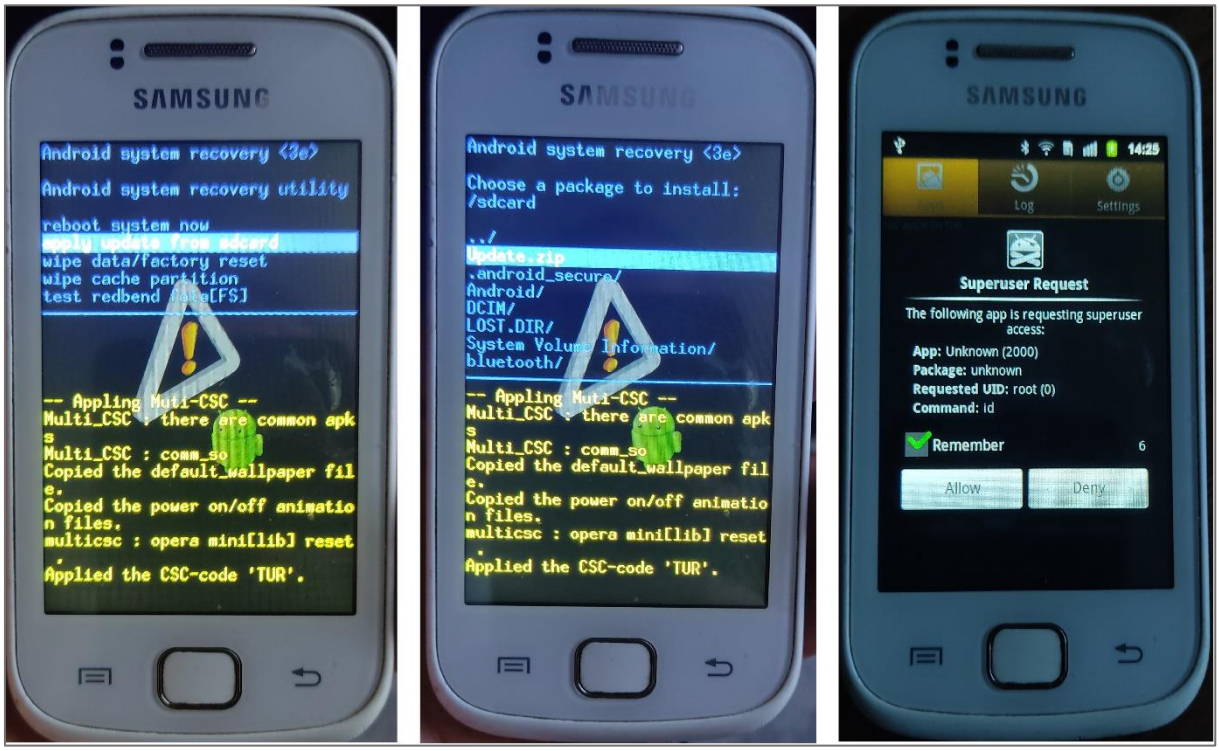
Dolayısıyla bootloader kilidi açık olmayan akıllı telefonlarda, daha farklı bir güvenlik açığının bulunması suretiyle root yetkisi kazanılmaya çalışılmalıdır. Bu da mümkün değilse bootloader kilidinin açılarak root yetkisinin kazanılması efektif bir çözüm olmayıp bu cihazlarda root yetkisi kazanılmadan sınırlı adli bilişim incelemeleri yapılması gerekmektedir.

Root yetkisini kazanma yöntemi, incelenen Android cihazın modeline veya sürüme göre değişebilmektedir. Android 2.3.3. sürümünde çalışan Samsung Galaxy Gio GT- s5660 cihazının root yetkisi kazanmak için cihazın USB hata ayıklama özelliği aktif hale getirilmiş, cihaz bilgisayar çalışma istasyonuna bağlanılmış, Resim 5.1'deki biçimde *"adb push 'Update.zip isimli dosyanın çalışma istasyonun bulunduğu dizin' /sdcard"* biçimdeki komut satırıyla Update.zip isimli dosya cihazın SD kartına aktarılmıştır.



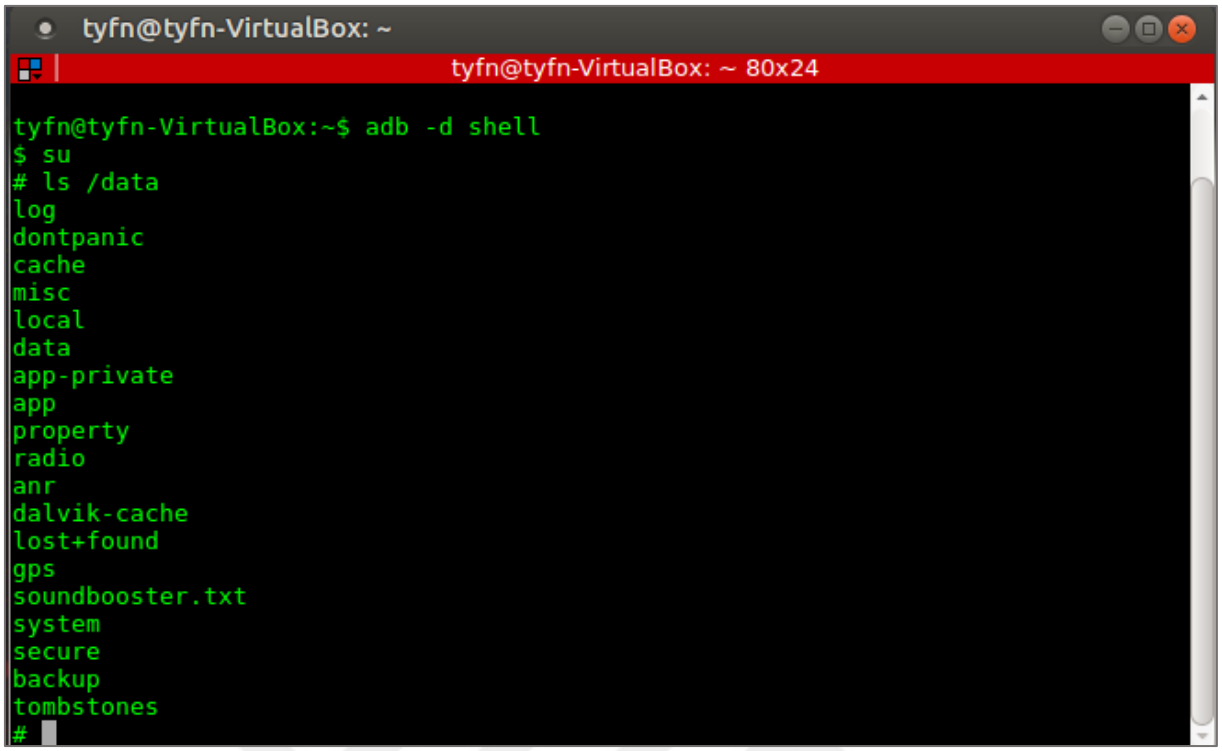
Resim 5. 1. Root yetkisini kazanmayı sağlamaya yarar dosyanın cihaza aktarılması

Daha sonrasında Resim 5.2'de gösterildiği gibi cihazın bootloader kısmına girilerek Update.zip isimli dosya ile cihazın güncelleştirilmesi gerçekleştirilmiştir (Akgül, 2014). Cihaz tekrar başlatıldığında superuser isimli uygulamanın cihaza yüklendiği gözlemlenmiştir. Superuser isimli uygulamaya girilerek ilgili modüllerin yüklenmesiyle cihazın root yetkisinin kazanılması mümkün olmuştur.



Resim 5. 2. Hedef cihazın root yetkisinin kazanılması

Akabinde Resim 5.3'de gösterildiği gibi çalışma istasyonundaki bilgisayardan *"adb shell"* komutu girildikten sonra *"su"* komutu girilmiş daha sonrasında superuser isimli uygulamadan telefona gelen bildirimde root yetkisinin kullanılmasına izin verilmiştir. "*ls /data"* komutunun yazılmasıyla cihazın */data* klasörüne ulaşılabildiği görülmüş, böylelikle root yetkisinin başarılı bir şekilde kazanıldığı anlaşılmıştır. Nitekim root yetkisine sahip olmadan */data* dizinine ulaşmak mümkün değildir. Yine hedef cihazın terminaline bağlanıldığında *"#"* ibaresinin meydana gelmesi de root yetkisinin kazanıldığını göstermektedir. Root yetkisi bulunmazken terminalde *"$"* ibaresi gözükecektir.



Resim 5. 3. Hedef cihazın root yetkisinin kazanılıp kazanılmadığının kontrolü

5.3.1.2. Cihaza Doğrudan Elle Müdahaleyle Veri Elde Edilmesi

Doğrudan cihazdan veri elde etme, cihaz çalışır durumdayken cihazla direkt olarak elle etkileşime geçerek cihazdan veri elde edilmesidir. Bu yöntem adli bilişim açısından uygun bir yöntem olmayıp zorunlu olmadıkça tercih edilmemesi gereklidir. Nitekim cihazla doğrudan temas halinde olunduğundan cihazdaki veriler kolaylıkla değiştirilebilir veya veri kaybı yaşanabilir.

Elle cihazdan veri elde etme yöntemi için Fernico ZRT, eDEC Eclipse veya Project-a- Phone gibi araçlar kullanılabilir. Nitekim Resim 5.4'te görüldüğü gibi araç, bir çanta içerisinde pratik olarak taşınabilmekte ve inceleme işlemi yapılırken ses ve görüntü kaydının etkili bir şekilde alınmasını sağlamak amacıyla tasarlanmıştır (Bijoy Boban, 2014).

Resim 5. 4. Eclipse 3 Pro Kit ekipman çantası ve kullanımı (*Eclipse 3 Pro Kit*, 2022)

5.3.1.3. Mantıksal İmaj Alınması

Mantıksal imaj, cihazın harici disk hafızasında ayrılmış alanlar üzerindeki dizinler ve dosyaların elde edilmesidir. Mantıksal imajda sadece ayrılmış dolayısıyla dizin ve dosyalardan oluşan bölüm elde edileceğinden kullanıcı tarafından silinmiş olan verilerin elde edilmesinin imkanı bulunmayacaktır.

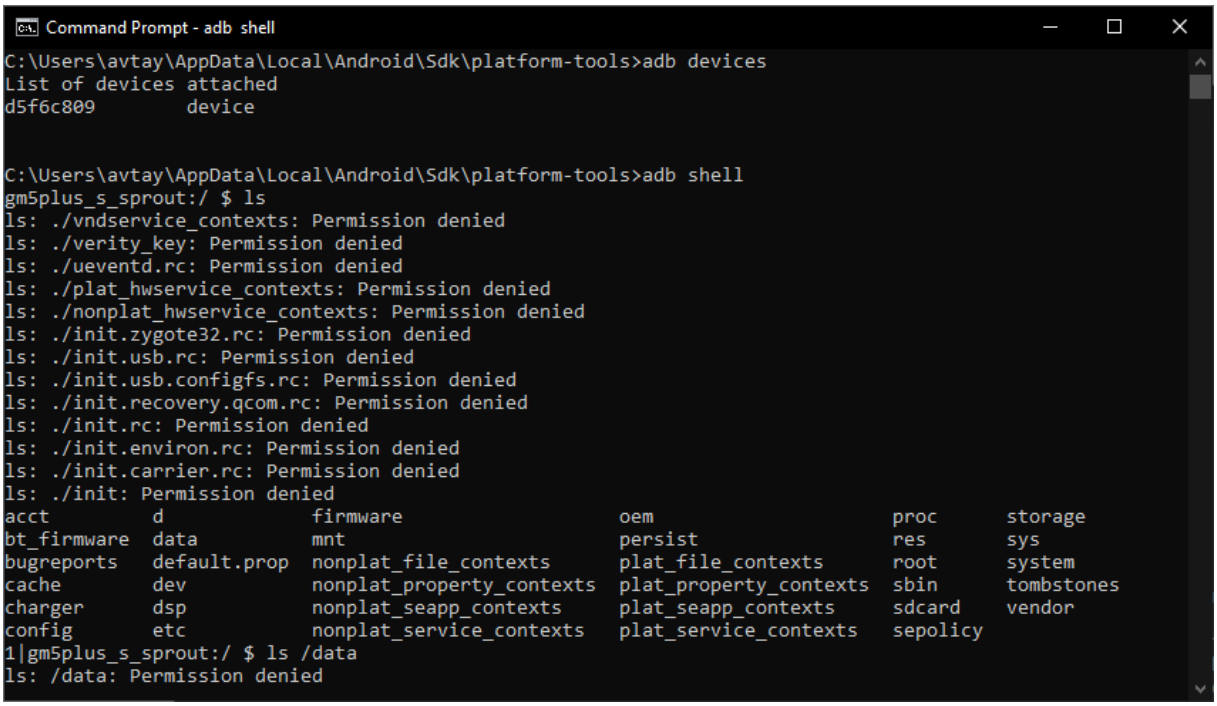
5.3.1.3.1. Android Debug Bridge Vasıtasıyla

Android Debug Bridge (ADB) sistemi; istemci, arka plan programı (Daemon) ve sunucu olmak üzere üç unsurdan oluşmaktadır. İstemci çalışma istasyonundaki bilgisayarda çalışır ve cihaza komutları gönderir. Daemon, Android akıllı telefonun arka planında çalışarak kendisine istemcinin göndermiş olduğu komutları uygular. Sunucu ise, Daemon ve istemci arasındaki iletişimi sağlar. Root yetkisine sahip olunmayan cihaz verilerin bir uygulama yahut ADB komutları vasıtasıyla yedeğinin alınması veya content providers'tan sağlanan bilgiler vasıtasıyla veri elde edilmesi mümkündür (Lin, 2018: 344).

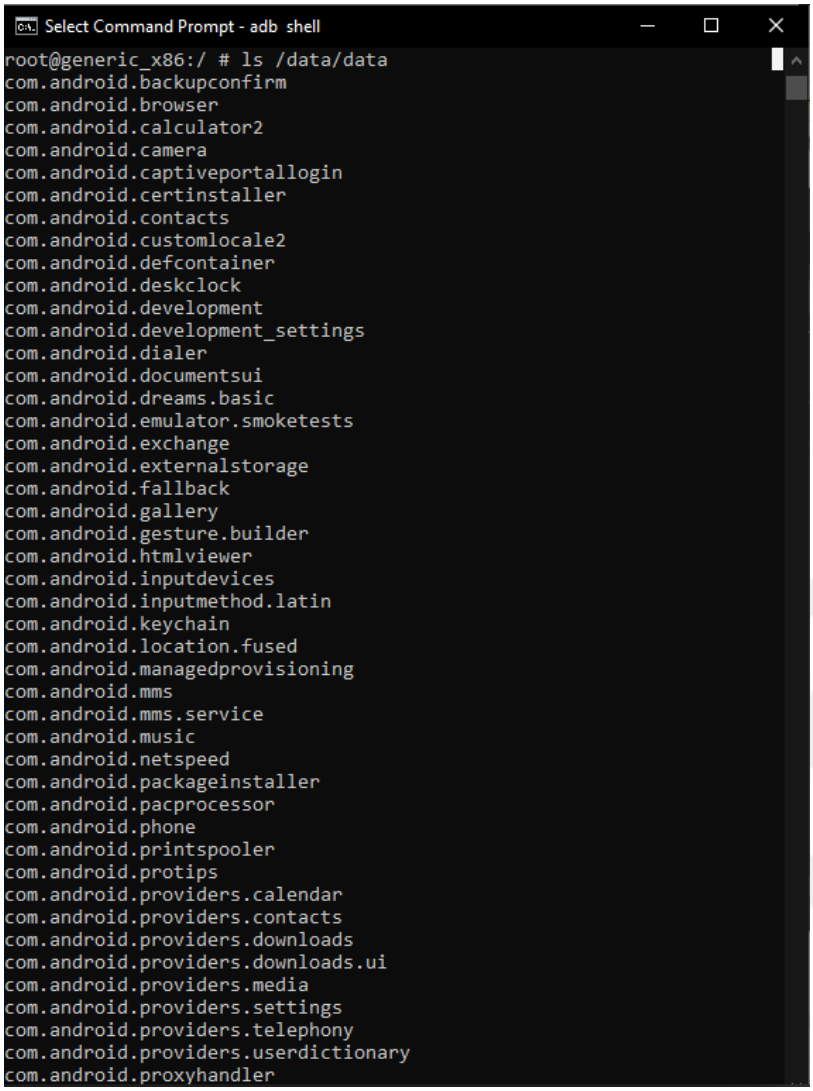
Android Debug Bridge (ADB) komutlarıyla Android akıllı telefonun mantıksal imajının alınması gerçekleştirilebilir. Ancak bu komutların uygulanabilmesi için hedef cihazın USB debug modu açık olmalıdır. Aksi halde ADB komutları çalışmayacaktır. Hedef akıllı telefondan, çalışma istasyonu bilgisayarına veri aktarımı yapmak için *"adb pull"* komut satırının kullanılması gerekmektedir. Bu bağlamda, *"adb pull 'akıllı telefonun hedef dizin adresi' 'çalışma istasyonun hedef dizin adresi'"* komutuyla akıllı telefondan veri elde

edinilmek istenen dizin adresi ve bu verilerin aktarılacağı çalışma istasyonu dizin adresinin belirlenmesiyle ilgili komut çalıştırılabilecektir.

Soruşturma açısından önem arz edebilecek birçok verinin */data* ve */system* dizinlerinde bulunduğu söylenebilir. Nitekim akıllı telefonda kullanılan uygulamaların kullanıcı verileri */data* dizine kaydedilmektedir. Ancak bu dizinlerden ADB komutlarıyla verilerin elde edilebilmesi için cihazın root yetkisinin kazanılmış olması gereklidir. Resim 5.5'te gösterildiği gibi root yetkisi kazanılmadan, bu dizinlere erişim izni elde edilemeyecektir.



Resim 5. 5. Root yetkisi bulunmayan cihazın birçok dizine erişimi reddetmesi



Resim 5. 6. Root yetkisi kazanılmış bir hedef cihazın */data/data* dizininin görüntülenmesi

Resim 5.6'daki gibi root yetkisi kazanılmış bir cihazın */data/data* dizinindeki klasör ve dosyalar, *"adb pull /data/data 'çalışma istasyonundaki bilgisayarda dosyaların kopyalanması arzu edilen dizin adresi'"* komutuyla çalışma istasyonu bilgisayarına kopyalanabilir. Komutta çalışma istasyonuna kopyalanmak istenilen dizinin belirtilmemesi halinde dosya ve klasörler, çalışma istasyonunda Android SDK araçlarının yüklü olduğu platform-tools klasörünün içine doğrudan kopyalanacaktır.

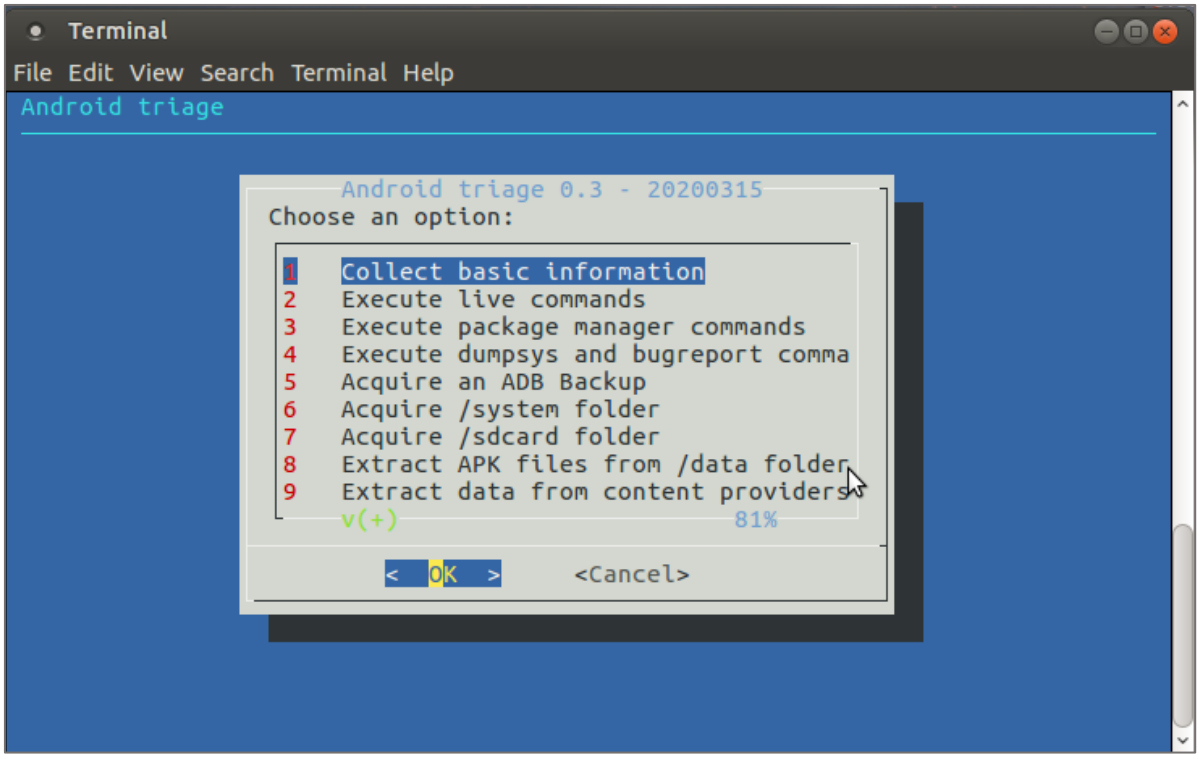
Böylelikle cihazın kısmen veya tamamen mantıksal imajı alınabilecektir. Bu şekilde elde edilen klasör ve dosyalar, mantıksal imaj niteliğinde olduğundan bu klasörlerde bulunan silinmiş verilerin kurtarılması mümkün olmayacaktır.

5.3.1.3.2. Android Triage İsimli Yazılım Aracıyla

Açık kaynak kodlu Android Triage isimli araç ile Android akıllı telefonların mantıksal imajını almak mümkündür (RealityNet, 2022). Bu aracın kullanılabilmesi için Android akıllı telefonun root yetkisine sahip olmak zorunlu değildir. Ancak root yetkisine sahip olunması halinde elde edilebilecek veriler, çok daha fazla olacaktır. Nitekim root yetkisine sahip olunulmadan */system* ve */data* dizininden elde edilecek veriler oldukça sınırlı düzeyde kalacaktır. Buna karşılık özellikle Android sistemindeki içerik sunucuları (content providers) adli bilişim bakımından oldukça yararlı veriler elde etmek mümkündür. Zira veri sağlayıcılardan işletim sisteminde kurulu bulunan tarayıcı internet sitesi geçmişi, yer imleri; telefon defterine kayıtlı kişilerin numaraları, adresleri, e-postaları, silinen kişi sayısı; takvime kayıtlı etkinlikler; cihaza indirilen dosyaların listesi; bluetooth cihazları vb. birçok bilgiye ulaşmak mümkün olmaktadır.

