T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ANDROİD CİHAZLARDA ZARARLI YAZILIM ANALİZİNİN ADLİ BİLİŞİM BAKIMINDAN GERÇEKLEŞTİRİLMESİ

Özge GÜNAY

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği Bilim Dalı

ARALIK 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

ANDROİD CİHAZLARDA ZARARLI YAZILIM ANALİZİNİN ADLİ BİLİŞİM BAKIMINDAN GERÇEKLEŞTİRİLMESİ

Tez Yazarı
Özge GÜNAY

Danışman
Doç. Dr. Fatih ERTAM

ARALIK 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Android Cihazlarda Zararlı Yazılım Analizinin Adli Bilişim Bakımından Gerçekleştirilmesi
Yazarı:	Özge GÜNAY
İlk Teslim Tarihi:	28.11.2022
Savunma Tarihi:	28.12.2022

TEZ ONAYI

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

		İmza
Danışman:	Doç. Dr. Fatih ERTAM Fırat Üniversitesi Teknoloji Fakültesi	Onayladım
Başkan:	Dr. Öğr. Üyesi Mustafa KAYA Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Hafzullah İŞ Batman Üniversitesi, Mühendislik Fakültesi	Onayladım

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

İmza

Prof. Dr. Burhan ERGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Android Cihazlarda Zararlı Yazılım Analizinin Adli Bilişim Bakımından Gerçekleştirilmesi" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

28.12.2022

Özge GÜNAY

ÖNSÖZ

Bu tez çalışmasının gerçekleştirilmesinde, bilgilerini benimle paylaşan, nasıl bir yol izlemem gerektiği konusunda bana yön veren, yardımlarını esirgemeyen, gelecekteki mesleki hayatımda verdiği bilgilerden faydalanacağımı düşündüğüm değerli hocam Sayın Doç. Dr. Fatih ERTAM' a, Fırat Üniversitesi Adli Bilişim Mühendisliğinde görevli olan değerli hocalarıma ve bana her zaman destek olan aileme, arkadaşlarıma sonsuz teşekkür ederim.

Bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **TEKF.21.36** protokol numaralı proje ile desteklenmiştir.

Özge GÜNAY
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Android Cihazlarda Zararlı Yazılım Analizinin Adli Bilişim Bakımından Gerçekleştirilmesi

Özge GÜNAY

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Aralık 2022, Sayfa: xii + 53

Teknolojinin ilerlemesiyle beraber günümüzde gerçekleştirilen siber suçlar saldırganlar tarafından saldırı vektörleri kullanılarak kullanıcının mobil cihazında çeşitli işlemler yapabilmektedir. Mobil cihaz türlerinden biri olan Android cihazlar, Android işletim sistemindeki zayıflıklardan, uygulama mağazasındaki zafiyetlerden kaynaklı kolayca istismar edilebilmektedir. Adli soruşturmalar için büyük verileri bulunduran Android cihazlardaki zararlı yazılımların adli bilişim bakımından incelenmesi önem arz etmektedir. Android cihazların, uygun adli bilişim araçları ile adli kopya alma, inceleme ve analiz süreçlerinin gerçekleştirilmesi soruşturmaların açığa çıkmasına katkı sağlamaktadır. Bu nedenle, uzmanların Android cihazları inceleyen adli bilişim araçları hakkında yeterli bilgiye, donanıma ve tecrübeye sahip olması gerekmektedir. Android cihazların sürekli olarak kendini güncellemesi, yeni özelliklerin eklenmesi nedeniyle Android cihazları inceleyen adli bilişim araçlarının güncel sürümlerinin kullanılması gerekmektedir. Yapılan tez çalışmasında, saldırgan bakış açısıyla sızma testi senaryoları gerçekleştirilerek teknik ve teori bilgilere yer verilmiş olup Android cihazda zararlı yazılım analizinin adli bilişim bakımından incelenmesi gerçekleştirilmiştir. Android cihazda zararlı yazılım analizinin adli bilişim bakımından gerçekleştirilmesi noktasında en az iki mobil adli bilişim yazılımı ile mantıksal ve fiziksel imaj yöntemi ile incelenmesi önerilmektedir. Zararlı yazılımlara ait bulgu tespit edildiği noktada manuel inceleme yöntemi tercih edilerek zararlı uygulamaların statik ve dinamik analizinin gerçekleştirilmesi gerektiği kanısına varılmaktadır.