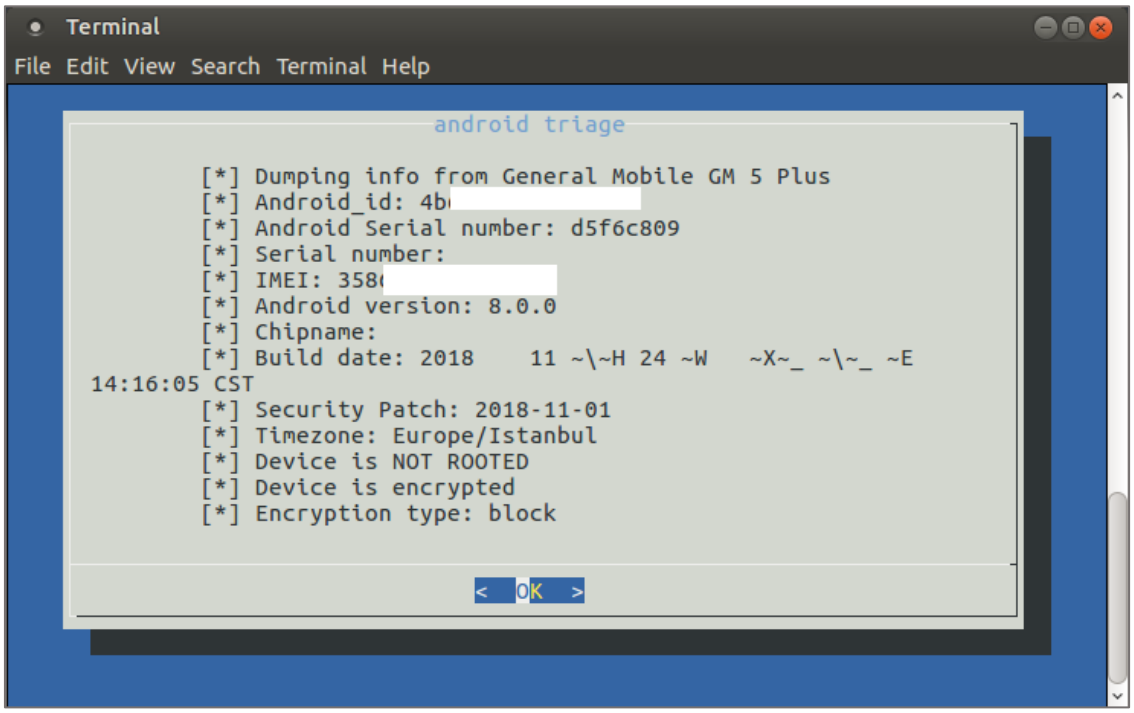
Bu nedenle root yetkisine sahip olunamayan cihazlardan sınırlı olsa da veri elde etmek için Android Triage isimli programın kullanılması yararlı olacaktır.

Android Triage, ADB komutlarını kullanarak çalışmaktadır. Birçok ADB komutunu, hızlı bir şekilde uyguladığı için cihazın tam mantıksal imajını almak açısından oldukça yararlıdır. Resim 5.7'de araç açıldığında kullanıcıya gösterilen arayüz sunulmuştur.



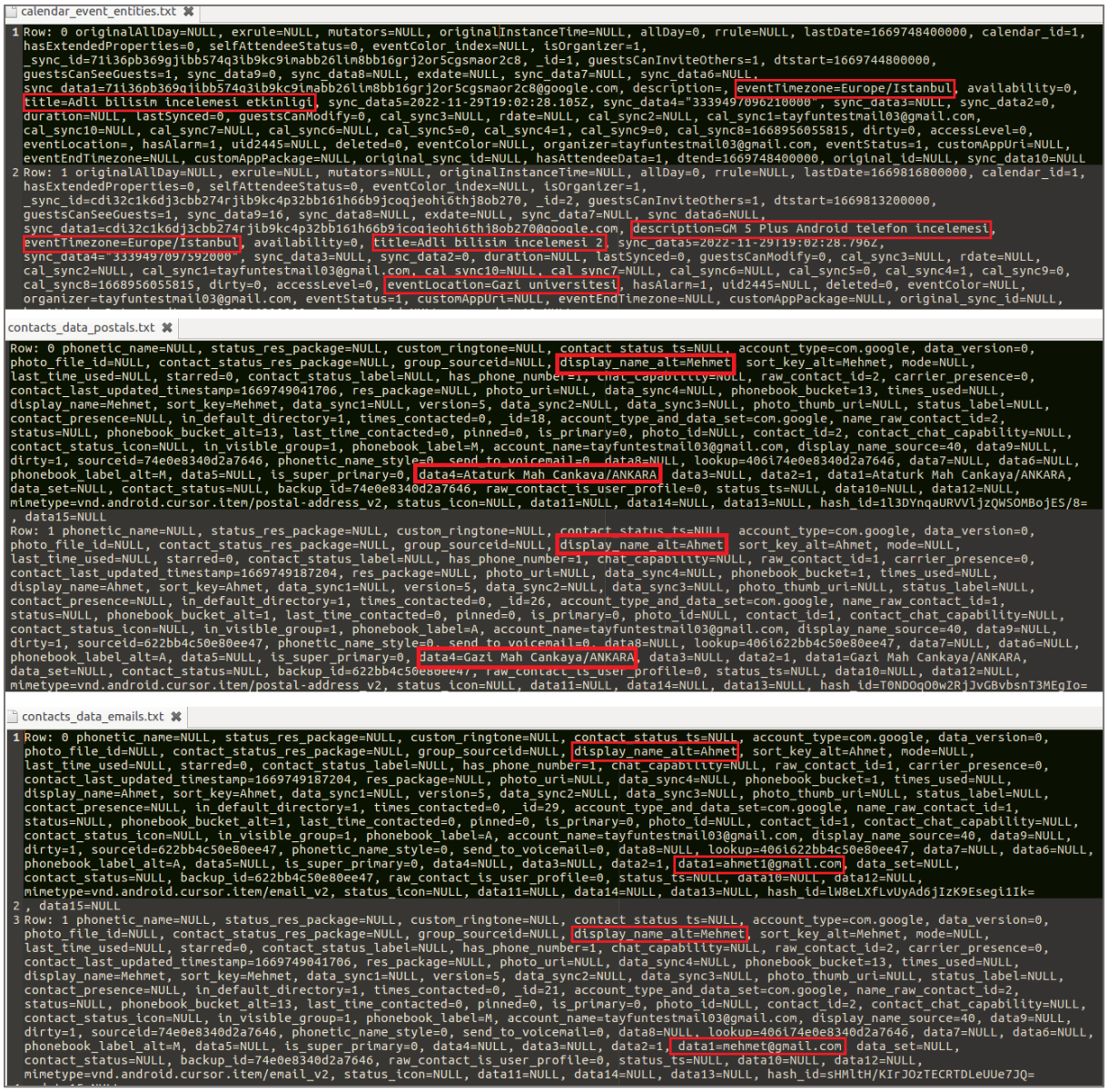
Resim 5. 7. Android Triage isimli uygulamanın arayüzü

1 numaralı *"Collect basic information"* seçeneğinin seçilmesiyle Android 8.0.0 sürümlü General Mobile GM 5 Plus cihazına ilişkin Resim 5.8'deki gibi genel bilgiler edinilmiştir. Buradaki elde edilen android_id numarasıyla araç çalışma istasyonundaki bilgisayarda bir klasör oluşturacaktır. Devam eden seçenekler vasıtasıyla elde edilen veriler bu klasör içerisinde saklanacaktır.

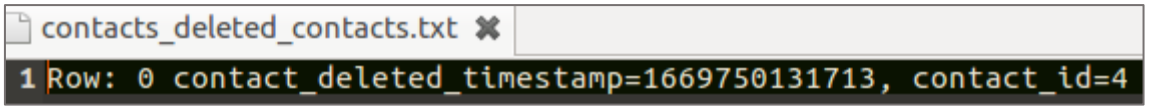


Resim 5. 8. Cihaz hakkında edinilen genel bilgiler

Yine root yetkisini bulunmayan mezkur cihazdan içerik sunucuları (content providers) vasıtasıyla elde edilen takvime kayıtlı etkinlikler, adres defterinden elde edilen kişiler ve bu kişilerin açık adresleri ve e-posta adresleri bilgileri Resim 5.9'ta ve cihazdan silinen kişi sayısı ve silinme zamanları hakkında edinilen bilgi ise Resim 5.10'da gösterilmiştir. Resim 5.10'dan anlaşılacağı üzere hedef cihaza kaydedilen dördüncü kişi, Unix zaman damgasının çözülmesiyle ulaşılan 29.11.2022 tarihi 10:28 saatinde silinmiştir.



Resim 5. 9. Content providers vasıtasıyla sırasıyla takvime kayıtlı etkinliklerin; telefon defterine kayıtlı kişilerin adresleri, e-posta bilgileri vb. elde edilmesi

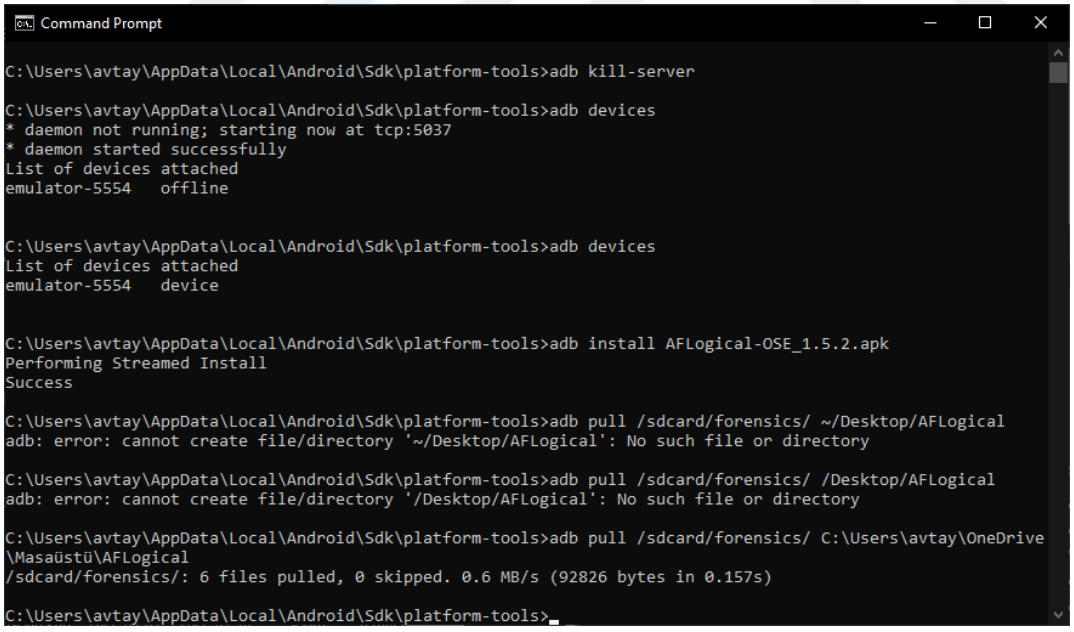


Resim 5. 10. Content providers vasıtasıyla telefon defterinden silinen kişi sayısı ve silinme zamanının elde edilmesi

5.3.1.3.3. AF Logical OS İsimli Uygulamayla

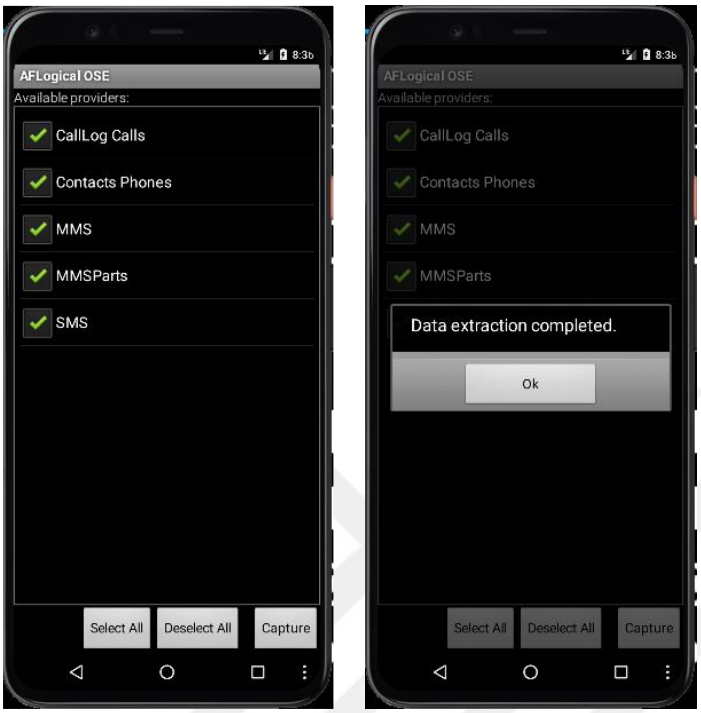
AF Logical OSE isimli uygulama ile Android telefondaki yapılan çağrılar, çağrıların süreleri, çağrıların kime yapıldığı veya kimden alındığı, SMS ve MMS mesajların kime

gönderilip alındığı ile içerikleri ve cihaza kayıtlı kişilerin elde edilmesi mümkündür. Bu uygulamayı kullanabilmek için cihazın root yetkilerine sahip olmak zorunlu değildir. Cihaza AF Logical OSE isimli apk dosyası yüklenmelidir. Bunun için *"adb install AFLogical-OSE.apk"* biçimindeki komut satırı kullanılabilir. Yüklenecek bu uygulamanın *platform tools* isimli dizinde olması halinde, doğrudan belirtildiği şekilde komut satırının sonuna uygulamanın isminin girilmesiyle uygulama hedef cihaza yüklenebilir. Uygulamanın farklı bir dizinde bulunması halinde uygulamanın bulunduğu dizinle beraber uygulamanın komut satırının sonunda belirtilmesi gerekmektedir. Daha sonrasında uygulama açılarak edinilmek istenilen bilgiler seçilerek *"Capture"* butonuna basılmalıdır. Akabinde cihaza takılı SD kartta forensics isimli klasör içerisinde cihazdan elde edilen bilgiler csv dosyası biçimde oluşturulacaktır. Bu csv dosyası */sdcard/forensics* dizininde oluşturulacaktır. Bu dosyanın inceleme istasyonuna çekilmesi için *"adb pull /sdcard/forensics/ 'csv dosyasının çekilmesi arzu edilen çalışma istasyonu bilgisayarı dizininin adresi'"* şeklindeki komut satırı kullanılabilir. Resim 5.11'de cihaza AF Logical OSE isimli uygulamayı yüklemek ve adli bilişim çalışma istasyonuna elde edilen veriler çekmek için gerekli olan adb komut satırları gösterilmiştir.



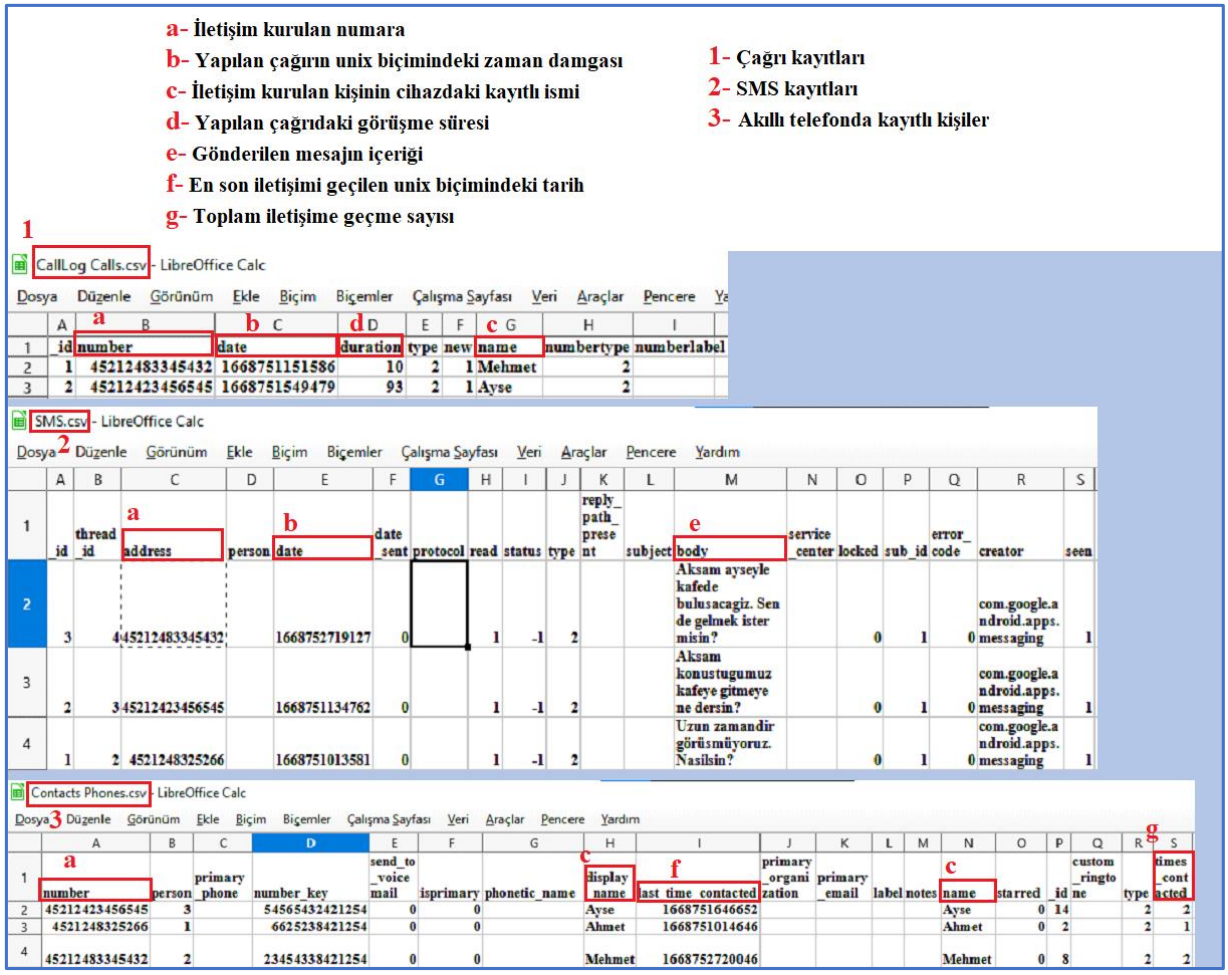
Resim 5. 11. Cihaza AF Logical OS isimli dosyanın yüklenmesi ve cihazdan elde edilen bilgilerin adli bilişim çalışma istasyonuna çekilmesi için gerekli kod satırları

Resim 5.12’de ise cihaza yüklenen uygulamayı çalıştırınca adli bilişim uzmanının karşılaşacağı ekran ve “Capture” seçeneğine bastıktan verilerin SD karta aktarılmasının tamamlandığına ilişkin uyarı veren ekran gösterilmiştir.



Resim 5. 12. Apk uygulaması yüklendikten sonra hedef cihazda uygulamanın kullanılması suretiyle SD Kart üzerinde çağrı, SMS, MMS, kişi kayıtları verilerinin oluşturulması

Resim 5.13’te elde edilen csv dosyaların içeriği sunulmuştur. Belirtilen bu resimlerde, Android Studio AVD Yöneticisi vasıtasıyla oluşturulan bir sanal akıllı telefonla bu uygulamanın nasıl yüklendiğiyle sanal akıllı telefondan elde edilen veriler gösterilmiştir.



Resim 5. 13. Cihazdan csv dosyası biçiminde elde edilen sırasıyla çağrı kayıtları, SMS ve kişi bilgilerinin görüntülenmesi

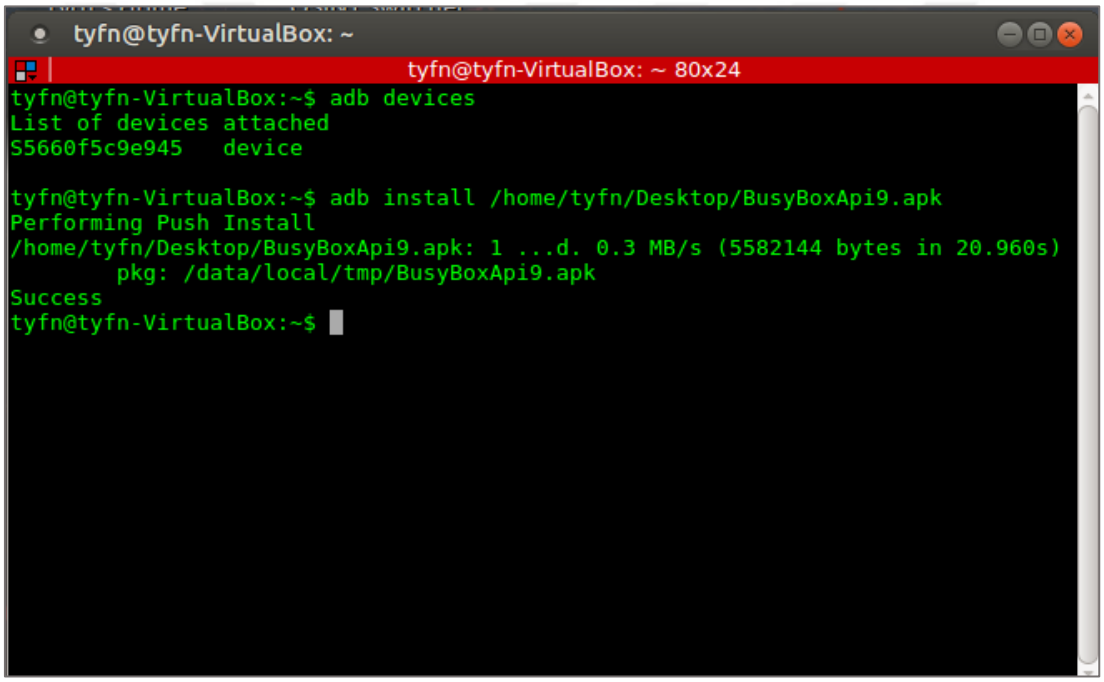
5.3.1.4. Fiziksel İmaj Alınması

Fiziksel imaj, cihazdaki disk hafızasının ayrılmış veya ayrılmamış, anlamlı veya anlamsız tüm alanlarının birebir kopyasının elde edilmesidir. Tüm diskin birebir kopyasının alınması sebebiyle cihazdan kullanıcı tarafından silinmiş verilerin elde edilmesi mümkündür. Zira silinmiş verilerin diskte bulunduğu alanın üzerine yeni bir veri yazılmadıysa, silinen veri diskte daha önceden bulunduğu alanda saklanmaya devam etmektedir.

5.3.1.4.1. DD Komutlarının Vasıtasıyla

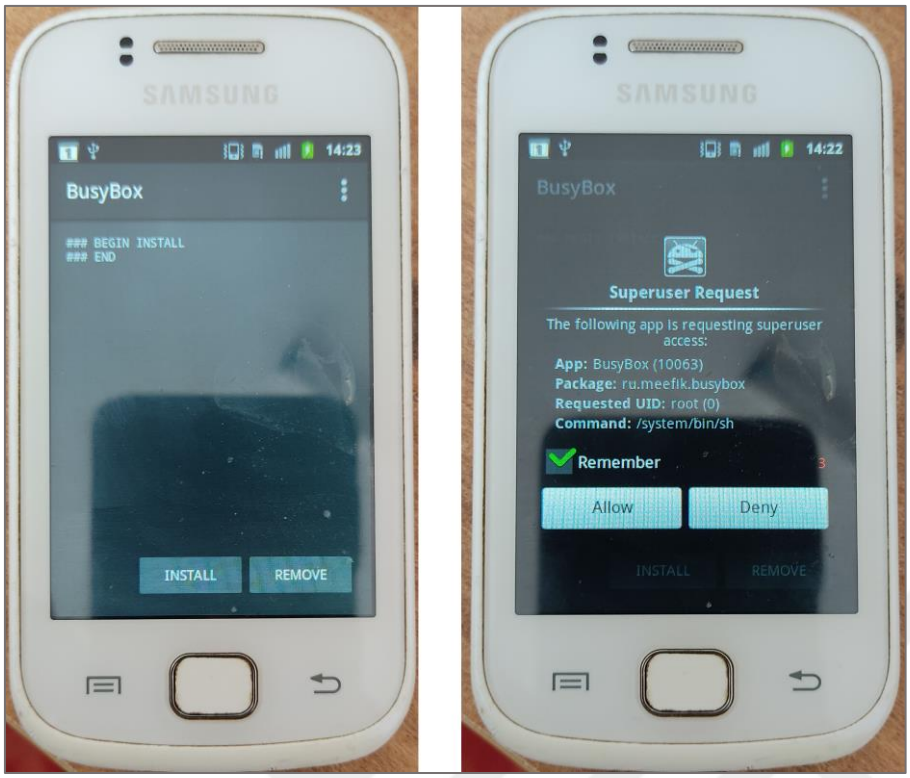
Android akıllı telefonların fiziksel imajının alınabilmesi için root yetkisine sahip olmak gerekmektedir. Aksi halde sadece mantıksal imajın alınması mümkün olur ve cihazdan silinmiş olan dosyaların incelenebilmesi mümkün olmaz.