Anahtar Kelimeler: Mobil Adli Bilişim, Android Adli Bilişim, Zararlı Yazılım

ABSTRACT

Performing Malware Analysis on Android Devices in terms of Forensics

Özge GÜNAY

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

December 2022, Pages: xii + 53

With the advancement of technology, today's cybercrimes can be performed by attackers using attack vectors on the user's mobile device. Android devices, one of the mobile device types, can be easily exploited due to weaknesses in the Android operating system and vulnerabilities in the application store. For forensic investigations, it is important to examine malicious software on Android devices with large data in terms of forensic information. Performing forensic copying, examination and analysis processes of Android devices with appropriate forensic tools contributes to the disclosure of investigations. For this reason, experts should have sufficient knowledge, equipment and experience about forensic tools that examine Android devices. Due to the constant updating of Android devices and the addition of new features, it is necessary to use the current versions of forensic tools that examine Android devices. In the thesis study, technical and theoretical information was given by performing penetration test scenarios from the perspective of the attacker, and the analysis of malware on the Android device was carried out in terms of forensic computing. At the point of performing malware analysis on Android device in terms of forensics, it is recommended to examine at least two mobile forensic software with logical physical image method. It is concluded that static and dynamic analysis of malicious applications should be performed by choosing the manual examination method at the point where the findings of malicious software are detected.

Keywords: Mobile Forensics, Android Forensics, Malware

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

ADB	: Android Debug Bridge
iOS	: iPhone Operating System
ITU	: International Telecommunication Union
NIST	: National Institute of Standards and Technology
RAM	: Random Access Memory
SIM	: Subscriber Identification Memory
URL	: Uniform Resource Locator
OFD	: Oxygen Forensic Detective

1. GİRİŞ

Günümüzde işlenen suçlar teknolojinin gelişmesiyle beraber üretilen cihazlar yoluyla dijital ortamlarda gerçekleşmektedir [1]. Dijital ortamlarda bilişim sistemleri aracılığıyla işlenen suçlar; ileri teknoloji, bilişim, siber ve bilgisayar suçları şeklinde adlandırılmaktadır. Bilgileri otomatik işleme tabi tutan veya verilerin taşınmasına sebep olan sisteme karşı gayri kanuni ahlakdışı ve yetkisiz icra edilen her türlü davranış 'Bilişim Suçu' olarak tanımlanmaktadır [2].

Dijital ortamlarda işlenen suçların oluşmasına sebep olan cihazlar ve bu cihazlar içerisindeki veriler ise 'dijital/elektronik delil' olarak adlandırılmaktadır. Dijital ortamlarda gerçekleşen suçların, elektronik deliller kullanılarak aydınlatılması disiplinine 'Adli Bilişim' denilmektedir [1]. Dijital ortamlarda gerçekleşen adli suçlarda, suç unsurunun olup olmadığını tespit etmek için adli bilişim incelemeleri yapılmaktadır. Adli bilişim incelemeleri, dijital/elektronik cihazların ve bilişim sistemlerinin dâhil olduğu adli suçlarda adli bilişim disiplininin oluşmasını sağlamaktadır [3]. Adli bilişim alanı teknoloji ilerledikçe akademik ve teknik çalışmalar ile hızlı bir şekilde büyüme göstermektedir. Adli bilişim alanı geliştikçe bu alanda yapılan ekonomik harcamalar istatistiklere de yansımaktadır. Adli bilişim incelemelerinde tercih edilen yazılım, donanım ve servis hizmetleri gibi alanlarda kullanılan ekonominin büyüklüğü 2017 yılında 4,62 milyar dolar seviyelerindeyken, 2022 yılına kadar yıllık %15,9 büyüme oranı ile 9,68 milyar dolar seviyelerine kadar geleceği tahmin edilmektedir [3]. Adli bilişim alanının gün geçtikçe gelişmesi nedeniyle incelenen cihaza göre; bilgisayar adli bilişimi, dosya sistem adli bilişimi, ağ adli bilişimi, mobil cihaz adli bilişimi, sosyal ağ adli bilişimi, ses adli bilişimi ve bulut adli bilişim gibi farklı türlere ayrılmaktadır [1].

Dijital ortamlarda işlenen suçların oluşmasında kullanılan mobil cihazlar 'mobil adli bilişim' türünün ortaya çıkmasına sebep olmuştur. Mobil cihazlar, her türlü yazılım, donanım ve teknoloji ile geliştirilerek kullanıcılar tarafından tercih edilen, bilgi ve iletişim çağı olarak adlandırılan günümüz dünyasına yön veren en önemli ürünlerden biri haline gelmiştir [4]. Mobil teknolojilerin ilerlemesiyle birlikte başta akıllı cep telefonları ve tabletler olmak üzere mobil cihazların kullanımının yaygınlaştığı görülmektedir. Ünlü araştırma şirketi Gartner'ın mobil ve kablosuz ağ teknolojilerine ilişkin raporunda, kullanıcıların mobil cihazlara yönelik kullanım eğilimlerinin mobil teknolojilerin gelişmesiyle beraber giderek artacağını tahmin etmektedir [5]. Hayatımıza giren mobil cihazlar başta akıllı telefonlar olmak üzere tabletler, taşınabilir bilgisayarlar, giyilebilir cihazlar; iletişimden sosyal yaşama, eğitimden sağlığa her türlü alanda kullanılmaktadır. Mobil cihazların istenilen işlemleri yapabilme kabiliyetlerinden dolayı kullanıcılar tarafından tercih edilmektedir. Mobil cihazlar; genel olarak kullanım biçimleri, sahip oldukları donanımlar ve işletim sistemleri bakımından sınıflandırılmaktadırlar [6]. Kullanıcılar tarafından günümüzde tercih edilen tablet, telefon gibi farklı çeşitlerdeki dijital cihazların yapısında bulunan, bu cihazlar için yazılım kodlarından oluşturulan işletim sistemleri 'mobil işletim sistemi' olarak adlandırılmaktadır [7].

Mobil cihazlarda; Apple iOS, Google Android, BlackBerry OS, Nokia'nın Symbian'ı, Hewlett-Packard'ın webOS'u (eski adıyla Palm OS) ve Microsoft'un Windows Phone OS'si gibi birçok mobil işletim sistemi bulunmaktadır [7]. Ünlü araştırma şirketi Gartner'a göre kullanıcılar tarafından Android işletim sistemi cep telefonlarında, iOS işletim sistemi ise tabletlerde daha fazla tercih edildiğini söylemektedir. İşletim sistemlerinin pazar payı oranlarına bakıldığında mobil cihazlarda, Android ve IOS işletim sistemlerinin daha fazla tercih edildiği görülmektedir [8]. Mobil cihaz türlerinden biri olan akıllı telefonlar ise internete bağlanabilen, kullanıcılar tarafından indirilebilen bazı uygulamaları destekleyen mobil cihaz türü olarak tanımlanmaktadır [9]. Akıllı telefonların kullanıcı dostu olmaları, daha hızlı bağlantı sağlayabilmeleri, uygulamaları destekleyebilmeleri, işlem hızında artış göstermeleri ve sahip oldukları özellikleri geliştirmeleri nedeniyle günümüzde akıllı telefon kullanıcı sayısı artış göstermektedir. Teknoloji ilerledikçe akıllı telefonlara cihaz şifrelemesi, gizlilik oluşturma gibi daha fazla özellik eklenmeye devam etmektedir. Teknolojinin ilerlemesiyle beraber akıllı telefonların destekledikleri uygulamalarda gelişim göstermektedir. IDC Araştırma anketine göre 2022'nin birinci çeyreğinin sonunda pazar payına göre ilk beş akıllı telefon satıcısı %24 oranıyla Samsung, %18,2 oranıyla Apple, %16,1 oranıyla Huawei, %13 oranıyla Xiaomi ve %10 oranıyla Oppo olduğunu tespit etmiştir. Aynı anket, 2022 akıllı telefon piyasasının %31,6'sını oluşturan 'diğer' akıllı telefon satıcılarından oluştuğunu tespit etmiştir [10].

Mobil adli bilişim, adli bilişimin bir dalı olarak öngörülen ve uygun bilimsel adli koşulları kullanarak mobil cihazlardan dijital delillerin kurtarılması olarak tanımlanmaktadır. Mobil cihazların kullanıcı sayısının artması, mobil adli bilişim alanının giderek karmaşık bir disiplin haline gelmesine sebep olmuştur [11]. Adli suçlarda kullanılan mobil cihazlar; arama geçmişleri, mesajlar, fotoğraflar, videolar, silinmiş veriler, sosyal medya uygulamaları, depolama alanları gibi soruşturma süreçlerinde ve güvenlik analizlerinde adli delil olabilecek yüksek veri kaynağına sahiptir [12]. Özellikle mobil cihaz türlerinden biri olan akıllı telefonlar; iletişim aracı olarak kullanılması, kullanıcı bilgilerini içermesi, suçu teşkil eden kanıtları depolaması ve suç işlenmesinde bir araç olarak kullanılmasından dolayı soruşturma süreçlerinin bir parçası haline gelmiştir [6]. Analistler, kolluk kuvvetleri, adli bilişim uzmanları; adli suçların işlenilmesinde kullanılan mobil cihazlardan veri elde etme ve analiz etme işlemini gerçekleştirmektedir. Mobil cihazlarda kullanılan teknolojinin çeşitliği, dijital delillerin biriktirilmesi, standartlaştırılmış veri çıkarma metodolojilerinin eksikliği gibi sebepler analistlerin mobil cihazlardan dijital delilleri elde edebilmeleri için zorluk oluşturmaktadır [11]. Mobil cihazların delil olabilecek çok fazla veri türünü içermesi ve bu delillerin silinme ihtimalinin olmasından dolayı analistlerin mobil cihaz incelemelerini belirli bir süreç (koruma, ele geçirme, inceleme, raporlama) dahilinde gerçekleştirmesi gerekmektedir. Mobil cihazı inceleyecek analistlere; gerekli eğitimlerin verilmesi, mobil incelemede kullanılacak gerekli yazılım (Encase, Oxygen Forensic, MOBILEdit, Paraben,