Root yetkisini kazandıktan sonra, cihazın sürümüne uygun olan BusyBox.apk isimli uygulamanın yüklenmesi gerekmektedir. Cihaza bu uygulamanın yüklenmesi ADB kullanılarak gerçekleştirilebilir. Bilgisayar inceleme istasyonunda, Platform tools isimli klasörün yüklü olduğu dizine, bu uygulamanın kopyalanmasıyla beraber ADB komutlarının kullanılmasıyla cihaza uygulamanın yüklenmesi gerçekleştirilebilir. Bu bağlamda, istasyon ile bilgisayar arasında ADB bağlantısı başarılı bir şekilde sağlandıktan sonra Resim 5.14'teki gibi *"adb install BusyBox.apk"* komut satırıyla beraber uygulama cihaza yüklenebilir. BusyBox.apk isimli uygulama dosyasının platform tools isimli klasörde bulunması halinde mezkur komut satırı çalışacaktır. Aşağıdaki resimlerde, Android 2.3.3. sürümlü Samsung Galaxy Gio GT- s5660 cihazının fiziksel imajının alınması aşamaları gösterilmiştir.



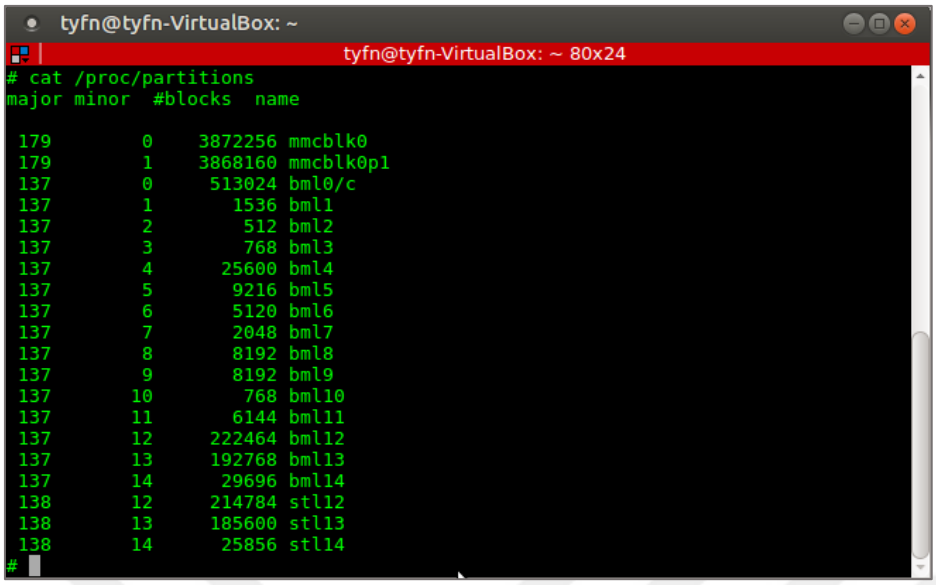
Resim 5. 14. BusyBox uygulamasının ADB vasıtasıyla hedef cihaza yüklenmesi

Eğer uygulama dosyası farklı bir dizinde bulunmaktaysa, komut satırının sonuna uygulamanın isminin doğrudan yazılması yerine ilgili dizinle beraber uygulamanın belirtilmesi gerekmektedir. Daha sonrasında Resim 5.15'te gösterildiği gibi cihazda uygulama açılarak "install" seçeneği seçilmelidir. Uygulama root yetkilerini kullanmak isteyecektir. Root yetkisi kazanılmamış bir cihazda uygulamanın başarılı bir şekilde çalışması mümkün değildir.



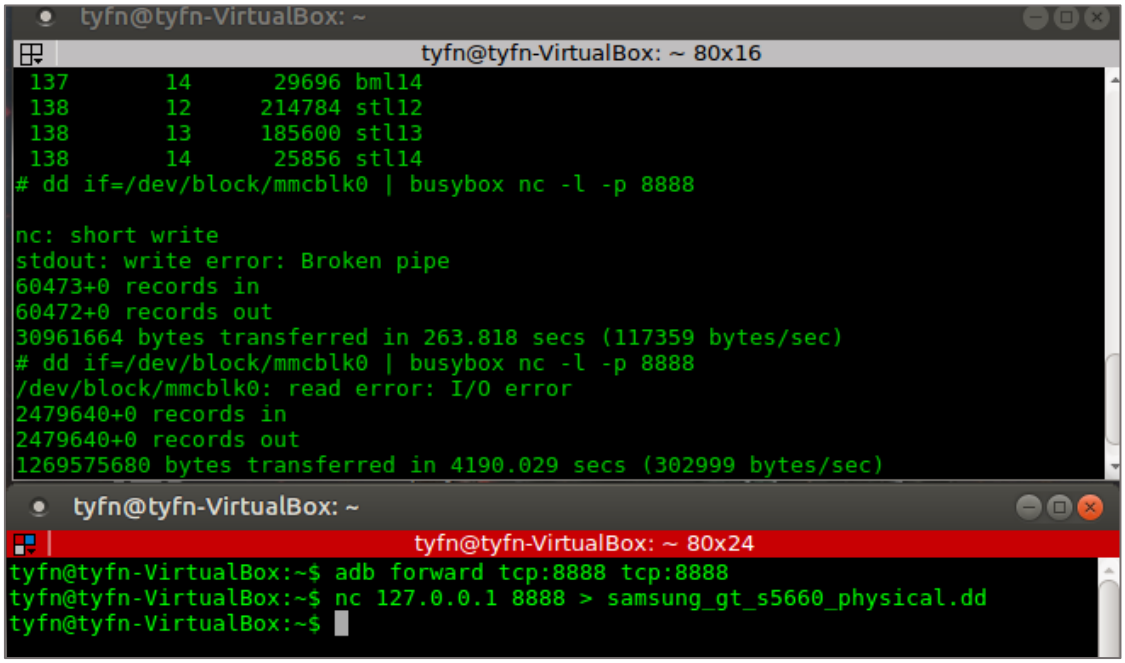
Resim 5. 15. Busybox isimli uygulamanın bileşenlerin root yetkisiyle yüklenmesi

Daha sonrasında *"adb forward tcp:8888 tcp:8888"* komutuyla disk imajının aktarımı yapılacak portun belirlenmesi gerekmektedir. Akabinde farklı bir terminal açılarak yine cihazla adb bağlantısı kurulup *"adb shell"* komutuyla cihazın kontrolüne sağlanıp su komutunu girerek cihazın root yetkilerine sahip olmak gerekmektedir. Bu sırada *"ls /data"* komut satırının girilmesiyle cihazın root yetkilerine sahip olunup olunmadığının kontrolü sağlanabilir. Root yetkilerine sahip olunduğuna emin olduktan sonra Resim 5.16'daki gibi *"cat /proc/partitions"* komutu yazılarak disk blokları gözlemlenebilir. Bu komutun girilmesi üzerine "mmcblk0" bloğunun en büyük bloğu oluşturduğu ve bu disk bloğuyla diskin fiziksel imajının alınabileceği anlaşılabilecektir.



Resim 5. 16. *"cat proc/partitions"* komutuyla cihaz disk bloklarının görüntülenmesi

Devamında *"dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888"* komut satırının girilmesi gerekmektedir. Sonrasında ise bir önceki terminale *"nc 127.0.0.1 8888 > 'oluşturulacak dd dosyası türündeki disk imajının ismi'"* komut satırının girilmesi gerekmektedir. Bu halde ilgili dosya adb araçlarının bulunduğu klasöre belirlenen isimle oluşturulmaya başlanacaktır. Belirtilen *"nc 127.0.0.1 8888 > 'oluşturulacak dd dosyası türündeki disk imajının ismi'"* komutu tamamlanıp terminalin bir alt satıra geçmesiyle birlikte fiziksel imajının alınması işlemi tamamlanmış olacaktır. Bu komutların uygulanması Resim 5.17'te gösterilmiştir.



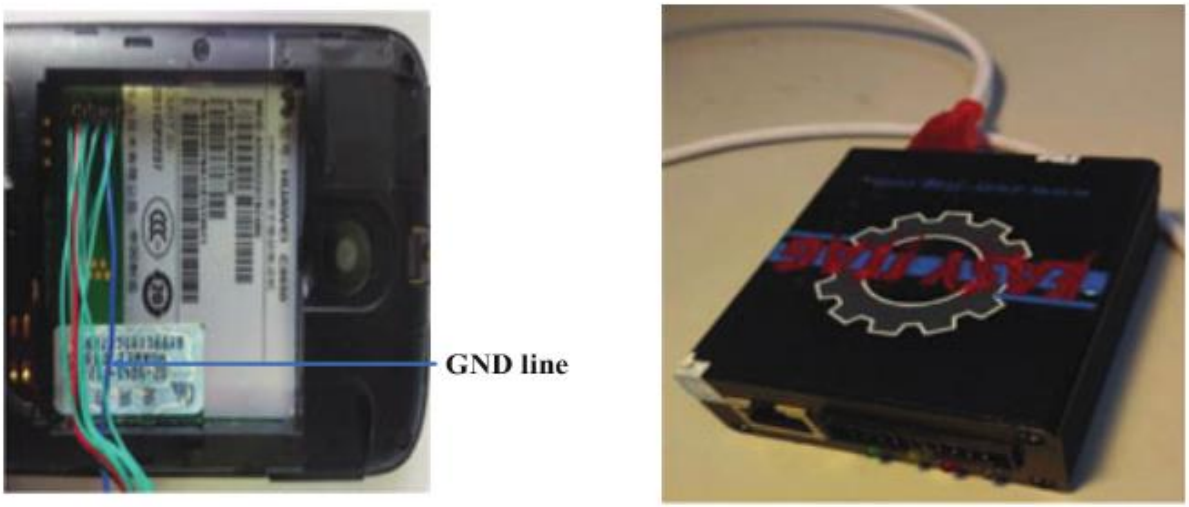
Resim 5. 17. Üst taraftaki terminal: hedef cihazın komut istemcisindeki girilen komutlar, alt taraftaki terminal: çalışma istasyonundaki bilgisayar terminalinde girilen komutlar

5.3.1.4.2. JTAG Yöntemiyle Fiziksel İmaj Alınması

JTAG yöntemi ise, JTAG kutusu ile cihazın anakartına bağlantı sağlanıp cihaz üzerindeki CPU işlemcilerinden yararlanmak suretiyle imajının alınmasıdır (Lin, 2018: 342). JTAG yöntemiyle USB debug modunun etkinleştirilmediği durumlarda, cihazın imajının alınması mümkündür. JTAG ile imaj alınması ise, cihaz üzerindeki JTAG portları üzerinden kablo yardımıyla cihazın fiziksel imajının alınmasıdır. Özelleştirilmiş Bootloader sisteminin yüklenmesi ve dosya sistemlerinin yeniden oluşturulmasının gerekli olabilmesi ihtimalleri nedeniyle JTAG yoluyla imaj alacak görevlilerin uygun bir şekilde eğitilmesi ve geniş teknik uzmanlar ile işlemlerin gerçekleştirilmesi ehemmiyetlidir (Rick ve diğerleri, 2014). Resim 5.18 ila 5.20 arasında telefonun JTAG giriş uçları, JTAG kablosu ve akıllı telefonla JTAG kutusu arasında JTAG bağlantısının sağlanılması gösterilmiştir.

Resim 5. 18. JTAG giriş uçları (Androulidakis, 2012: 75-99)

Resim 5. 19. JTAG kablosu (Androulidakis, 2012: 75-99)



Resim 5. 20. JTAG kablosu ile JTAG kutusuna akıllı telefonun bağlanması (Lin, 2018: 342)

5.3.1.4.3. Çip Çıkarımı (Chip-Off) Yöntemiyle İmaj Alınması

Chip-off yöntemi, NAND flaş çiplerinin anakarttan sökülüp bu çiplerin farklı bir donanımla etkileşimiyle cihazın imajının alınmasıdır. Bu yöntem bazı güçlükleri de barındırmaktadır. Nitekim bu çiplerin sökülmesi sırasında anakart veya çiplere zarar verilebileceği gibi bu işlemin gerçekleştirilmesi de oldukça zaman alıcıdır. Bu nedenle hızlı bir soruşturma gerektiren durumlarda imaj almak için elverişli bir yöntem olmayabilir (Lin, 2018: 341).

Chip-off yöntemi, cihazın flash belleğinin fiziksel olarak cihazdan ayrılması ile uygulanır. Bu yöntem, ilgili flash belleğin wear-leveling algoritmasına tersine mühendislik uygulanmasıyla tümleşik ikili formattaki dosyaların oluşturulmasıdır (Rick ve diğerleri, 2014).

JTAG yöntemi ile cihaz üzerinde daha az modifikasyon yapıldığından Chip-off yöntemine nazaran cihaz donanımlarına zarar verilme ihtimali daha düşüktür. Ancak JTAG işleminin başarılı olabilmesi için cihaz üzerindeki işlemcinin zarar görmemiş, çalışır vaziyette bulunması gerekmektedir. Aksi halde bu yöntemle cihazdan veri elde edilmesi mümkün olmayacaktır. Chip-off yöntemiyle ise hedef cihaz üzerindeki işlemcinin zarara uğramış olması halinde dahi imajın alınması mümkündür. Cihazın ekranın kilitli olması veya root yetkilerinin bulunmaması durumlarında bile hedef cihazın imajının alınabilmesi ile alınan imajın fiziksel imaj niteliğinde olması, JTAG ve Chip-off yöntemlerinin avantajlarındandır. Nitekim fiziksel imaj ile mantıksal imaja göre, çok daha fazla soruşturmaya veya kovuşturmaya yararlı verilerin elde edilmesi mümkün olmaktadır (Lin, 2018: 343)

5.3.1.4.4. Geçici Belleğin (RAM) İmajının Alınması

Geçici bellekteki veriler, cihaz çalışmaktayken sürekli değişmekte olduğundan ilk olarak geçici belleğin imajının alınması daha sağlıklı olacaktır.

Android akıllı telefonlarda, geçici belleğin elde edilmesi oldukça güçtür. Nitekim geçici bellek imaji için kernel boyutunda işlemlerin yapılması gerekmektedir. Bu bağlamda LiMe, AMExtractor, PASM gibi araç veya yöntemler bulunmaktadır. LiMe için hedef cihazın linux çekirdek kaynak koduna ihtiyaç bulunmaktadır (504ENSICS Labs, 2014). Hedef cihazın linux çekirdek kaynak kodu, üreticisinin internet sitesinde bulunabilmektedir. Linux çekirdek kaynak koduyla beraber cihazın dosya sisteminin /proc dizininden "config.gz" isimli dosyanın elde edilip bu linux çekirdek kaynak kodu ile cihaz çekirdeğinin çapraz derlenmesi gerekmektedir. Daha sonrasında LiMe tarafından oluşturulan modülün, cihaza aktarılması suretiyle geçici bellek elde edinilebilir. Ancak her hedef cihaz için bu linux çekirdek koduna ulaşmak mümkün olmayabilir. Bu durum da LiMe isimli aracın etkinliğini azaltmaktadır .

AMExtracotor uygulamasının kullanılabilmesi için Linux çekirdek kaynak koduna gerek bulunmamaktadır. Sadece geçici belleğin çeşitli özelliklerinin öğrenilmesi ve bu özelliklerden yola çıkarak çekirdek modülünün oluşturulması ile modülle ilgili dosyanın cihaza aktarılması suretiyle geçici belleğin verisinin elde edilmesi mümkündür (Haiyu Yang, 2022). Bir çalışmada (Yang ve diğerleri, 2016), AMExtractor'ün LiMe'ye göre cihazların geçici belleğinin imajının alınmasında daha başarılı olduğu neticesine varılmıştır.

Yapılan farklı bir çalışmada ise (Feng ve diğerleri, 2019), PASM isimli yöntemle Root yetkisine gerek duyulmadan cihazın geçici belleğinin imajının alınmasının mümkün olduğu

belirtilmiştir. Yukarıda belirtilen iki aracın kullanılması sırasında cihazın root yetkisine sahip olunulması gerekmektedir. Bu yüzden root yetkisine sahip olunamayan cihazlar için PASM isimli yöntem etkili olabilecektir.

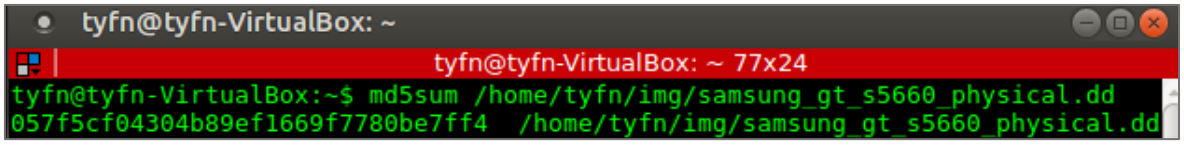
5.3.1.5. Mikro Okuma ile Veri Elde Edilmesi

Mikro okuma, elektron mikroskopu yardımıyla NAND ve NOR çiplerindeki kapılarının fiziksel görüntüsünün kaydedilmesidir. Oldukça zor bir yöntem olup ilgili araştırmanın çok ehemmiyetli olması ve diğer yöntemlerin yarar sağlamayacak olması halinde uygulanması gereklidir (Rick ve diğerleri, 2014). Nitekim bu yöntem veri elde edilmesi oldukça maliyetli ve zaman alıcı olacaktır.

5.4. Delillerin Muhafazası

Adli bilişimin önemli ilkelerinden birisi de kaynak veri ve elde edilen verinin doğruluğunun korunmasıdır. İlk durum hedef cihaz üzerinde yazma korumasının etkinleştirilmesi, son durum ise çıkarılan verinin hash değerlerinin alınmasıyla sağlanabilir. Nitekim yazma koruması ile hedef cihazda verilerin değiştirilmesi önlenecekken, hash değerlerinin alınmasıyla da alınan imajdaki verilerin değişime uğrayıp uğramadığı değerlendirilebilecektir. Zira alınan imajın tekrar tekrar adli bilişim aşamaları açısından incelenmesi yahut analiz edilmesi söz konusu olabilecektir (Rick ve diğerleri, 2014).

Örneğin 5.3.1.3.1. numaralı “DD Komutları Vasıtasıyla” isimli başlıkta belirtildiği şekilde akıllı telefonun fiziksel imajı alındıktan sonra Resim 5.21’deki gibi *“md5sum”* komutuyla imaj dosyasının hash değerini almak mümkün olmuştur.



Resim 5. 21. *“md5sum”* komutuyla imaj dosyasının hash değerinin belirlenmesi

Ancak hedef cihazdan fiziksel imaj alma işlemlerinin farklı zamanlarda uygulanması halinde, elde edilen imaj verilerin hash değerleri birbirinden farklı olabilecektir. Çünkü cihaz sürekli etkin olduğundan ve cihaz saati sürekli değiştiğinden dolayı elde edilen imaj küçük de olsa farklı olabilecek ve bu durum tamamen farklı hash değerlerinin oluşmasına sebep verebilecektir (Rick ve diğerleri, 2014).

Root yetkisi kazanmak için cihazın sistem dosyalarında değişiklikler gerçekleştirilmektedir. Root yetkisinin kazanılması gerekip gerekmediği, her somut olay açısından kazanılması düşünülen fayda ile temel hak ve özgürlükler arasında denge gözetilerek değerlendirilmelidir. Root yetkisini kazanılması gerekmesi halinde, sistem dosyalarında en az değişiklik ile yetki kazanılmaya çalışılmalı ve kullanıcı verilerine zarar verilmemelidir. Root işlemini geri alarak cihazı eski haline getirmenin mümkün olacağı şekilde root yetkisi kazanılmalıdır (Akarawita ve diğerleri, 2015).

"Delillerin Toplanması ve İmaj Alınması" Başlığında belirtildiği şekilde cihazın dışarıyla ağ veya operatör bağlantısı keserek yeni verilerin cihaza girişini önlemek, delillerin muhafazası için ehemmiyetlidir. Delillerin muhafazası aşaması aslen, sadece delillerin toplanması ve imaj alınmasından itibaren başlamayıp tüm adli bilişim süreçlerinde uygulanması gereken tedbirleri barındırmaktadır. Buna ilişkin detaylı açıklamalar, "Android Akıllı Telefonların Tanımlanması" ve "Delillerin Toplanması ve İmaj Alınması" başlıklarında yapılmıştır.

5.5. Delillerin Analizi

Bazı yazısal içerikli telefon numaraları, adres defterleri, e-posta veya SMS şeklindeki dosyalar telefon üreticilerine özgü sahiplikteki, yaygın olmayan dosya türleri içerisinde saklanabilir (Lutes & Mislan, 2008). Bu durum da hedef dosya türünün analiz işlemlerinin yapılmasını zorlaştırılabilir.

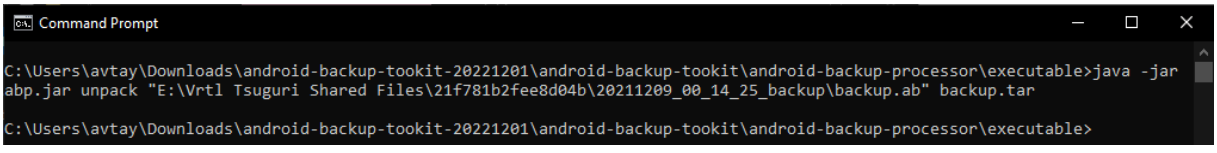
Fail kullanmış olduğu telefona gerçeğe aykırı yapay verileri yüklemesi suretiyle kendisini suçtan aklamaya ya da çeşitli kötü amaçlı yazılımlarla verilerin ele geçirilmesi önlemeye çalışabilir. Yine karine olarak telefonun sahibinin telefon üzerinde yapılan işlemleri gerçekleştirildiği kabul edilse de ilgili akıllı telefonu sahibinden farklı bir kişinin kullanmış olması da mümkündür (Androulidakis, 2012: 75-99).

Yapılan bir çalışmada (Mirza ve diğerleri, 2020), WhatsApp üzerinden gönderilen özellikle tehdit ve şantaj içerikli mesajların herkesten sil seçeneği kullanılmak suretiyle silinmesi halinde yok olan mesaj kayıtları için Message Rocevery isimli bir uygulama geliştirilmiştir. Bu uygulama mağdurun cihazındaki bildirim merkezinin yardımıyla silinen mesajları tekrar oluşturabilmektedir. Böylelikle Whatsapp üzerinden hakaret, tehdit, şantaj gibi suçlara sistematik şekilde maruz kalan ve delillerini soruşturma dosyasına sunamayan mağdurların delillerini sunarak etkili bir soruşturma yapılabilmesine olanak tanınmıştır.

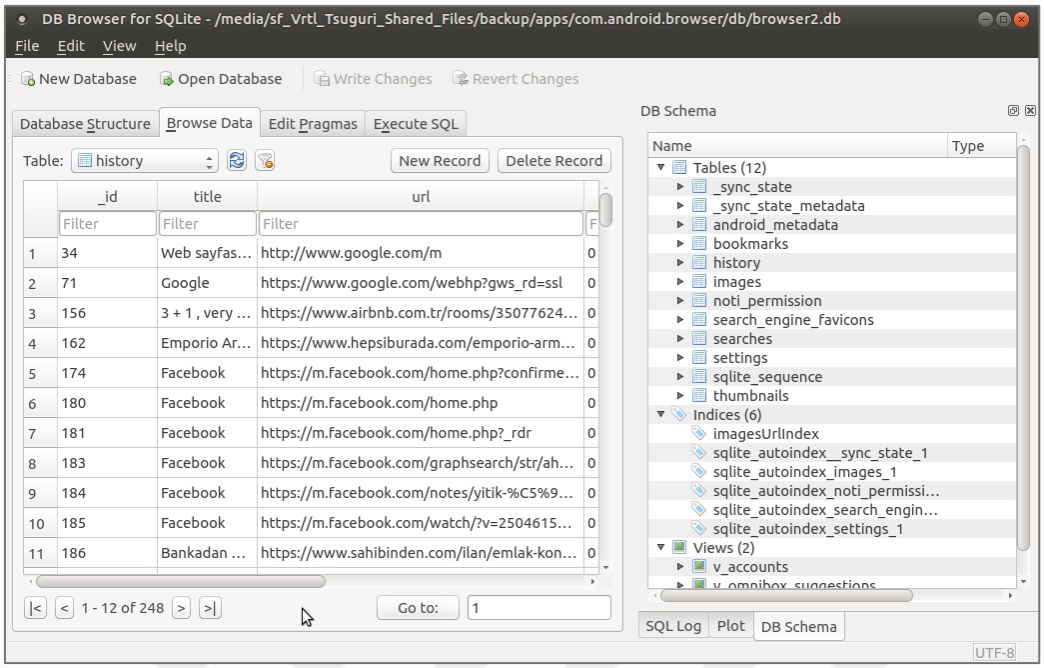
Yine bir çalışmada (Mehrotra & Mehtre, 2013), Wickr isimli uygulamanın kullanılmasıyla iletişim sağlanması halinde, adli bilişim analizinde herhangi bir iz bırakmadığına ilişkin tespitler yapılmıştır. Bu gibi uygulamalarla failler kendilerini anonim kılarak suç işleyebilirler. Dolayısıyla adli bilişim analizlerinin yapılması sırasında, adli bilişim incelemelerinin baltalanması amacını taşıyan yaklaşımları etkisiz kılacak metotların geliştirilmesi de oldukça önemlidir. Nitekim KakoaTalks da bu yaklaşım ile oluşturulmuş bir uygulama olsa da çeşitli çalışmalarla bu uygulamada kapsamında oluşan verilerin elde edilmesi mümkün olmuştur (Kim & Lee, 2020).

5.5.1. DB Browser for SQLite İsimli Yazılım Aracıyla

Hedef cihazın backup dosyası, ADB vasıtasıyla *"adb backup"* komutlarının kullanılmasıyla suretiyle oluşturulabilir. Yine yukarıda açıklanan Android Triage aracının backup seçeneği ile de backup dosyası elde edilinebilir. Bu dosyanın elde edilebilmesi için hedef cihazın root yetkisine sahip olmak zorunluluğu bulunmamaktadır. DB Browser for SQLite aracıyla android backup vasıtasıyla edinilmiş *"backup.ab"* dosyasında mevcut olan cihaz uygulamaların analizi yapılabilir (Mauricio Piacentini ve diğerleri, 2021). Ancak daha öncesinde *"backup.ab"* dosyasının .tar dosyası biçiminde çıkartılması gerekmektedir. Bunun için Android Backup Toolkit isimli araç takımı kullanılabilir (*Android-Backup-Toolkit*, 2022). Bu takım içerisindeki android backup processor klasöründe komut satırı açıldıktan sonra Resim 5.22'de gösterildiği şekilde *"java -jar abp.jar unpack 'backup.ab dosyasının bulunduğu dizin' backup.tar 'backup dosyasının şifrelenmiş olması halinde şifresi'"* komutunun kullanılması suretiyle Android backup (.ab) dosyası, .tar dosyasına dönüştürülebilecektir. Daha sonrasında oluşturulan sıkıştırılmış dosya biçimi olan .tar dosyası da klasöre ayıklanarak meydana gelen klasör içerisinde DB Browser for SQLite aracıyla cihazdaki uygulamaların klasör ve dosyaları arasında gezinti yapılabilir. Uygulama klasörlerinin db klasörü altında bulunan .db dosyaları açılınarak SQL kayıtları analiz edilebilecektir.

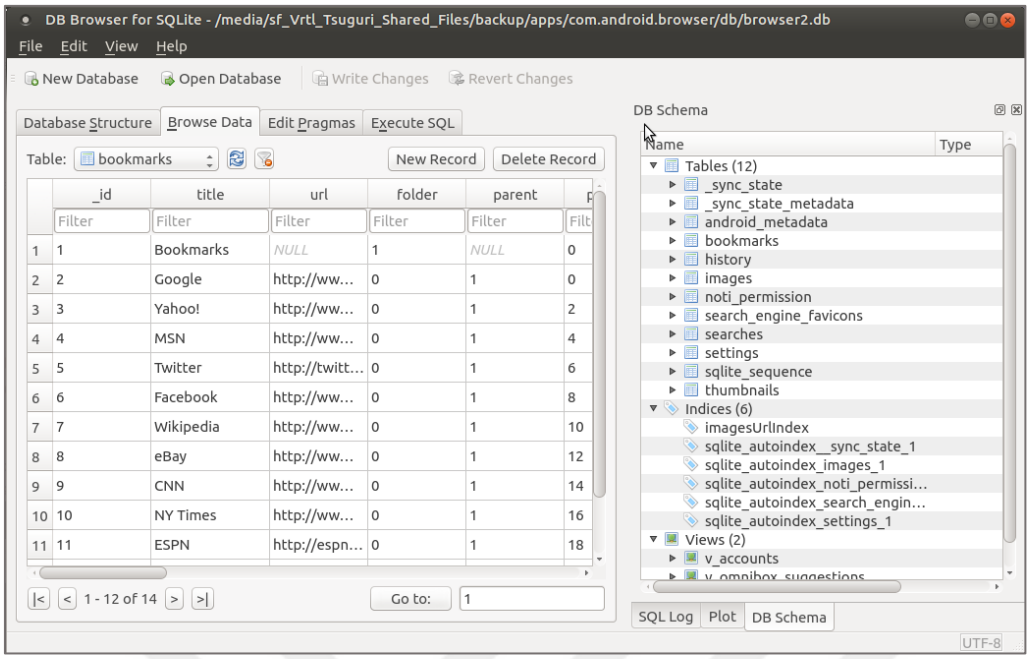


Resim 5. 22. Backup.ab dosyasının sıkıştırılmış bir dosya türü olan .tar dosyasına dönüştürülmesine ilişkin komut satırı.



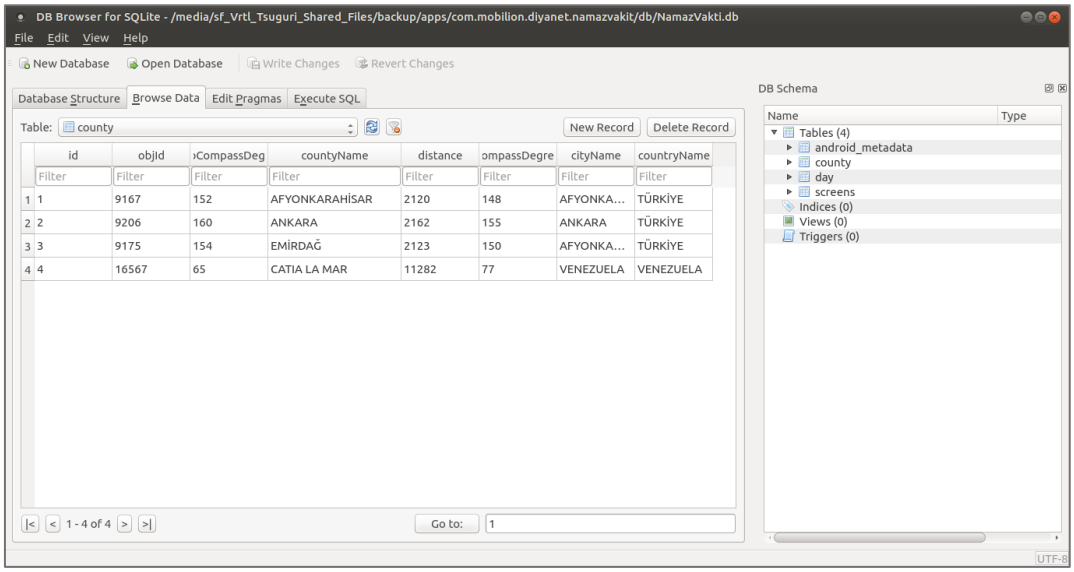
Resim 5. 23. Cihazın yerleşik tarayıcısının internet sitesi geçmişi

Android Triage aracı ile root yetkisi bulunmayan Android 6.0 sürümündeki LG G4 cihazından elde edilen backup.ab dosyası analiz edilmiştir. Resim 5.23'de cihazda bulunan yerleşik internet tarayıcısı ile ziyaret edilen internet sitelerinin geçmişinin elde edilmesi gösterilmiştir. Resim 5.24'de ise cihazın yerleşik tarayıcısına kullanıcı tarafından sık kullanılanlara kaydedilen internet siteleri (yer imleri) görüntüsü sunulmuştur.



Resim 5. 24. Cihazın yerleşik tarayıcısının yer imleri

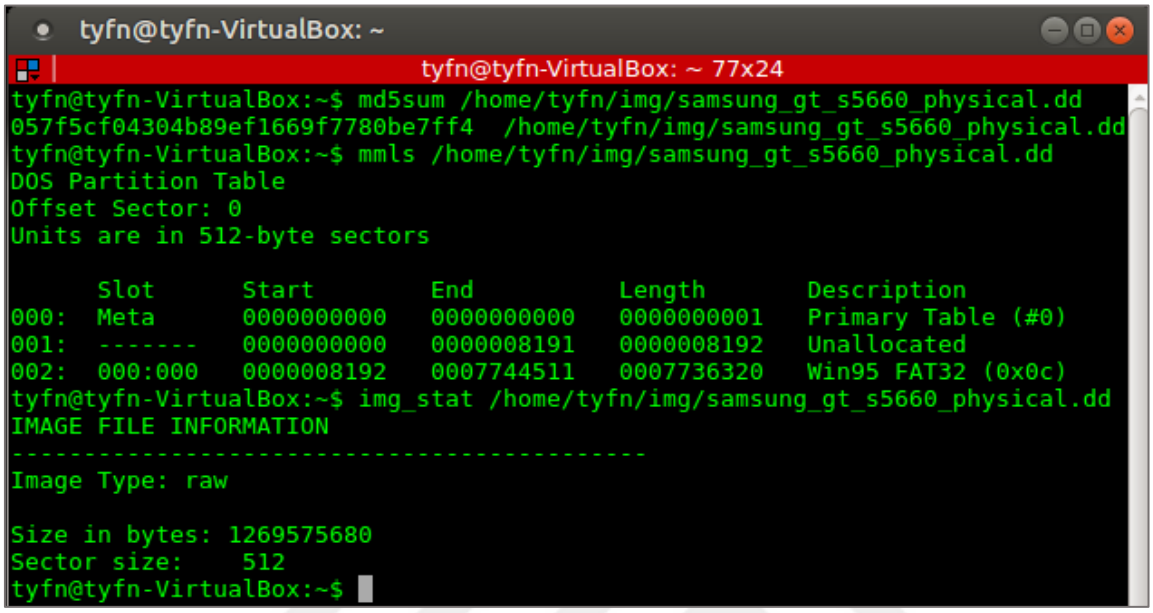
Resim 5.25'te cihazda bulunan namaz vakti uygulamasına hangi şehirlerin kaydedildiğine ilişkin veriler gösterilmiştir. Yapılan bir soruşturmada şüphelinin nerede bulunduğuna ilişkin bir kuşku bulunması halinde, bu uygulamaya kaydedilen şehirlerden yola çıkarak maddi gerçeğe ulaşılabilir.



Resim 5. 25. Namaz vakti isimli uygulamadaki kayıtlı şehirler

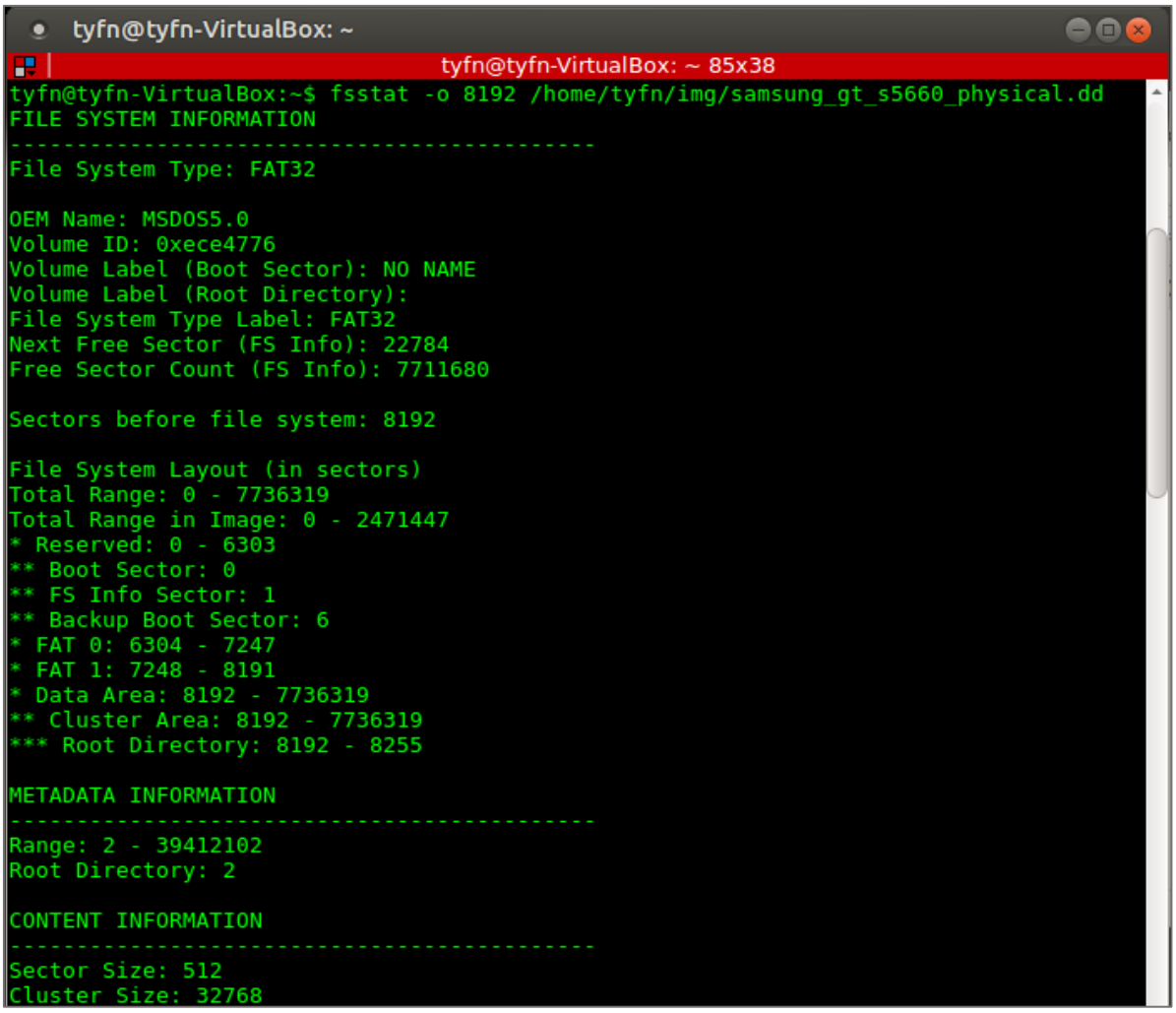
5.5.2. Autopsy Sleuth Kit İsimli Yazılım Aracıyla

Autopsy arayüzü ve araç takımlarıyla kolaylıkla imaj dosyaların analiz edilmesini sağlayan açık kaynak kodlu bir yazılım aracıdır (Brian Carrier, 2021).



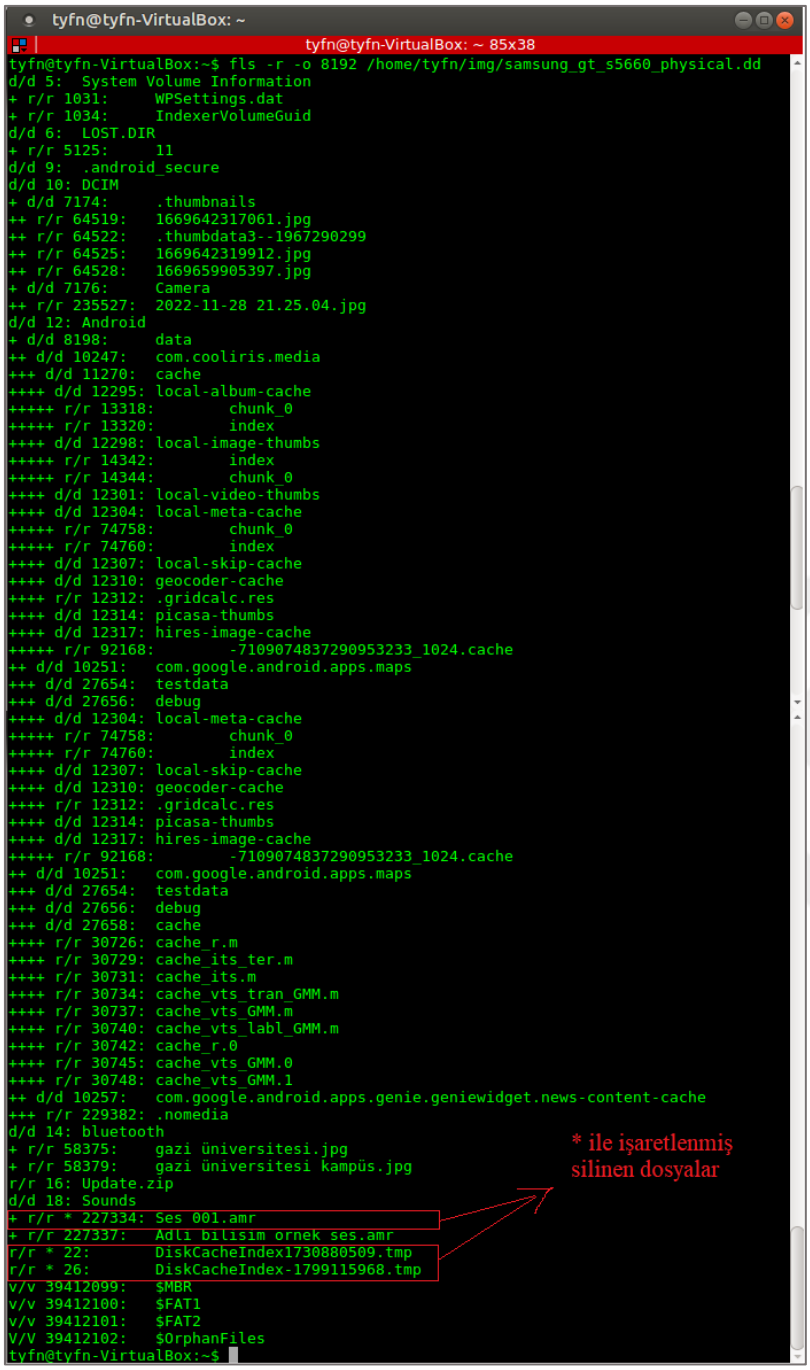
Resim 5. 26. İmajın sektörlerinin başlangıç ve bitişinin, boyutunun, fiziksel imaj dosyası olup olmadığının kontrol edilmesi

Autopsy Sleuth Kit vasıtasıyla fiziksel imajın analiz edilmesi mümkündür. "DD Komutlarının Vasıtasıyla" Bölümünde anlatıldığı şekilde, Android 2.3.3. sürümlü Samsung Galaxy Gio GT- s5660 cihazından elde edilen fiziksel imaj dosyası aşağıdaki resimlerde gösterildiği şekilde analiz edilmiştir. Bu bağlamda Resim 5. 26'daki gibi *"md5sum"* komutuyla imaj dosyasının doğruluğu kontrol edilip, *"mmls"* komutuyla fiziksel imajın ayrılmış ve ayrılmamış alanları, bölümlerinin başlangıç ve bitişi, boyutu belirlenebilir. Yine Resim 5. 27'te gösterildiği şekilde *"fsstat"* komutuyla imaj hakkında daha detaylı bilgilere ulaşılabilir.



Resim 5. 27. Fiziksel imaj hakkında çeşitli bilgilerin elde edilmesi

Yine Resim 5.28'deki biçimde *"fls -r -o 'dosya sisteminin başlangıç sektörü'"* komutuyla imajın dosya sistemindeki klasörler ve klasörler içerisindeki dosyaların dökümü elde edilebilir. Bu dökümde, *"*"* ibaresiyle işaretlenmiş dosyalar silinen dosyaları temsil etmektedir. Bu Resim'de görülen silinmiş *"Ses 001.amr"* dosyası aslen, hemen altındaki *"Adli bilişim örnek ses.amr*" dosyasının aynısıdır. Nitekim kullanıcı tarafından alınan ses kaydı ilk olarak akıllı telefonun ses kaydetme uygulaması tarafından Ses 001.amr adıyla kaydedilmiş, kullanıcı tarafından ise dosya adı "*Adli bilişim örnek ses.amr*" olarak değiştirilmiştir. Dolayısıyla her ne kadar kullanıcı sadece dosya adını değiştirdiyse de Ses 001.amr dosyasının üzerine yazılmadan saklanıp bu dosyanın kopyası yeni isimle kaydedilmiştir. Cihazın flaş belleğinde *"Ses 001.amr"* dosyasının bulunduğu alan üzerine yeni bir veri yazılmadığından dosyayı kurtarmak mümkün olmuştur.



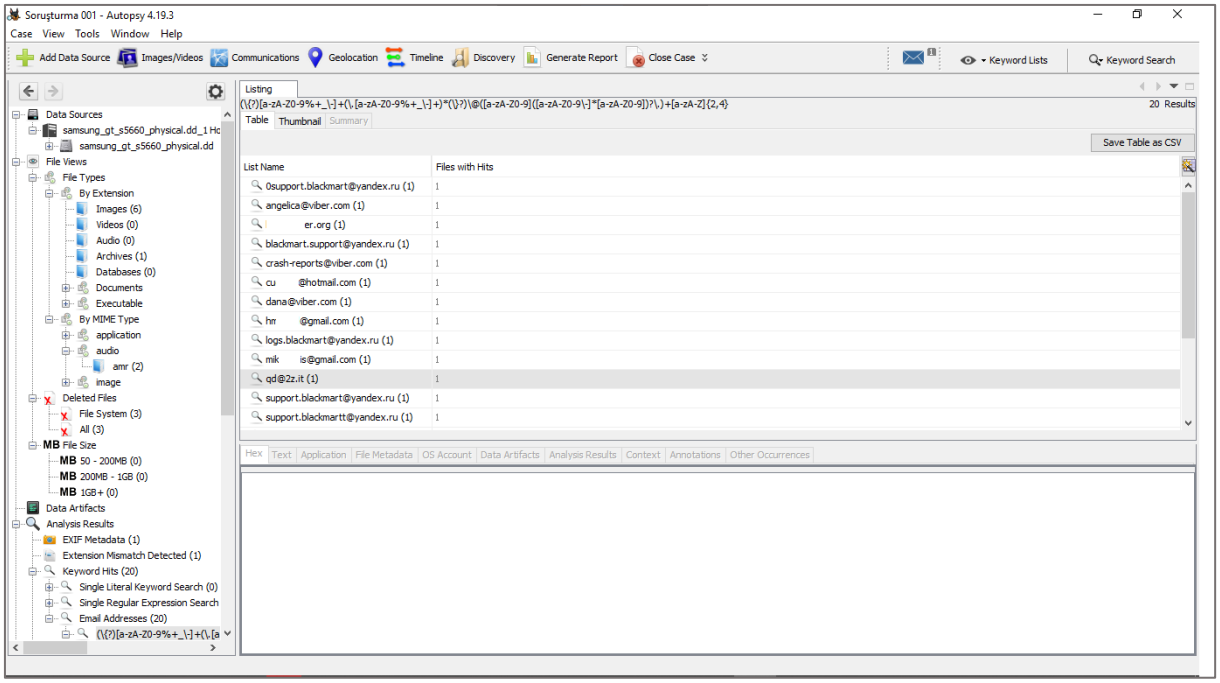
Resim 5. 28. Sleuth Kit vasıtasıyla klasör ve dosyaların görüntülenmesi

İmaj dosyasındaki dosyaları, dosya sistemi oluşturacak şekilde kurtarabilmek için Resim 5.29'daki gibi *"tsk_recover -o 'dosya sisteminin başlangıç sektörü' -e 'imaj dosyasının bulunduğu dizin' kurtarılan dosyaların çıkartılacağı dizin adresi'"* komutu kullanılabilir.

```
tyfn@tyfn-VirtualBox:~/img$ tsk_recover -o 8192 -e samsung_gt_s5660_physical.dd home/tyfn/img/recovered
Files Recovered: 30
tyfn@tyfn-VirtualBox:~/img$
```

Resim 5. 29. Silinen dosyalar da dahil olmak üzere tüm klasör ve dosyaların kurtarılarak çalışma istasyonundaki bilgisayara aktarılması

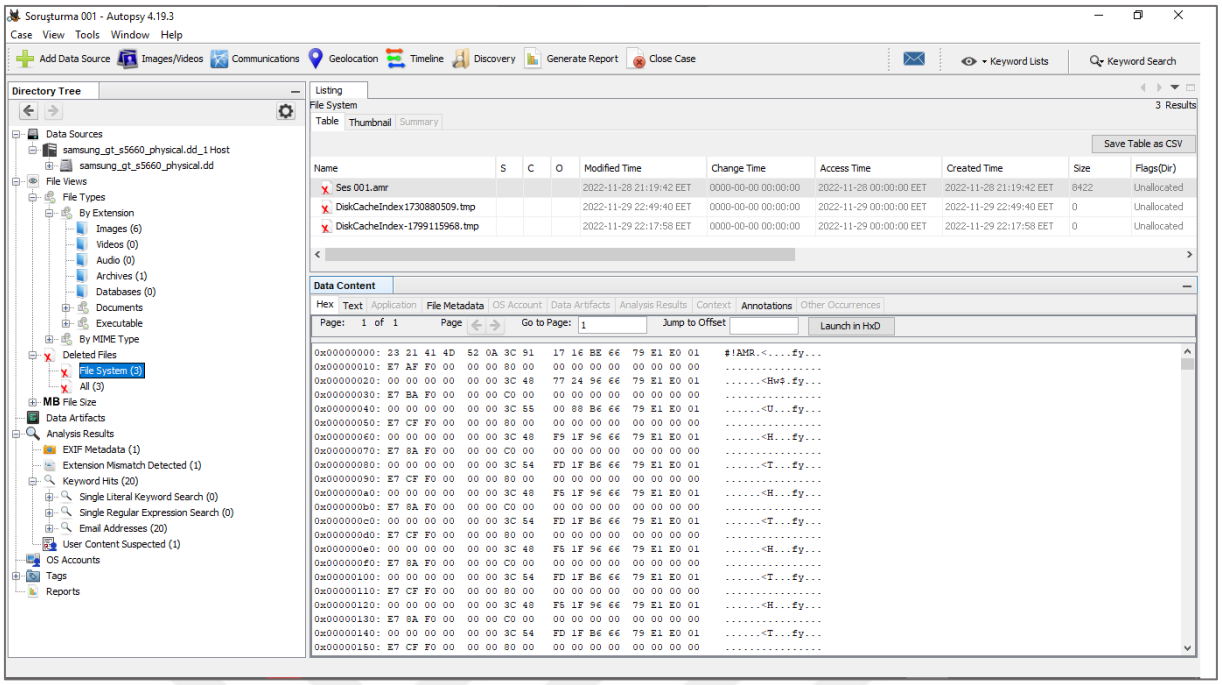
Bununla beraber Autopsy yazılımının arayüzü yardımıyla imaj dosyasının da incelenmesi mümkündür. Resim 5.30'da daha öncesinde cihazın fabrika ayarlarına sıfırlanmasına karşılık sıfırlamadan önce cihazda mevcut anahtar kelimeler vasıtasıyla elde edilen e-posta verileri gösterilmiştir.



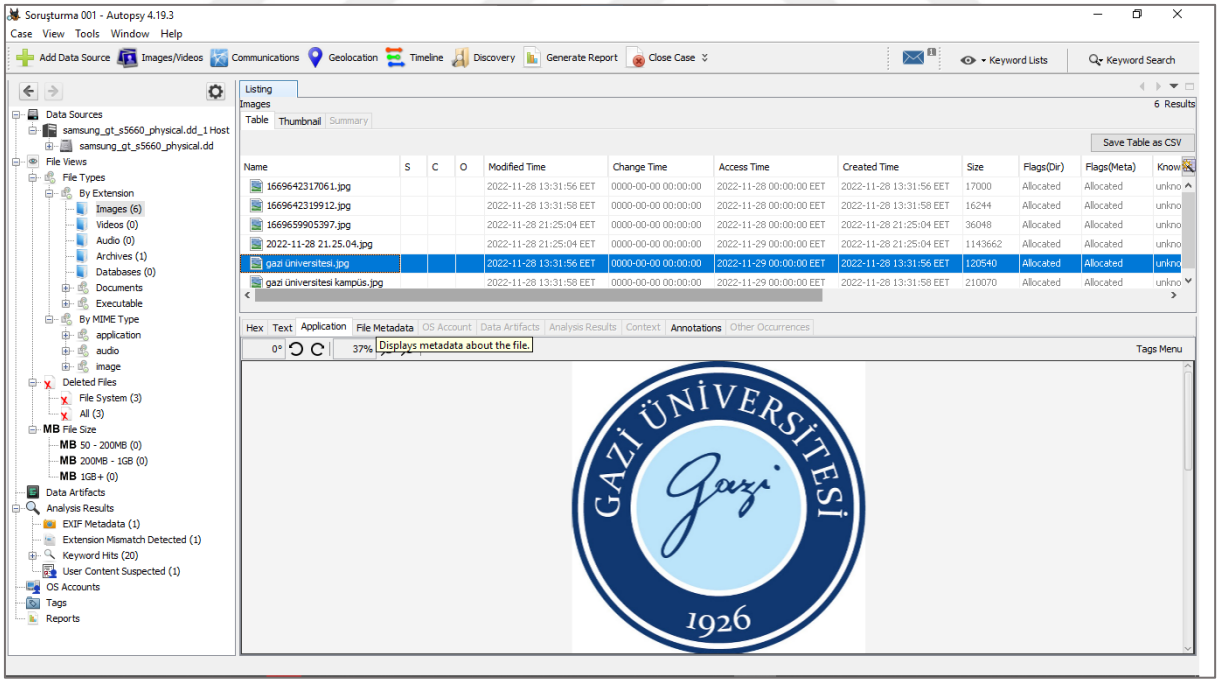
Resim 5. 30. Fiziksel imajdaki anahtar kelimeler vasıtasıyla e-posta adreslerinin elde edilmesi

Resim 5.31'de silinen bir dosya ve bu dosyanın Hex kaydı gösterilmiştir. Resim 5.32'de ise, imaj dosyasından elde edilen bir görselin doğrudan Autopsy yardımıyla açılması sunulmuştur.

Dolayısıyla Autopsy arayüzü yardımıyla imajdaki dosyaların Hex bilgilerinin, meta verilerinin, dosya sisteminin analiz edilmesi geniş bir şekilde gerçekleştirilebilir.



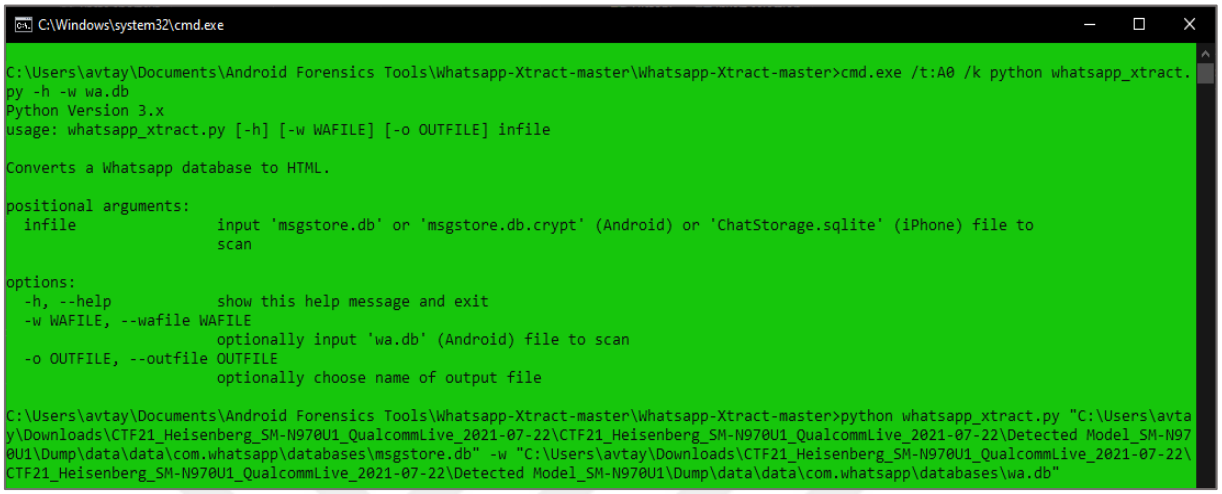
Resim 5. 31. Fiziksel imajdaki silinen dosyaların belirlenmesi ve Hex kayıtlarının incelenmesi



Resim 5. 32. Fiziksel imajdaki bir görselin analizi

5.5.3. Whatsapp Xtract İsimli Yazılım Aracıyla

Açık kaynak kodlu Whatsapp Xtract aracıyla *"msgstro.db"* ve *"wa.db"* dosyalarının analiz edilerek Whatsapp mesajları ve durumlarının incelenmesi mümkündür (KBase, 2022).

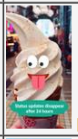


Resim 5. 33. Whatsapp Xtract aracında konsola mesaj kayıtların incelenmesi için gerekli kodun girilmesi

Resim 5.33, Whatsapp-Xtract aracıyla konsolun çalıştırılmasından sonra *"python whatsapp-xtract.py 'msgstore.db dosyasının bulunduğu dizin' -w 'wa.db dosyasının bulunduğu dizin'"* kod satırının girilmesine ilişkin ekran görüntüsüdür. Bu kodun çalıştırılmasının akabinde tarayıcıda bir .html dosyası doğrudan açılarak ilgili mesaj kayıtlarını, paylaşılan durumları Resim 5.34'teki gibi gösterecektir.

PK	Contact Name	Contact ID	Status	# Msg	# Unread Msg	Last Message
1	status	status@broadcast	N/A	N/A	N/A	N/A

Chat session # 1: status

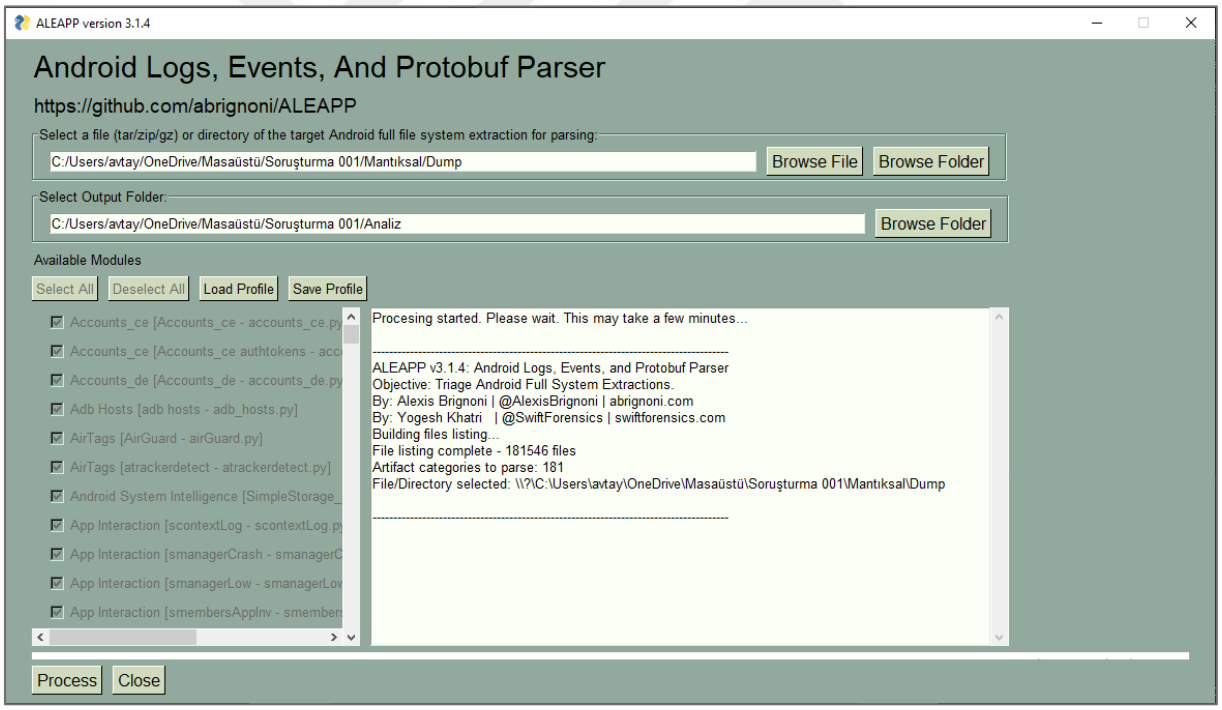
PK	Chat	Msg date	From	Msg content	Msg status	Media Type	Media Size
2	status	2017-02-14 22:20:01	0@s.whatsapp.net	 | Image	0	1	91858
3	status	2017-02-14 22:20:02	0@s.whatsapp.net	N/A	0	13	274412
4	status	2017-02-14 22:20:03	0@s.whatsapp.net	 | Image	0	1	97786
5	status	2017-02-14 22:20:04	0@s.whatsapp.net	 | Image	0	1	72973
							

Resim 5. 34. Whatsapp-Xtract aracı ile whatsapp mesaj ve durum kayıtlarının elde edilmesi

Android akıllı telefonlarda *"msgstore.db"* ve *"wa.db"* dosyaları cihazın */data/data/com.whatsapp/databases/* dizininde saklanmaktadır. Ancak bu dosyaların elde edilebilmesi için cihazın root yetkisine sahip bulunmak gerekmektedir.

5.5.4. ALEAPP İsimli Yazılım Aracıyla

Açık kaynak kodlu ALEAPP (Android Log, Events, And Proof Parser) aracı ile alınan mantıksal veya fiziksel imajın analizinin yapılması mümkündür (Brignoni, 2022). Araç Python programlama dili ile çalıştığından Python'un çalışma istasyonundaki bilgisayar kurulması ve aracın bulunduğu dizinde komut istemcisinin açılarak *"pip install -r .\requirements.txt"* komut satırının uygulanması gerekmektedir. Daha sonrasında aleappGUI.py isimli dosyanın çalıştırılmasıyla Resim 5.35'teki gibi açılacak arayüz vasıtasıyla ilgili imajın bulunduğu dosya veya mantıksal imaj olması halinde dosyaların bulunduğu dizinin seçilip analizin yapılmasını sağlamak mümkündür.

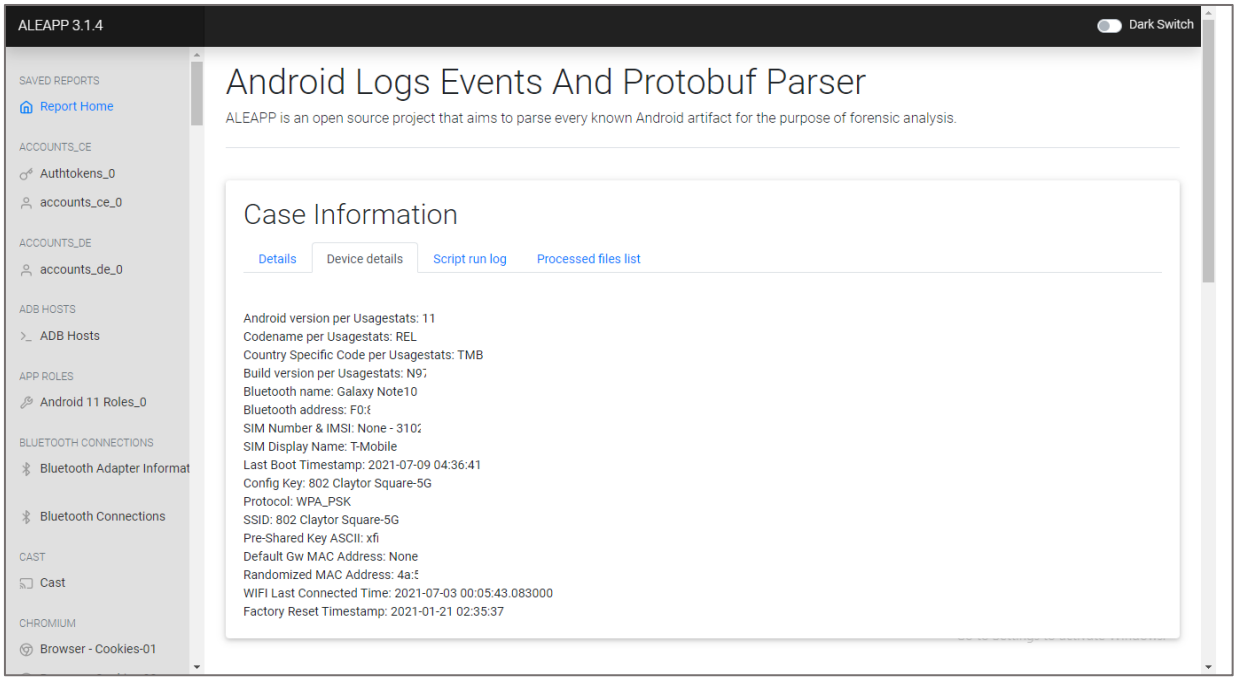


Resim 5. 35. ALEAPP isimli aracın kullanıcı arayüzü

Analiz raporu bir .html dosyası şeklinde çalışma istasyonu bilgisayarında belirlenen dizin adresinde oluşacaktır. Örnek bir mantıksal imaj dosyası (James, 2021) bu araç vasıtasıyla analiz edilmiştir. Bu araç vasıtasıyla tarayıcıların geçmişi, çerezleri, çevrimdışı sayfaları, arama motoru anahtar kelimeleri; SMS ve MMS bilgileri; Gmail hesapları; cihazdaki

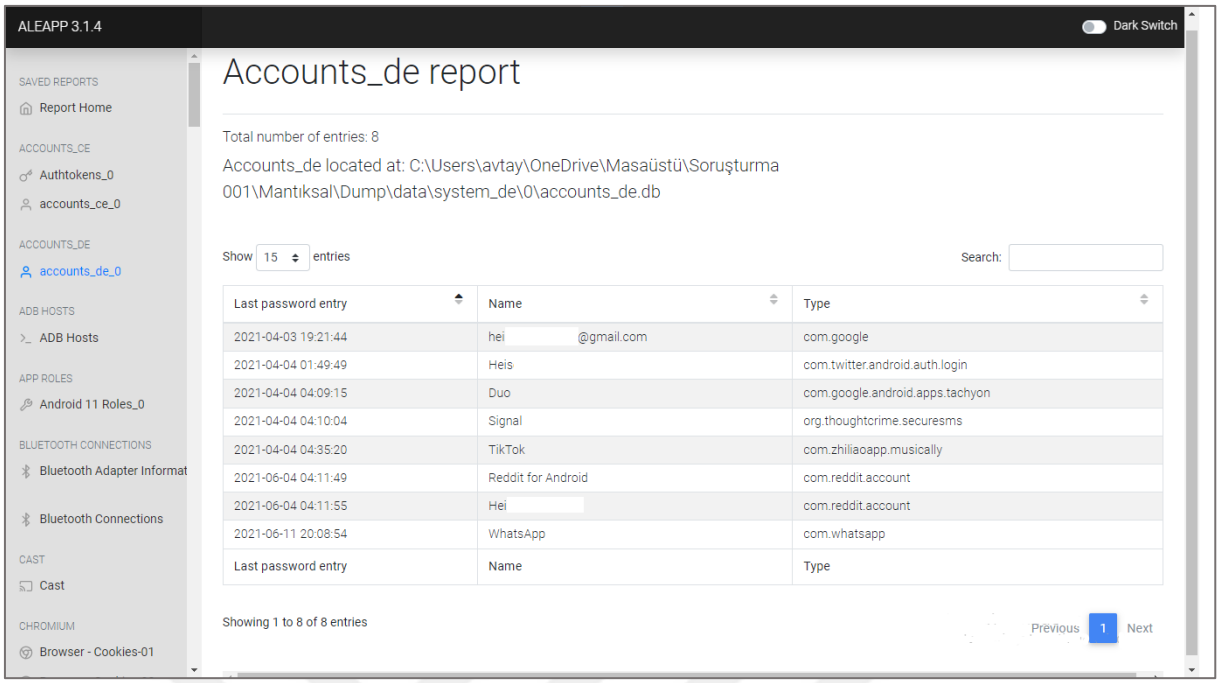
uygulamaların çalıştırılma zaman aralıkları; cihazın gücünün kapatılması ve yeniden başlatılmasının, fabrika ayarlarına sıfırlanmasının tarihleri; bluetooth bilgileri ve bağlanılan bluetooth cihazları; WiFi bilgileri; Snapchat hesap bilgileri; Whatsapp hesap ve mesaj bilgileri; SIM kart bilgileri vb. birçok verinin analizine oldukça kapsamlı ve hızlı bir şekilde ulaşmak mümkündür. Resim 5.36'da .html dosyası biçimindeki analiz raporu gösterilmiştir.

Resim 5.37 ila Resim 5.43 arası cihazdan elde edilen verilerin muhtelif analiz bilgileri gösterilmiştir. ALEAPP aracı, imajların analiz edilmesi açısından oldukça kapsamlı, hızlı ve etkili bir çözüm sunmaktadır.

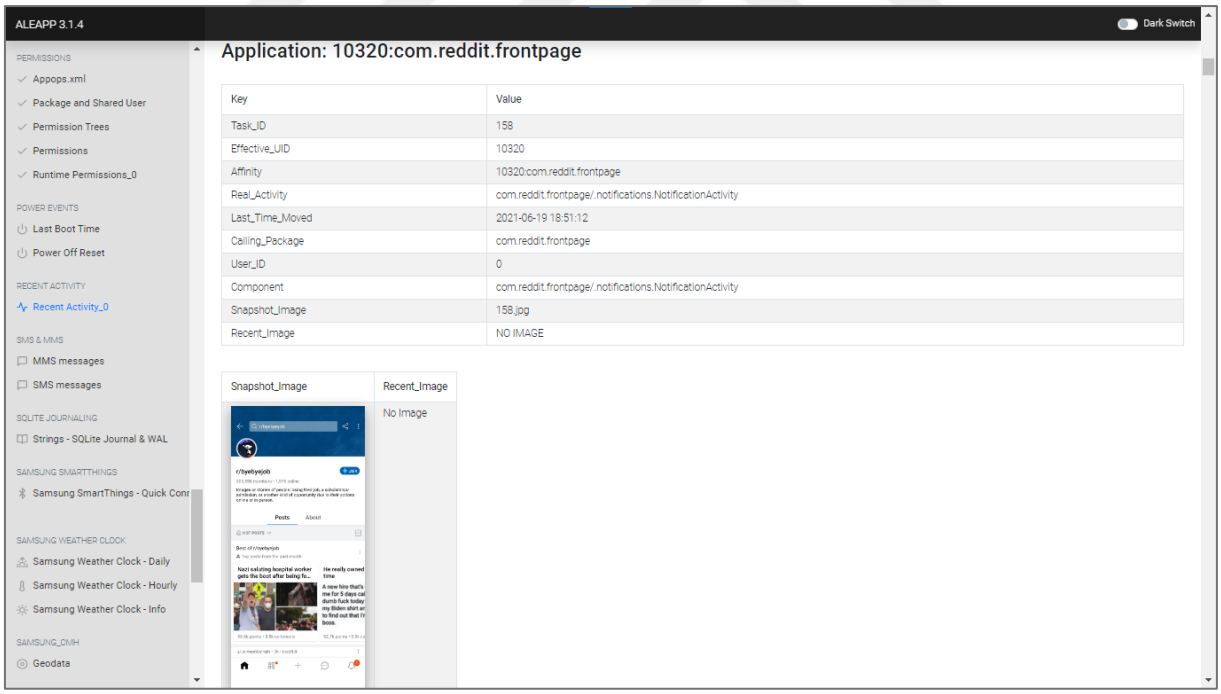


Resim 5. 36. Analiz sonucu açılan html dosyasında hedef cihaz bilgilerinin görüntülenmesi

Resim 5.37'de hedef cihazdan elde edilen Whatsapp, Google, Reddit, Tiktok gibi hesap bilgileri gösterilmiştir. Resim 5.38'de Reddit isimli sosyal medya uygulamasının ekrandaki son aktivite durumunun görüntülenmesi sunulmuştur.

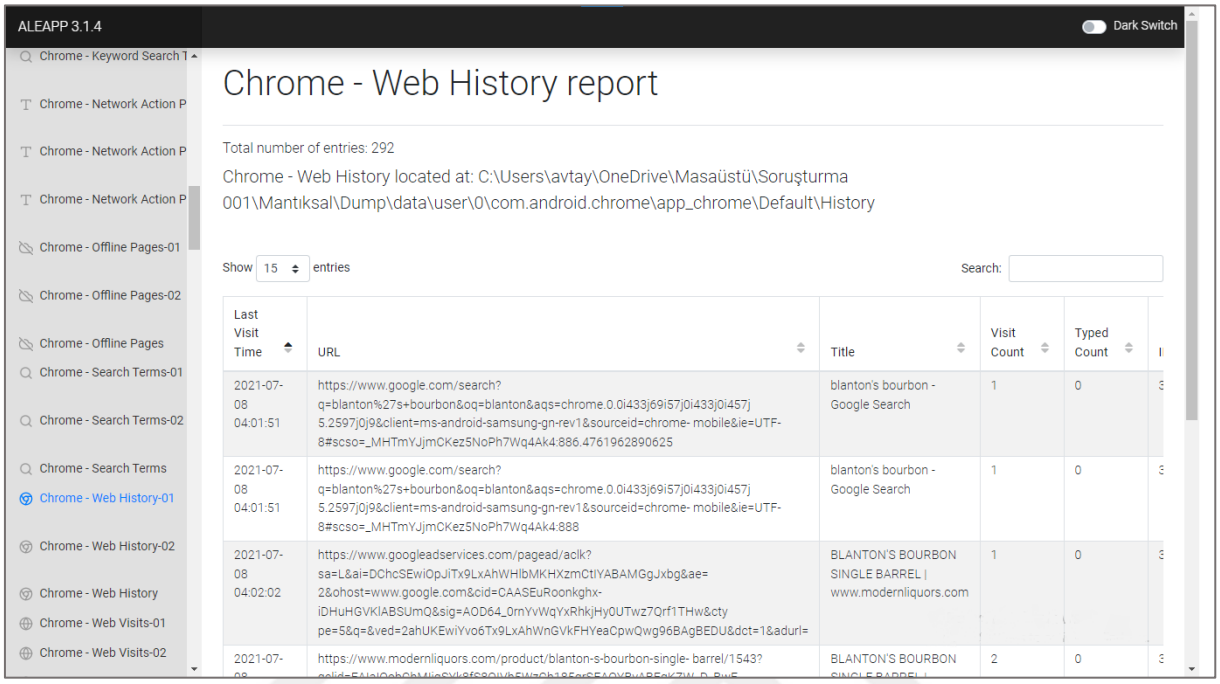


Resim 5. 37. Akıllı telefondaki çevrimiçi hesapların görüntülenmesi

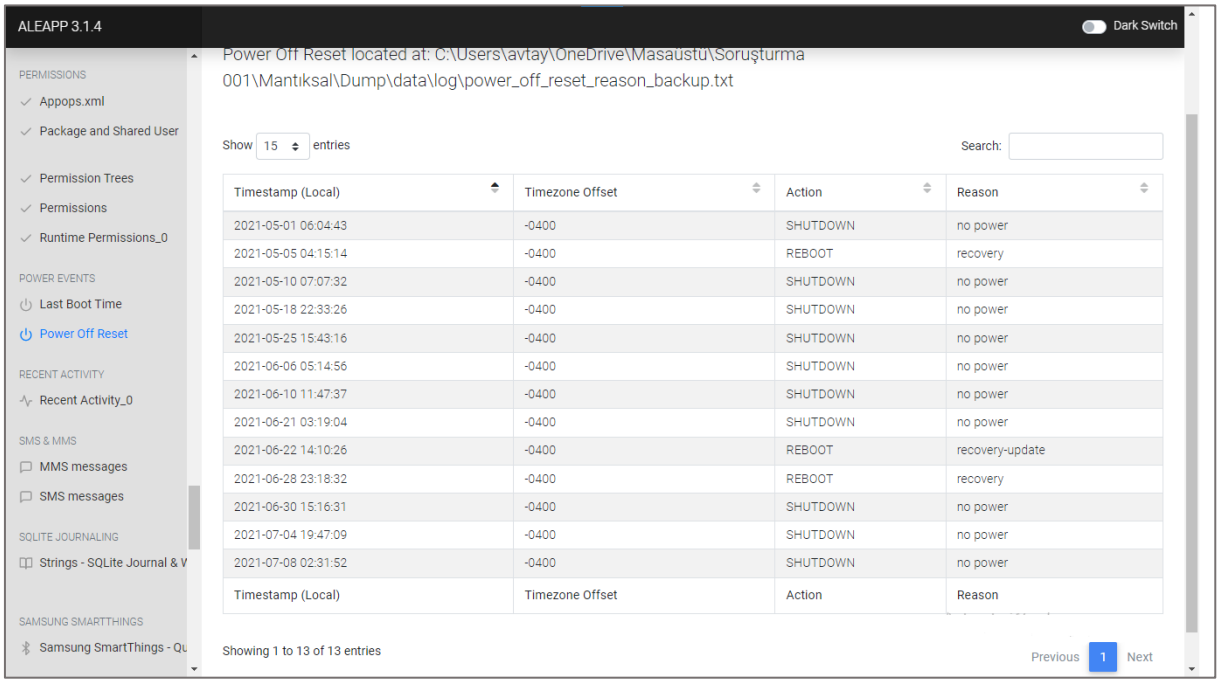


Resim 5. 38. Cihazdaki Reddit isimli sosyal medya uygulamasındaki son aktivitenin görüntülenmesi

Resim 5.39'da hedef cihazdaki Chrome isimli internet tarayıcısında ziyaret edilen internet sitelerinin geçmişi gösterilmiştir. Resim 5.40'ta ise, Cihazın açılma kapatılması tarih ve saatleri gösterilmiştir.

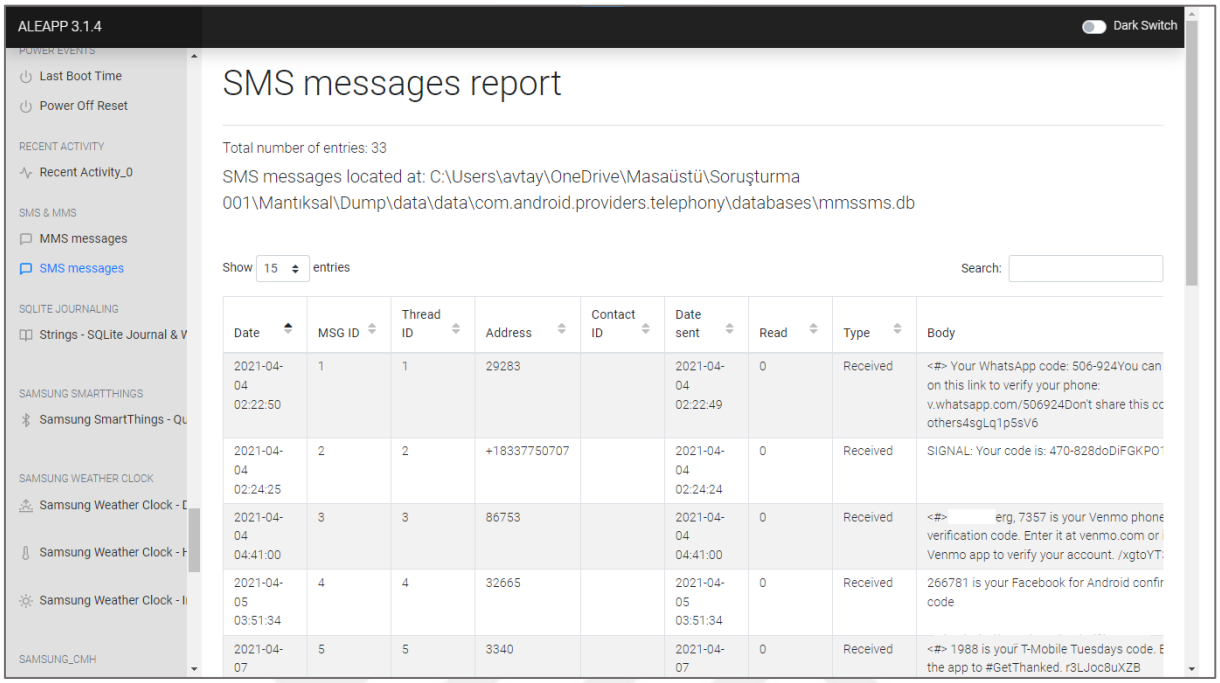


Resim 5. 39. Cihazdaki Chrome internet tarayıcısında ziyaret edilen internet sitelerinin görüntülenmesi

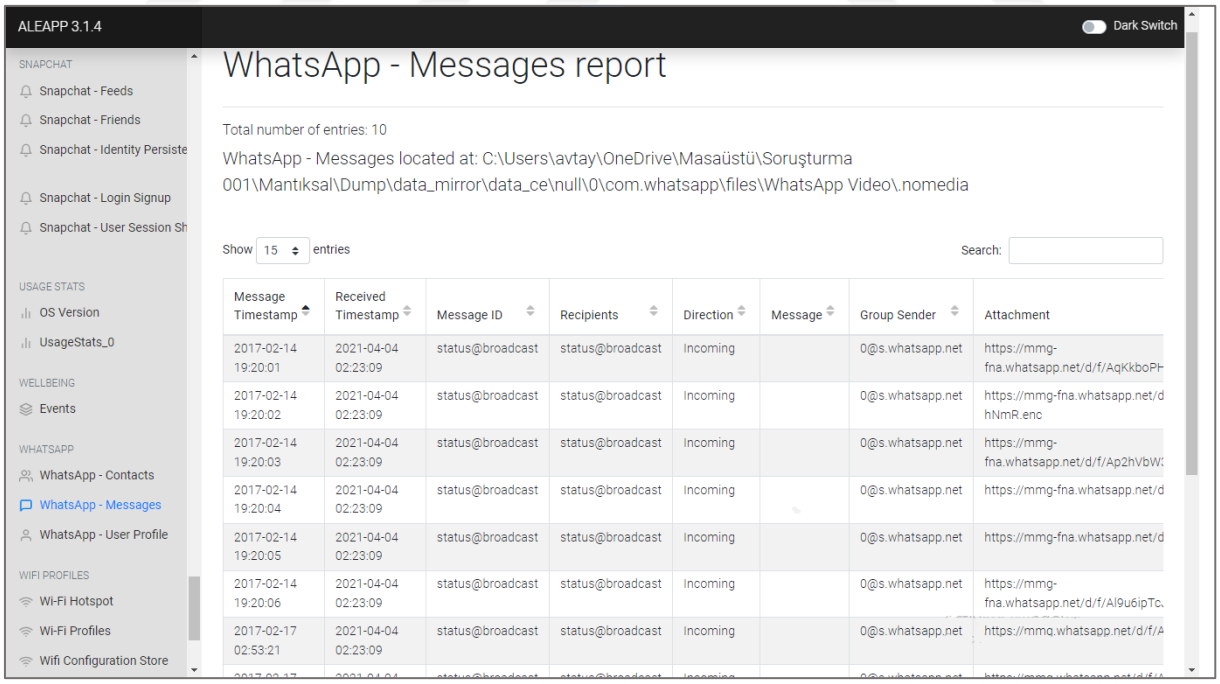


Resim 5. 40. Cihazın gücünün kapatılması ve yeniden başlatılması tarihlerinin görüntülenmesi

Resim 5.41'de Cihazdaki SMS mesajları, 5.42'de Whatsapp üzerindeki kişilerin paylaştığı durumlar ve gönderdiği mesajların analiz edildiği bölüm gösterilmiştir.

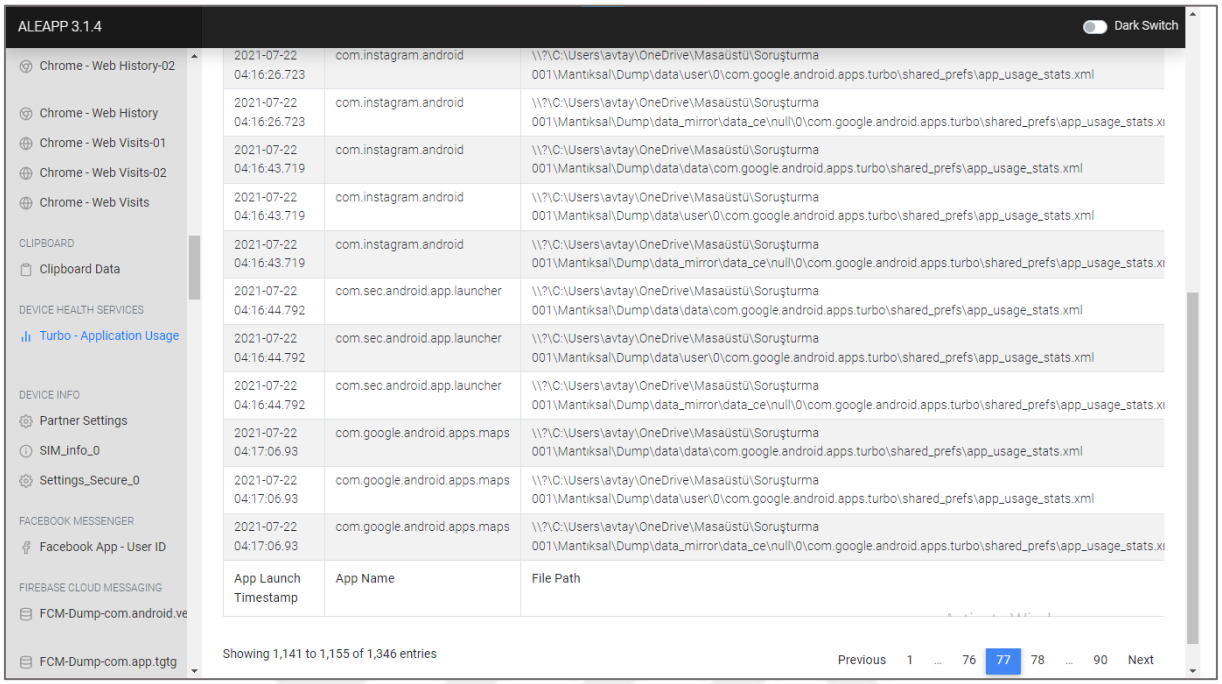


Resim 5. 41. Cihazdaki SMS mesajlarının görüntülenmesi



Resim 5. 42. Cihazdaki Whatsapp mesaj ve durumlarının görüntülenmesi

Resim 5.43'te cihazdaki uygulamaların hangi zaman aralıklarında çalıştırıldığı, ne kadar süreyle çalışmalarının devam ettiğine ilişkin analiz ekranı gösterilmiştir.



Resim 5. 43. Cihazdaki uygulamaların çalıştırılma zaman aralıklarının görüntülenmesi

5.5.5. Open Source Android Forensics (OSAF) Yazılım Araç Takımıyla

OSAF yazılım araç takımıyla hedef cihazda kötü amaçlı yazılımların bulunup bulunmadığı tespit edilebilir. OSAF-Toolkit, kötü amaçlı Android yazılımların analizinin standardının sağlanmasına öncü olmak ve yol açabilmek için Cincinnati Üniversitesindeki birkaç Bilişim öğrencisinden oluşan grup tarafından bitirme tasarım projesi olarak geliştirilmiştir. OSAF araç takımı, kod incelebilmesinin ve kötü amaçlı yazılım analizinin yapılabilmesi sağlamak için gerekli olan tüm araçlarla birlikte Ubuntu 11.10 işletim sistemi tabanlı olarak kurulmuştur (OSAF Community, 2015). Alt başlıklarda bu araç takımındaki araçlarla analiz işlemlerinin nasıl yapılabileceği açıklanmıştır.

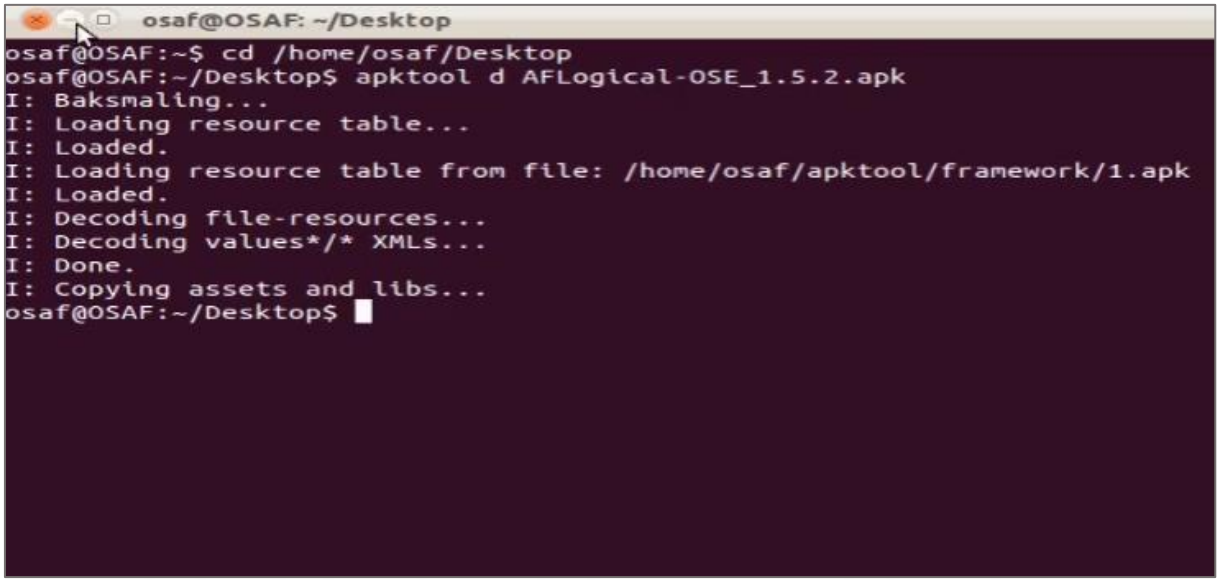
5.5.5.1. Apktool İsimli Yazılım Aracıyla

Apktool isimli araç Android uygulamaların tersine mühendislik yöntemleriyle kaynak kodu dosyalarının açılımını veren açık kaynak kodlu bir yazılım aracıdır (Tumbleson, 2022).

Apktool isimli aracı kullanmak için Terminal ekranında ilk olarak Apktool aracının bulunduğu masaüstü klasörüne gitmemiz gereklidir. Bunun için Resim 5.44'teki gibi

Terminalde, *"cd /home/osaf/Desktop"* komutuyla masaüstü dizinine gitmemiz gereklidir. İnceleyeceğimiz .apk dosyasını da masaüstü dizinine kopyalamamız gerekmektedir.

Terminalde devamında *"apktool d apkdosyasınınismi.apk"* kodunu yazmamızla beraber apk dosyasının kaynak dosyaları masaüstündeki bir klasörde oluşacaktır. Bu kaynak dosyaları, OSAF araç takımında bulunan diğer araçlarla inceleyerek apk dosyasının zararlı bir yazılım içerip içermediğini denetlenebilir.

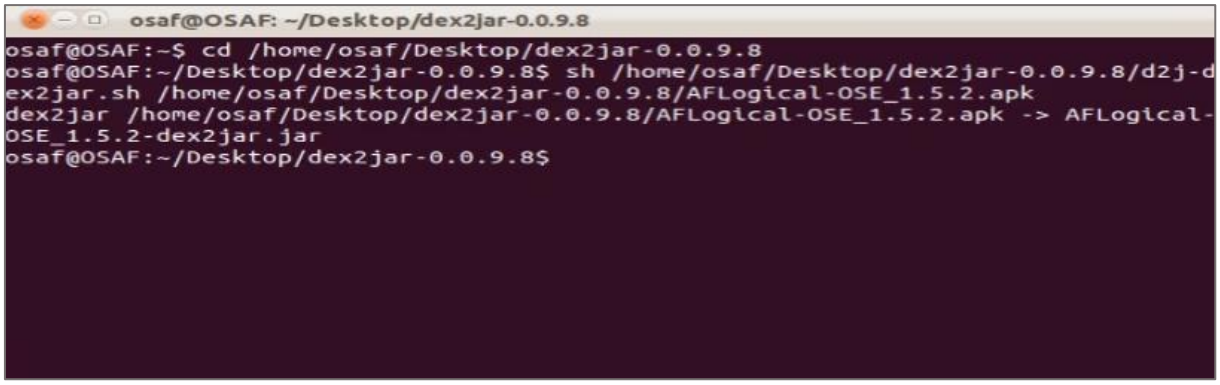


Resim 5. 44. Desktop dizinine gidilerek *"apktool d apkdosyasınınismi.apk"* komutunun uygulanması

5.5.5.2. Dex2Jar İsimli Yazılım Aracıyla

Dex2Jar isimli uygulama .apk dosyalarını .jar dosyalarına dönüştürerek JD-GUI ve JarComparer isimli uygulamalarla .apk dosyalarının analinizin yapılabilmesi sağlamaktadır. Böylelikle DVM tarafından çalıştırılması için Android uygulamalarda oluşturulmuş olan dex kodlarını Java class dosyalarına dönüştürmektedir (Pan, 2015).

Uygulamayı kullanmak için OSAF araç takımında uygulamanın bulunduğu masaüstündeki *"dex2jar-0.0.9.8"* klasörüne Terminalde gidilip ve de analiz edilmek istenen .apk dosyası da bu klasöre kopyalanması gerekir. Bunun için terminale, *"cd /home/osaf/Desktop/dex2jar-0.0.9.8"* komutu yazılarak dex2jar klasörüne gidilir. Devamında terminale, *"sh /home/osaf/Desktop/dex2jar-0.0.9.8/d2j-dex2jar.sh 'dönüştürülmek istenen .apk dosyasının bulunduğu dizin'"* komutu yazılarak .apk dosyasının .jar dosyasına dönüştürülmesi sağlanabilir oluşturulabilir. Resim 5.45.'te terminale girilmesi gereken kodlar belirtilmiştir.



Resim 5. 45. Dex2jar dizinine gidilerek .apk dosyasının .jar dosyasının oluşturulması için uygulanan kodlar

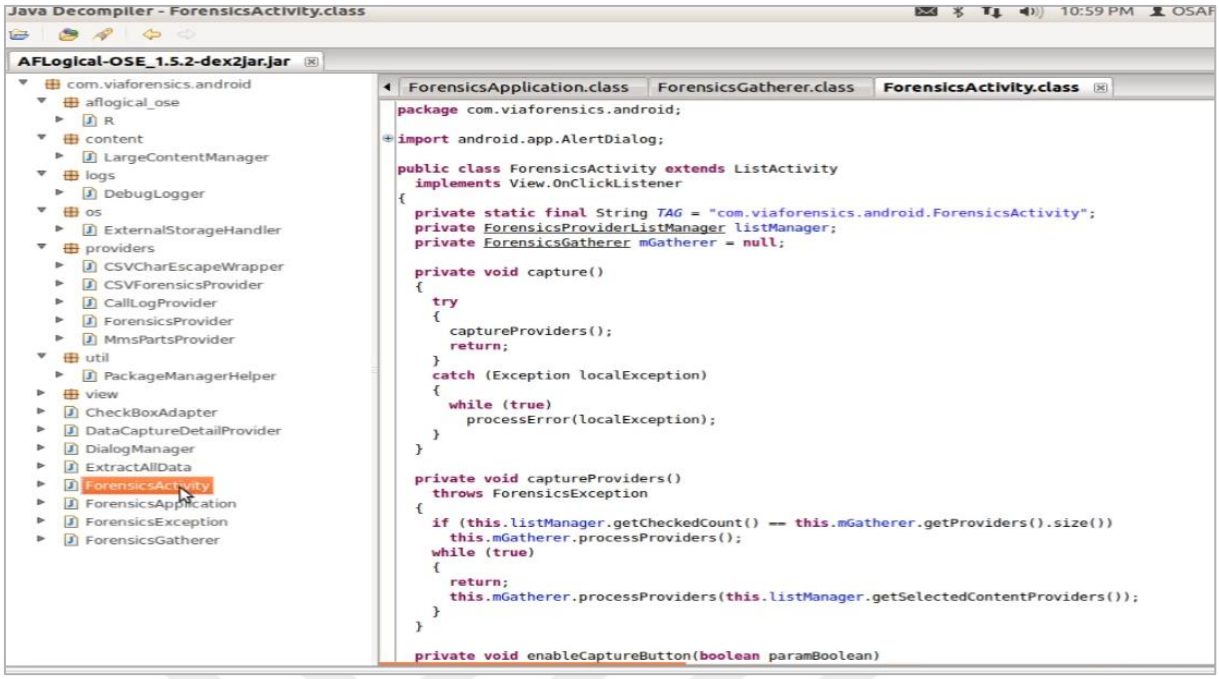
5.5.5.3. JD-GUI İsimli Yazılım Aracıyla

JD-GUI isimli uygulama ile Java dili ile oluşturulmuş .class dosyalarının Java kodlarının analiz edilmesini sağlamaktadır (Java Decompiler, 2015).

Uygulamayı açtığımızda Resim 5.46'daki gibi karşımıza gelen pencerede, "Open a file" seçeneği seçilerek .apk dosyasına ilişkin .jar dosyasında bulunan .class dosyasının Java kodları Resim 5.47'deki gibi incelenebilir.

JD-GUI Uygulaması masaüstündeki kısayoldan direk olarak çalıştırılabilir.

Resim 5. 46. JD-GUI aracında "Open a file" seçeneğinin seçilmesi

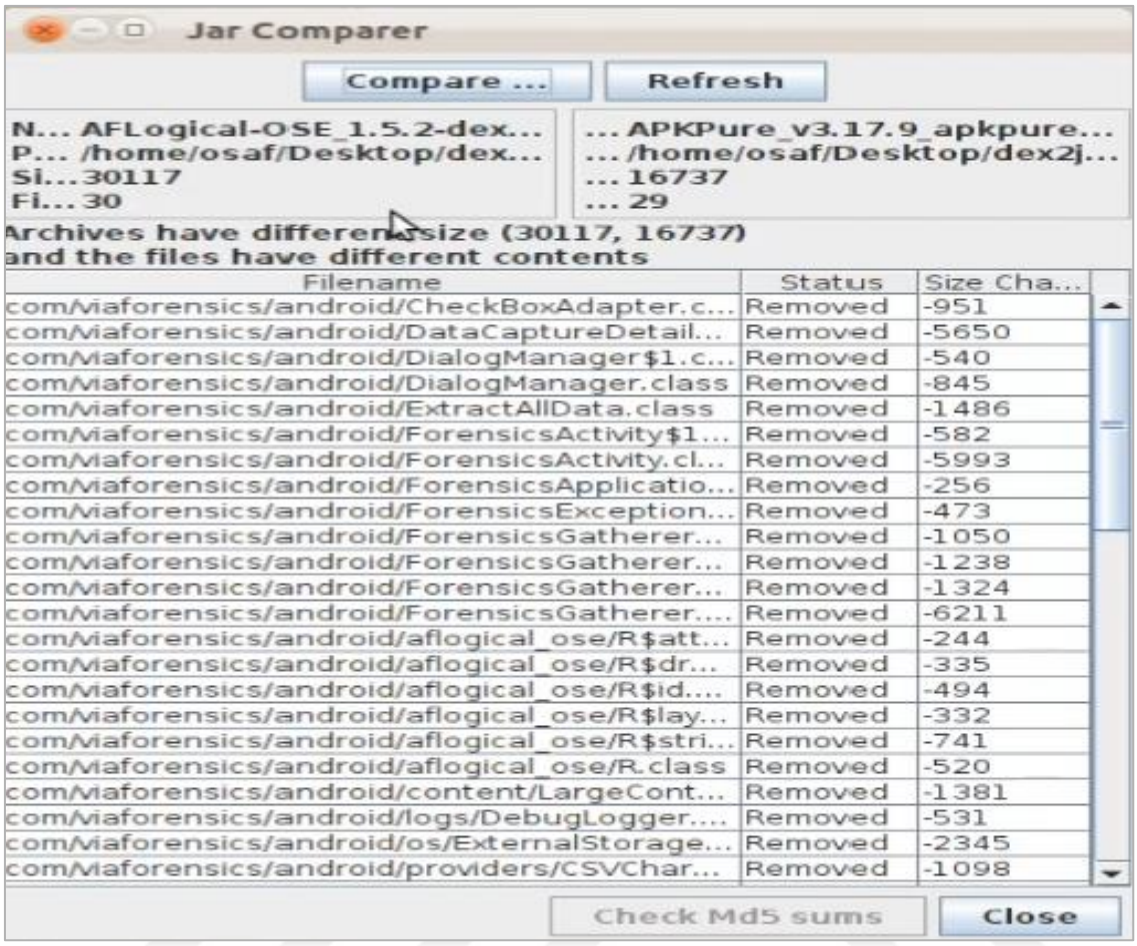


Resim 5. 47. .apk dosyasının .class Java kodlarının incelenmesi

5.5.5.4. Jar Comparer İsimli Yazılım Aracıyla

Jar Comparer Uygulaması iki farklı .jar dosyası karşılaştırak .jar dosyaları içerisinde bulunan farklı dosyaları tespit etmektedir . Bu uygulama özellikle, Android bir cihazdan ele geçirilen .apk dosyasıyla, aynı .apk dosyasının Google Play'de bulunan .apk dosyasının karşılaştırılması ile .apk dosyaları arasında bir fark bulunup bulunmadığı ve de böylece ele geçirilen .apk dosyasının kötü amaçlı bir yazılım içerip içermediği tespit edilebilir. Örneğin hedef cihazdan elde edilen Whatsapp uygulamasının temel .apk dosyasıyla, Google Play'de bulunan aynı sürümü karşılaştırılarak herhangi bir şekilde adli bilişim incelemelerin baltalanmasının amaçlanıp amaçlanmadığı tespit edilebilir.

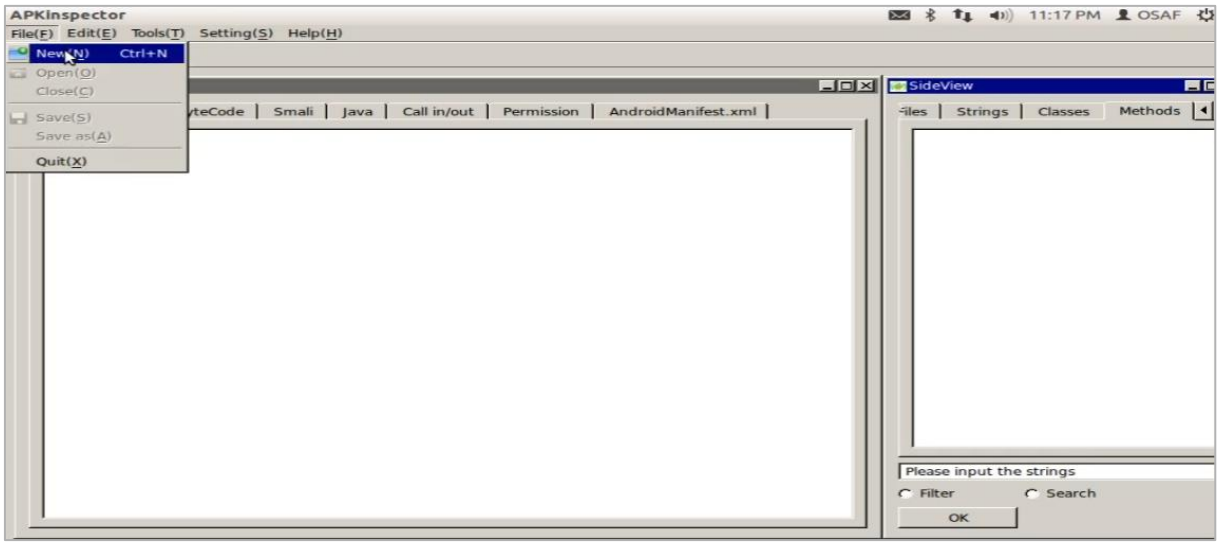
Jar Comparer Uygulaması da OSAF araç takımında masaüstündeki kısayoldan direkt olarak çalıştırılabilir. Resim 5.48'de tamamen farklı iki uygulamanın Jar Comparer aracıyla karşılaştırılması gösterilmiştir.



Resim 5. 48. İki farlı .apk dosyasına ilişkin .jar dosyalarının Jar Comparer ile karşılaştırılması

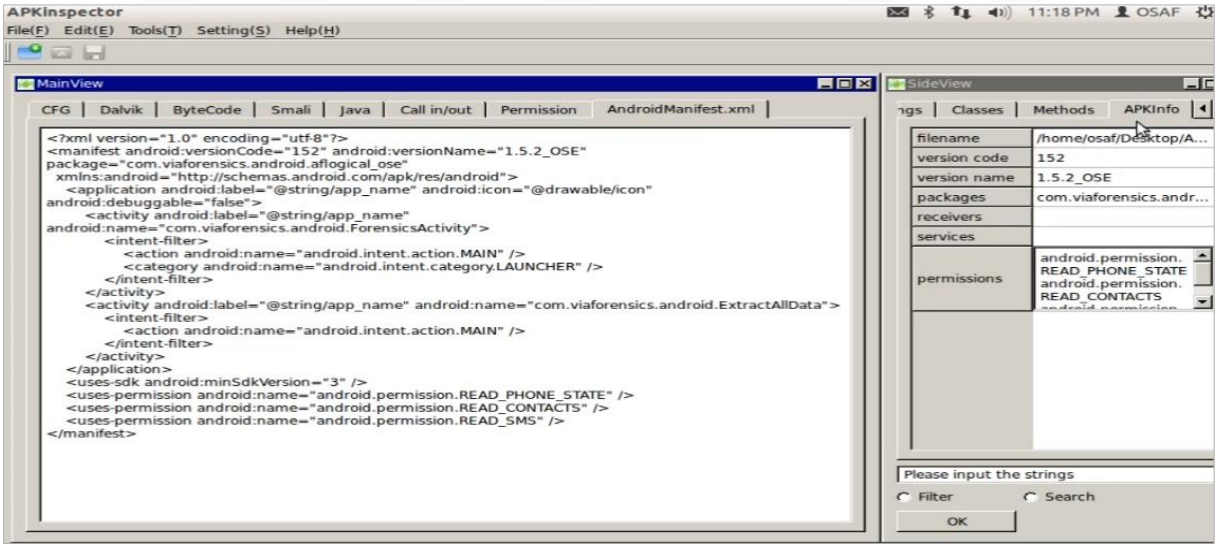
5.5.5.5. APK Inspector İsimli Yazılım Aracıyla

Apk Inspector Uygulaması da çok ayrıntılı bir şekilde .apk dosyalarının kodlamalarını göstermektedir (The Honeynet Project, 2013). Uygulamayı kullanırken Resim 5.49'daki gibi "File" seçeğininden "new" başlığı seçilip açılan pencerede incelenmek istenen .apk dosyası belirlenebilir.



Resim 5. 49. İncelenmesi arzu edilen .apk dosyasının seçilmesi

Bu uygulama ile .apk dosyasına ilişkin verilen izinler, "AndroidManifest.xml" dosyası, yöntem kuralları, Strings, CFG, Dalvik, Classes kodları gibi birçok bilgiler ayrıntı bir şekilde incelenebilmektedir. Resim 5.50'de AF Logical OSE isimli Android uygulamasının manifest.xml dosyasının analizi gösterilmiştir.



Resim 5. 50. Apk Inspector aracında incelenen örnek bir uygulama

5.6. Raporlama

Güzel bir şekilde neticelendirilmiş rapor; fotoğraflamaya, video kayıtlarına, notlara, dokümanlara ve araçların kullanılması ile oluşturulmuş kayıtlara dayanır. Bu raporlama ile elde edilen verilerin değişime uğramadığı ve doğruluğunun korunduğunun ispatlanması

oldukça önemlidir. Dolayısıyla yapılan tüm işlemlerinin her adımında not alınması, fotoğraflanma ve video kayıtlarıyla işlem adımların desteklenmesi oldukça önemlidir (Rick ve diğerleri, 2014).

Rapor genel olarak; raporu hazırlayan kurumun tanımlanmasını, ilgili soruşturma veya kovuşturma numarasını, inceleyici ve araştırmacıların tanımlanmasını, delillerin elde edilme tarihini, raporun düzenlenme tarihini, incelen cihazların marka, model, IMEI numarası gibi tanımlamalarını, analizcilerin imzasını, kullanılan yazılım araçları veya ekipmanlarını, inceleme aşamalarının özeti, delillerin dijital kopyasını, yapılan analiz işlemlerinin detaylı açıklamasını içermelidir. Analiz işlemlerin detaylı açıklamaları için talep edilen belirli dosya türleri, bulguları destekleyen silinmiş veriler de dahil olmak üzere diğer veriler, telefon sisteminde ve uygulamalarda yapılan arama kayıtları, internet tarayıcısı aktiviteleri, imajın görselleştirilmiş analizi, cihaz sahipliğini gösterir uygulamalara kayıt olma verileri dahil olmak üzere detaylar, imajdaki verilerin analizi, analiz edilen cihazdaki uygulamaların tanımlanması, gizlenmeye çalışılan verilerin gizlenme yöntemleri ile bu verilere nasıl ulaşıldığına ilişkin açıklama bilgileri sayılabilir (Rick ve diğerleri, 2014).

Elde etme, erişim, aktarma ve muhafaza süreçlerinin tümünde yapılan işlemler raporlanmalı ve potansiyel bir incelemeye hazır bulundurulmalıdır. Elde etme sırasında olay yerinde fotoğraflamalar ve video kaydına alma işlemleri gerçekleştirilmelidir. Son olarak ise, analizcilerin uygun eğitimi almış olması ve böylece başka bir analizci tarafından aynı prosedürlerin takip edilmesi halinde aynı sonuçların alınarak analizin doğrulanması mümkün olmalıdır. Aynı zamanda ele geçirilen akıllı telefonun imajının alınması ve cihazdaki verilerin incelenip analiz edilmesi işlemleri en kısa sürede yerine getirilmelidir. Aksi takdirde akıllı telefonun üzerindeki verilerin değiştirildiği iddiası gündeme gelebilecektir (Androulidakis, 2012: 75-99).

Zira Eoghan Casey de, raporlamanın her adım için çok kritik olduğunu, yapılan her işlemin ve işlemin oluşturduğu değişiklerin not edilmesi gerektiğini belirtmektedir (Casey, 2009a: 25).

Böylelikle elde edilen verilerin doğruluğu, bütünlüğü ve hukukiliği açısından herhangi bir aykırılık bulunup bulunmadığı tartışılabilir olmalıdır. Yargılama sırasında kendisini savunan bir sanık veya müdafii bu unsurlarının raporda bulunmaması halinde, elde edilen delillerdeki verilerin her türlü şüpheden uzak ve cezalandırmaya yeterli bir delil olmadığı yönünde savunma yapabilecektir.

5.7. Hukuki Boyutu

Türk Ceza Hukuku'nda adli bilişim ile ilgili başlıca düzenleme 5271 sayılı Ceza Muhakemesi Kanunu madde 134'de yapılmıştır (CMK, 2004).

Açık bir tanımlamanın bulunmaması ve madde lafzında bilgisayar kavramının kullanılması sebebiyle teknik bilgisi yetersiz bir kişi tarafından 5271 sayılı Ceza Muhakemesi Kanunu m.134'ün akıllı telefonlara uygulanamayacağı iddia edilebilir. Ancak akıllı telefonlar da kişisel bilgisayarlara birçok açıdan benzeyen özelliklere sahiptir. Nitekim kişisel bilgisayarlarla yapılabilecek tüm işlemlerin neredeyse akıllı telefonlar vasıtasıyla da gerçekleştirilmesi mümkündür (Doğanay, 2019). Zira Yargıtay 17. Ceza Dairesi de akıllı telefonların işlev itibariyle bilgisayar niteliğinde olduğunu ve CMK m.134 bağlamında adli bilişim incelemelerinin gerçekleştirilmesi gerektiğini belirtmiştir (*Y. 17. CD 2015/27517 E. 2017/1716 K.,* 2017). Kaldı ki akıllı telefon teknolojisinin gelişmesiyle beraber akıllı telefonlar; kimi kişisel bilgisayarlardan dahi daha güçlü geçici belleğe, depolama alanına veya işlemci gücüne sahip olabilmektedirler.

CMK m.134/1'de, bilgisayar ve bilgisayar kütüklerinde aramanın ancak bir soruşturma ile kuvvetli suç şüphesinin varlığı ve başka suretle delil edilmesi imkanının bulunmaması halinde gerçekleştirilebileceği belirtilmiştir. Bu bağlamda eğer elde edilen deliller bağlamında suç sübuta eriyor ya da kamera kayıtları, darp raporları, tanık anlatımları, şüphelinin ikrarı gibi delillerle şüpheye yer bırakmayacak biçimde maddi gerçeğe ulaşmak mümkünse akıllı telefonların adli bilişim bağlamında incelenmemesi gerekmektedir. Şüphelinin akıllı telefonu üzerinde yapılacak adli bilişim incelemesinin özel hayatına büyük oranda müdahale oluşturması nedeniyle şüphelinin kendisini savunması kapsamında incelemenin gerçekleştirilmesini istemesi hali dışında, akıllı telefonların incelenmesine en son çare olarak başvurulması temel hak ve özgürlükleri bağlamında daha yerinde olacaktır.

Akıllı telefonlara ilişkin arama yapılması sırasında, uygulamada genellikle Cumhuriyet Savcısının Kararı ile hareket edilmektedir. Bu durum çoğu zaman bu cihazlar üzerinde hukuka aykırı aramalar yapılmasına sebebiyet vermektedir. Nitekim Cumhuriyet Savcısının Kararı ile cihazlara el konulması yahut cihazlardaki verilerin kopyalanabilmesi için gecikmesinde sakınca bulunan hal mevcut olmalıdır. Gecikmesinde sakınca olmayan hallerde dahi Savcılık Kararı ile hareket edilebilmektedir.

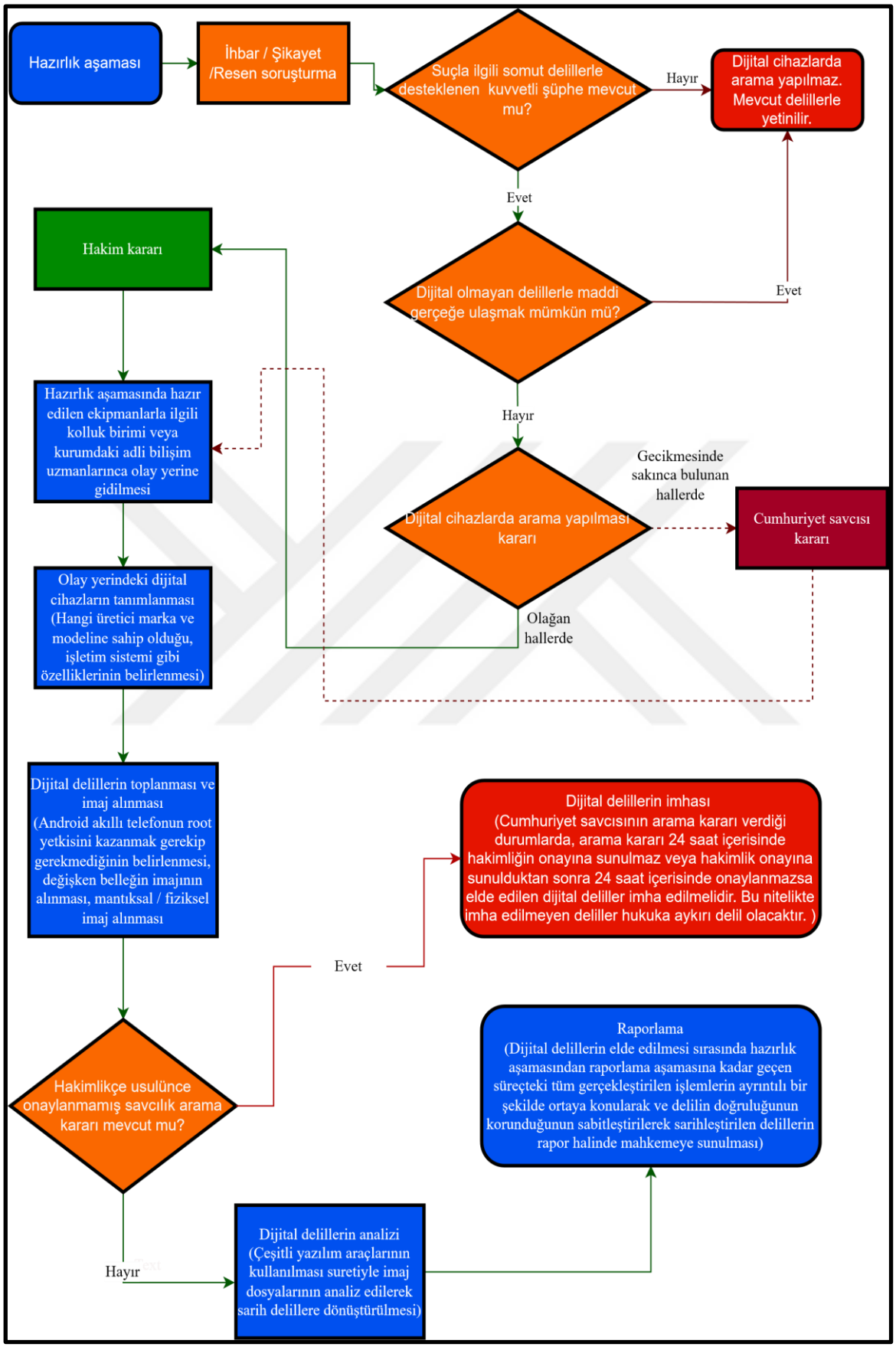
Yargıtay Ceza Genel Kurulu gecikmesinde sakınca bulunan hale ilişkin, derhal arama işlemi yapılmaması ve hakimlikten karar alınmasının beklenmesi halinde arama işleminin mümkün

olmayacak veya hiçbir faydası kalmayacak durumda olması söz konusuysa, gecikmesinde sakınca bulunan hal bulunduğunu kabul etmektedir. Böyle bir durum mevcut değilken, Cumhuriyet savcısı kararıyla arama işlemi yapılması halinde arama neticesinde delillerin hukuka aykırı delil niteliğinde olacağı, bu şekilde gerçekleştirilen aramaya sonradan hakim kararıyla onay verilmesi halinin de aramayı hukuka uygun hale getirmeyeceği belirtilmiştir (*YCGK 2016/75 E. 2019/18 K.,* 2019).

Yine Yargıtay Ceza Genel Kurulu, aramanın kural olarak gündüz yapılması gerektiğini, gecikmesinde sakınca bulunan hallerde ise gece de arama yapılabileceğini belirtmiştir (*YCGK 2016/57 E. 2016/374 K.,* 2016). Yargıtay 7. Ceza Dairesi ise, aramanın aciliyetine ilişkin hiçbir gerekçe bulunmadan gündüz vakti Cumhuriyet savcısının kararıyla arama yapılması neticesinde elde edilen delillerin hukuka aykırı olduğunu belirtmiştir (*Y. 7. CD 2014/30389 E. 2016/9769 K.,* 2016).

Ayrıca CMK m.134/1 uyarınca gecikmesinde sakınca bulunan halin varlığı durumunda Cumhuriyet savcısının kararıyla akıllı telefonda arama yapılması halinde ise, Cumhuriyet savcısının kararı yirmi dört saat içerisinde hakim onayına sunulmalıdır. Hakimliğin onay vermemesi veya hakim onayına sunulmaması halinde, ele geçirilen deliller derhal imha edilmelidir.

Hazırlık aşamasından raporlama aşamasına kadar ilgili yargılama makamlarıyla farklı durumlarda nasıl hareket edilmesi gerektiği Şekil 5.2'de gösterilmiştir.



Şekil 5. 2. Adli bilişim süreci akış çizelgesi

Uygulamada hukuka aykırı olarak gerçekleştirilen bir diğer işlem ise, el koymanın koşulları oluşmadığı halde cihazlara el konulmasıdır. Nitekim CMK m.134/2, *"Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir."* hükmüne amirdir.

Madde lafzından anlaşılacağı üzere; her durumda alelade şekilde cihazlara el koymak mümkün değildir. Akıllı telefonlara el koymak için akıllı telefondaki uygulama veya uygulama verilerine şifrenin çözülememesinden dolayı erişilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması hallerinin bulunması gereklidir. Yine el koymanın amacı, şifrenin çözülmesi ve akıllı telefonunun imajının alınması olmalıdır. Nitekim mezkur maddenin beşinci fıkrasında el koymadan da cihazlardaki verilerin tamamının veya bir kısmının kopyasının alınabileceği belirtilmiştir.

Bununla beraber CMK m.134/4 uyarınca, el koyma işlemi sırasında sistemdeki tüm verilerin yedekleri alınarak, bu yedeğin bir kopyasının şüpheli veya vekiline verilmesi gerektiği öngörülmüştür. Ancak pratikte bunun uygulanması oldukça güçtür. Nitekim akıllı telefondaki verilerin kopyasının alınmasında güçlüklerle karşılaşılması nedeniyle cihaza el konulabileceği CMK m.134/2'de belirtilmiştir. Bu güçlükler el konulma sırasında halen mevcutken verilerin bir yedeğinin de şüpheliye verilmesi genellikle mümkün olmayacaktır. Bu bağlamda CMK m.134'te yapılan düzenlemenin, kendi içerisinde çeliştiği söylenebilir.

Yine şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, gecikme olmaksızın cihazların iade edilmesi gerekirken; uygulamada cihazlar uzun seneler boyunca adli emanette kalabilmektedir.

Bununla beraber pratikte kolluk kuvvetleri şüpheli üzerinde baskı kurmak suretiyle; ele geçirilen cihazın şifresinin kendilerine söylenerek şifrenin geçilmesini istemektedirler. Ancak bu durum da şüphelinin kendini savunma, kendi aleyhine beyanda bulunmama hakkını ihlal etmektedir. Kişinin kendi rızası ve doğru iradesiyle pek tabi ki şifre bilgisini kolluk görevlilerine yahut inceleyicilere vermesi mümkündür. Bu halde hukuka aykırılık oluşmayacaktır.

Nitekim CMK m.48 uyarınca hiç kimse kendisi ve yakını aleyhine tanıklık yapmaya zorlanamaz. CMK 147/1-e maddesinde belirtilen susma hakkının bir tezahürü olan bu 48. maddeden anlaşılacağı üzere kimse kendisi veya yakını aleyhine delil vermeye zorlanamaz. Şifre bilgisinin şüpheliden zor ve baskı kullanmak suretiyle alınması halinde şüphelinin savunma hakkının kısıtlanması söz konusu olacağından ele geçirilen veriler hukuka aykırı delil niteliğinde olacaktır.

6. SONUÇ VE ÖNERİLER

Android akıllı telefonlarda her ne kadar temelde aynı işletim sistemini kullanılsa da bu akıllı telefonların birçok farklı üreticisi bulunmaktadır. Bu nedenle donanım ve üreticilerin kendisinin özelleştirmeleriyle oluşturdukları sistem alanı (ROM) birçok açıdan farklılaşabilmektedir. Ayrıca Android işletim sistemi, cihazların donanımları, üreticilerin kendi özelleştirdikleri sistem alanı, işletim sistemine özgü uygulamalar sürekli gelişmekte ve güncellenmektedir. Android işletim sistemi her güncellenmesinde açıklarını kapatarak güvenlik seviyesini artırmaktadır. Bu durum Android akıllı telefonların adli bilişim incelemesinin yapılmasını güçleştirmektedir. Nitekim mobil adli bilişimi, bu gelişmelere ayak uyduramamaktadır. Bilhassa Android akıllı telefonların adli bilişim incelemesinin etkili bir şekilde yerine getirebilmesi için root yetkisinin kazanılması, büyük önem arz etmektedir. Ancak mezkur gelişmeler, root yetkisinin kazanılması zorlaştırmakta ya da root yetkisi kazanılsa dahi hedef cihazdaki tüm verilerin silinmesi gündeme gelebilmektedir. Android işletim sisteminin mimarisi hakkında bilgi sahibi olmak, bu telefonları incelerken daha etkili hareket etmeyi sağlayacaktır. Android akıllı telefonların incelenmesi sırasında tek bir araç kullanmak çoğu zaman yetersiz olacaktır. Bu sebeple birden fazla aracın bir arada kombine şekilde kullanılması, daha etkili neticeler alınmasını sağlayacaktır. Nitekim bu çalışmada da imaj alınması ve analizlerin yapılabilmesi için birçok farklı açık kaynak kodlu araç kullanılarak adli bilişim pratiğine yardımcı olacak bir eser meydana getirilmiştir. Yine incelemeyi gerçekleştirirken hukuka aykırılık oluşturmayacak şekilde hareket etmek, oldukça önemlidir. Aksi halde Android akıllı telefonlardan elde edilen deliller, hukuka aykırı delil niteliğinde olabilecektir. Android akıllı telefonlar incelenmesi sırasında root yetkisinin kazanılması halinde, bu yetkinin kazanılmasına ilişkin tüm işlemler her adımda raporlanmalıdır. Root yetkisini kazanma işleminin geri alınabilmesi mümkün olmalıdır. Android akıllı telefonların incelenmesindeki tüm aşamalarda yapılan işlemler, en son aşamada oluşturulan raporda yer tutmalıdır. Zira adli bilişim bilimi, soruşturma ve kovuşturma dosyalarına delil sağlama amacında olduğundan bu bağlamda oluşturulan raporlar adli bilişim biliminin bel kemiği niteliğindedir. Bu çalışmada Android akıllı telefonların adli bilişim incelemesi yöntemlerinin bu cihazlardan veri elde etme bağlamında, Android akıllı telefonların yazılımsal ve donanımsal gelişmeleri bakımından çok daha geride kaldığı neticesine varılmıştır. Her ne kadar mezkur akıllı telefonlardan elde edilen verileri analizini sağlamaya birçok yönden çözüm sunan araçlar bulunsa da bilhassa yazılım araçları ile veri elde etme yönünden yeni metotlar geliştirilmesi gerekmektedir.

KAYNAKLAR

İnternet: 504ENSICS Labs. (2014). *LiME (linux memory extractor)*. 504ENSICS Labs. URL: https://github.com/504ensicsLabs/LiME, Son Erişim Tarihi: 15 Aralık 2022.

İnternet: *Activity*. (2022). Android Developers. URL: https://developer.android.com/reference/android/app/Activity, Son Erişim Tarihi: 17 Aralık 2022.

Ahmed, R., & Dharaskar, R. V. (2008). Mobile forensics: An overview, tools, future trends and challenges from law enforcement perspective. *6th international conference on e-governance, iceg, emerging technologies in e-government, m-government*, 312-323.

Akalın, U. (2016). *Mobil cihazlarda adli bilişim çalışmalarına yönelik bir model önerisi*. Gazi Üniversitesi Bilişim Enstitüsü.

Akarawita, I., Perera, A., & Atukorale, A. (2015, Ağustos 24). *ANDROPHSY - forensic framework for Android*. https://doi.org/10.1109/ICTER.2015.7377696

Akgül, H. (2014, Mayıs 13). *Samsung S5660 Galaxy Gio Root Yapma*. URL: https://www.ceplik.com/samsung-s5660-galaxy-gio-root-yapma/, Son Erişim Tarihi: 28 Kasım 2022.

Alamin, A. A. M., & Mustafa, A. B. A. (2015). A survey on mobile forensic for android smartphones. *IOSR Journal of Computer Engineering (IOSR-JCE), 17*(2), 15-19.

Almehmadi, T., & Batarfi, O. (2019). Impact of android phone rooting on user data integrity in mobile forensics. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1-6.

İnternet: *Android (operating system)*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Android_(operating_system)&oldid=1126863711, Son Erişim Tarihi: 17 Aralık 2022.

İnternet: *Android Runtime*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Android_Runtime&oldid=1119960029, Son Erişim Tarihi: 17 Aralık 2022.

İnternet: *Android-backup-toolkit*. (2022). SourceForge. URL:https://sourceforge.net/projects/android-backup-toolkit/, Son Erişim Tarihi: 21 Aralık 2022.

Androulidakis, I. I. (2012). Mobile phone forensics. *Mobile Phone Security and Forensics* (ss. 75-99). Springer.

Aneeshya Rose K. M. (2020). *Android Binder IPC Framework*. PathPartnerTech. URL: https://www.pathpartnertech.com/android-binder-ipc-framework-scatter-gather-optimization/, Son Erişim Tarihi: 17 Aralık 2022.

Årnes, A. (2018). The identification phase. *Digital forensics*. John Wiley & Sons.

Aydoğan, H. (2009). *Adli bilişim'de yeni elektronik delil elde etme yöntemleri,* Yüksek Lisans Tezi, Polis Akademesi Güvenlik Bilimleri Enstitüsü, Ankara, 16.

Ayed, A. B. (2015). A literature review on android permission system. *International Journal of Advanced Research in Computer Engineering & Technology*. https://www.academia.edu/42250747/A_literature_Review_on_Android_Permission_System

İnternet: *Bada*. (2022). Wikipedia. URL:https://en.wikipedia.org/w/index.php?title=Bada&oldid=1116429362, Son Erişim Tarihi: 16 Aralık 2022.

Baggili, I. M., Mislan, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence*, *6*(2), 168-178.

Başlar, Y. (2019). Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri. *TBB Dergisi*, *2020 (148)*.

Baştürk, İ. (2014). The Road Map for Digital Forensic Law of Turkey. *Proceding Book*, 124.

Bijoy Boban. (2014). *An analysis on iphone and smart phone forensics*.

İnternet: *BlackBerry OS*. (2022). Wikipedia. URL:https://en.wikipedia.org/w/index.php?title=BlackBerry_OS&oldid=1123078506, Son Erişim Tarihi: 16 Aralık 2022.

Boueiz, M.-R. (2020). Importance of rooting in an Android data acquisition. *2020 8th international symposium on digital forensics and security (ISDFS)*, 1-4.

Brahler, S. (2010). Analysis of the android architecture. *Karlsruhe institute for technology*, *7*(8).

İnternet: Brian Carrier. (2021). *Autopsy*. Autopsy. URL: https://www.autopsy.com/about/, Son Erişim Tarihi: 21 Aralık 2022.

İnternet: Brignoni, A. (2022). *ALEAPP* [Python]. URL: https://github.com/abrignoni/ALEAPP, Son Erişim Tarihi: 21 Aralık 2022.

İnternet: *Broadcast overview*. (2022). URL: https://developer.android.com/guide/components/broadcasts, Son Erişim Tarihi: 17 Aralık 2022.

Bucak, Y. (2019). *Adli bilişim ve türk ceza muhakemesi hukukunda bilgisayarda arama*, Yüksek Lisans Tezi, Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü, İstanbul, 17-18.

Casey, E. (2009a). Applying the scientific method to digital forensics. *Handbook of digital forensics and investigation*. Academic Press.

Casey, E. (2009b). *Handbook of digital forensics and investigation*. Academic Press.

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

Casey, E. (2011b). Digital evidence in the courtroom. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Casey, E. (2011c). Digital investigation process models. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Ceza Muhakamesi Kanunu, Resmi Gazete (25673) (2004). https://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1

Chao Wang, Wei Duan, Jianzhang Ma, & Chenhui Wang. (2011). The research of android system architecture and application programming. *Proceedings of 2011 International Conference on Computer Science and Network Technology*, 785-790. https://doi.org/10.1109/ICCSNT.2011.6182081

İnternet: *Content Providers*. (2022). URL: https://developer.android.com/guide/topics/providers/content-providers, Son Erişim Tarihi: 17 Aralık 2022.

Doğanay, H. A. (2019). *Mobil adli bilişiminin önemi bağlamında hukuki süreç ve delil zinciri kavramı ile yeni nesil mobil cihazların incelenmesinde karşılaşılan güncel zorlukların değerlendirilmesi*, Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 16.

İnternet: *Eclipse 3 Pro Kit*. (2022). OffGrid. URL: https://offgrid.co/products/eclipse-3-pro-kit, Son Erişim Tarihi: 18 Aralık 2022.

İnternet: Ekizer, A. H. (2014). *Adli Bilişim (Computer Forensics)*. URL: https://www.ekizer.net/adli-bilisim-computer-forensics/, Son Erişim Tarihi: 22.12.2022.

Feng, P., Li, Q., Zhang, P., & Chen, Z. (2019). Private data acquisition method based on system-level data migration and volatile memory forensics for android applications. *IEEE Access*, *7*, 16695-16703.

İnternet: *Firefox OS*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Firefox_OS&oldid=1115961802, Son Erişim Tarihi: 16 Aralık 2022.

Ghosh, A., Majumder, K., & De, D. (2021). Android forensics using sleuth kit autopsy. *Proceedings of the Sixth International Conference on Mathematics and Computing*, 297-308.

İnternet: Haiyu Yang. (2022). *AMExtractor*. URL: https://github.com/ir193/AMExtractor, , Son Erişim Tarihi: 15.12.2022.

Hoog, A. (2011). *Android forensics: investigation, analysis and mobile security for Google Android*. Elsevier.

Huang, D., & Wu, H. (2018). Virtualization. *Mobile Cloud Computing* (ss. 31-64). Elsevier. https://doi.org/10.1016/B978-0-12-809641-3.00003-X

Induruwa, A. (2009). Mobile phone forensics: An overview of technical and legal aspects. *International Journal of Electronic Security and Digital Forensics*, *2*(2), 169-181.

İnternet: *iOS*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=IOS&oldid=1125166909, Son Erişim Tarihi: 16 Aralık 2022.

İnternet: James, J. I. (Direktör). (2021). *Fast Android forensic triage with ALEAPP*. URL: https://www.youtube.com/watch?v=_cm1n0stVrA, Son Erişim Tarihi: 20 Aralık 2022.

İnternet: Java Decompiler. (2015). *JD-GUI* [Java]. Java Decompiler. URL: https://github.com/java-decompiler/jd-gui, Son Erişim Tarihi: 22 Aralık 2022.

İnternet: KBase. (2022). *Whatsapp Xtract* [Python]. URL: https://github.com/kbaseio/Whatsapp-Xtract, Son Erişim Tarihi: 21 Aralık 2022.

Khan, J., & Shahzad, S. (2015). Android architecture and related security risks. *Asian J. Technol. Manag. Res.[ISSN: 2249–0892]*, *5*, 14-18.

Kılıç, M. S. (2012). *İşletim sistemlerinin adli bilişim açısından incelenmesi*, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara,1.

Kim, D., & Lee, S. (2020). Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Science International: Digital Investigation*, *33*, 200897.

Küçükyılmaz, T. C. (2015). *Android ART nedir ve nasıl açılır*. Teknoloji Haberleri - ShiftDelete.Net. URL:https://shiftdelete.net/android-art-nedir-ve-nasil-acilir-57368, Son Erişim Tarihi: 17 Aralık 2022.

İnternet: *LiMo OS*. (2022). URL: https://www.gsmarena.com/glossary.php3?term=limo-os, Son Erişim Tarihi: 16 Aralık 2022.

Lin, X. (2018). Android forensics. *Introductory Computer Forensics* (ss. 335-371). Springer.

Lutes, K. D., & Mislan, R. P. (2008). Challenges in Mobile Phone Forensics. *Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA)*.

İnternet: *Maemo*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Maemo&oldid=1121888890, Son Erişim Tarihi: 16 Aralık 2022.

Marturana, F., Me, G., Berte, R., & Tacconi, S. (2011). A quantitative approach to triaging in mobile forensics. *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 582-588.

İnternet: Mauricio Piacentini, Raquel Ravanini, Jens Miltner, Pete Morgan, René Peinthor, & Martin Kleusberg. (2021). *About—DB Browser for SQLite*. URL: https://sqlitebrowser.org/about/, Son Erişim Tarihi: 21 Aralık 2022.

İnternet: *MeeGo*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=MeeGo&oldid=1117215902, Son Erişim Tarihi: 16 Aralık 2022.

Mehrotra, T., & Mehtre, B. M. (2013). Forensic analysis of Wickr application on android devices. *2013 IEEE International Conference on Computational Intelligence and Computing Research*, 1-6.

Mirza, M. M., Salamh, F. E., & Karabiyik, U. (2020). An android case study on techical anti-forensics challenges of whatsapp application. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-6.

Mosa, M. J. (2018). *Theory and Practice of Forensics Techniques for Smart Phones*, Master's thesis, Al-Azhar University Master of Computing & Information Systems, Egypt, 12-13.

MRKAIĆ, I. (2016). Android forensic using some open source tools. *The Eighth International Conference on Business Information Security (BISEC-2016), Belgrade, Serbia,, 15th October*.

Nimodia, C., & Deshmukh, H. R. (2012). Android operating system. *Software Engineering*, *3*(1), 10.

İnternet: OSAF Community. (2015). *Open source android forensics toolkit*. SourceForge. URL: https://sourceforge.net/projects/osaftoolkit/, Son Erişim Tarihi: 22 Aralık 2022.

İnternet: Pan, B. (2015). *Dex2jar* [Java]. URL: https://github.com/pxb1988/dex2jar, Son Erişim Tarihi: 22 Aralık 2022.

Pandiyan, D., & Paranjape, S. (2012). *Android architecture and binder*.

Petraityte, M., Dehghantanha, A., & Epiphaniou, G. (2017). Mobile phone forensics: An investigative framework based on user impulsivity and secure collaboration errors. *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (ss. 79-89). Elsevier.

İnternet: *Platform architecture*. (2021). Android Developers. URL: https://developer.android.com/guide/platform, Son Erişim Tarihi: 17 Aralık 2022.

İnternet: RealityNet. (2022). *Android Triage* [Shell]. RealityNet. URL:https://github.com/RealityNet/android_triage, Son Erişim Tarihi: 21 Aralık 2022.

Rick, A., Sam, B., & Jansen, W. (2014). Guidelines on mobile device forensics. *National Institute of Standards and Technology, US Department of Commerce. National Institute of Standards and Technology. Retrieved*, *6*(17), 2014.

Roy, N. R., Khanna, A. K., & Aneja, L. (2016). Android phone forensic: Tools and techniques. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 605-610.

Saraydere, İ. (2018). *Dijital delillere ilk müdahale, imaj alma ve inceleme süreçleri*, Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyonkarahisar, 26-27.

Skulkin, O., Tindall, D., & Tamma, R. (2018). *Learning android forensics: Analyze android devices with the latest forensic tools and techniques*. Packt Publishing Ltd.

Song, M., Xiong, W., & Fu, X. (2010). Research on architecture of multimedia and its design based on android. *2010 International Conference on Internet Technology and Applications*, 1-4.

İnternet: StatCounter. (2022). *Operating system market share worldwide*. StatCounter Global Stats. URL: https://gs.statcounter.com/os-market-share, Son Erişim Tarihi: 9 Aralık 2022.

İnternet: *Symbian*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Symbian&oldid=1126173736#Version_history, Son Erişim Tarihi: 16 Aralık 2022.

Tayeb, H. F., & Varol, C. (2019). Android mobile device forensics: A review. *2019 7th international symposium on digital forensics and security (ISDFS)*, 1-7.

İnternet: The Honeynet Project. (2013). *Apk Inspector* [Java]. The Honeynet Project. URL: https://github.com/honeynet/apkinspector, Son Erişim Tarihi: 22 Aralık 2022.

İnternet: *Tizen*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Tizen&oldid=1127194434, , Son Erişim Tarihi: 16 Aralık 2022.

İnternet: Tumbleson, C. (2022). *Apktool* [Java]. URL: https://github.com/iBotPeaches/Apktool, Son Erişim Tarihi: 22 Aralık 2022.

Umale, M. M. N., Deshmukh, A. B., & Tambhakhe, M. D. (2014). Mobile phone forensics challenges and tools classification: A review. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(3), 622-626.

Umar, R., Riadi, I., & Muthohirin, B. F. (2019). Live forensics of tools on android devices for email forensics. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 17*(4), 1803-1809.

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Digital Investigation, 14*, S77-S84.

İnternet: *WebOS*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=WebOS&oldid=1124710375, Son Erişim Tarihi: 16 Aralık 2022.

What are the differences between Dalvik and ART? (2019). URL: https://blog.mindorks.com/what-are-the-differences-between-dalvik-and-art, Son Erişim Tarihi: 17 Aralık 2022.

İnternet: *Windows Mobile*. (2022). Wikipedia. URL: https://en.wikipedia.org/w/index.php?title=Windows_Mobile&oldid=1126860730, Son Erişim Tarihi: 16 Aralık 2022.

Y. 7. CD 2014/30389 E. 2016/9769 K., (Yargıtay 7. Ceza Dairesi 29 Eylül 2016).

Y. 17. CD 2015/27517 E. 2017/1716 K., (Yargıtay 17. Ceza Dairesi 15 Şubat 2017).

Yang, H., Zhuge, J., Liu, H., & Liu, W. (2016). A tool for volatile memory acquisition from android devices. *IFIP International Conference on Digital Forensics*, 365-378.

YCGK 2016/57 E. 2016/374 K., (Yargıtay Ceza Genel Kurulu 18 Ekim 2016).

YCGK 2016/75 E. 2019/18 K., (Yargıtay Ceza Genel Kurulu 17 Ocak 2019).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : YILDIRIM, Tayfun

Uyruğu : T.C.

Doğum Yeri :

E-posta :

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Adli Bilişim	Devam Ediyor
Lisans	Çankaya Üniversitesi / Hukuk Fakültesi	2018

İş Deneyimi

Yıl	Yer	Görev
2019-Halen	Kendi Hukuk Bürosu	Avukat
2018-2019	Muhtelif Hukuk Büroları	Stajyer Avukat

Yabancı Dili

İngilizce

GAZİLİ OLMAK AYRICALIKTIR.