Cellebrite, Salvationdata SPF vb.) ve donanımların temin edilmesi ve mobil adli bilişim süreci hakkında yeterli tecrübeye sahip olmaları gerekmektedir [13].

Mobil cihaz işletim sistemlerinden biri olan Android işletim sistemine sahip Android cihazlar kullanıcılar tarafından tercih edilerek yüksek pazar payı oranına sahip olmuştur. Bu bağlamda günümüzde saldırganlar tarafından kullanıcıların kullandığı Android cihazlar da hedef odağı olmaktadır. Saldırganlar tarafından Android cihazda depolanan ve aktarılan verilere yetkisiz erişim elde etmeye çalıştığı birçok potansiyel saldırı vektörü bulunmaktadır. Saldırganlar tarafından çeşitli yöntemler (uygulama/işletim sistemlerindeki güvenlik açıklığı, sosyal mühendislik) ile kullanıcının cihazına bulaşan Ransonware(fidye yazılımı), trojan(truva atı), virüs, worm gibi çeşitli zararlı yazılımlar Android cihazın kontrolünü ele geçirerek saldırgan tarafından istenilen aksiyonlar alınabilmektedir[14]. Bu bağlamda kullanıcıların olası saldırıya karşı farkındalığının oluşturulması, cihaz üzerinde gerekli antivirüs programlarının kullanılması, doğrudan Android paket yükleyicilerinin(apk) indirilmemesi, Android uygulama izinlerine dikkat edilmesi, veri kaybını engellemek için yedekleme işlemlerinin yapılması gibi aksiyonlar alınarak güvenliğin sağlanması gerekmektedir [15].

Kullanıcılar tarafından kullanılan Android cihazlar, dijital ortamlarda işlenen suçlarda yüksek delil niteliğinde verileri bünyesinde bulundurmaktadır. Adli vakalarda delil niteliği olan Android cihazlara zararlı uygulamaların yüklenerek kullanıcının haberi olmaksızın saldırganlar tarafından eylemlerin gerçekleştirilmesi muhtemeldir. Bu sebeple analistlerin, adli bilişim uzmanlarının; zararlı yazılım türlerini, davranışlarını bilmekle beraber Android cihaza bulaşmış zararlı uygulamanın analiz edilmesiyle ilgili teknikler hakkında bilgi sahibi olması gerekmektedir. Analistler, adli bilişim uzmanları tarafından adli suçların çözülmesinde, Android cihazlarda zararlı yazılım analizinin adli bilişim bakımından gerçekleştirilmesi büyük katkı sağlamaktadır [16].

Literatür araştırmasında Android cihazlarda zararlı yazılım analizi konusunda geliştirilen yöntemler, zararlı yazılım tespiti için yaklaşımlar, korunma sistemleri gibi çeşitli çalışmalar bulunmaktadır. Bu çalışmalardan bazıları aşağıda açıklanmıştır.

Mert Can Coşguner tarafından kum havuzu tasarlanarak zararlı yazılımların tespiti hybrid, statik ve dinamik analiz yöntemleri ile yapılabilmektedir. Kum havuzu yöntemiyle analiz edilen Android uygulama statik analiz, dinamik analiz ve raporlama adımlarından geçmektedir. Analistler tarafından incelenen Android uygulamalardan zararlı olabileceğinin tespiti statik/dinamik analiz ile elde edilen bulgular raporlanabilmektedir [17].

F. Tong ve arkadaşları tarafından yapılan çalışmada net_link teknolojisi kullanılarak zararlı yazılım ve zararsız uygulamaların örnekleri alınarak statik ve dinamik analiz yöntemleri benimsenmiş olup yeni bir hybrid yaklaşım önerilmiştir. Hybrid yaklaşım ile statik ve dinamik analize göre zararlı yazılımın tespit edilmesinin daha başarılı bir şekilde gerçekleştirildiğinin sonucuna varılmıştır [18].

P. Teulf ve arkadaşları tarafından yapılan çalışmada Android platformlar üzerinden gerçekleşen zararlı yazılımların algılanması ve analiz edilmesi ile ilgili çalışmalar yapılmıştır. Yapılan çalışma sonucunda Google Play Store üzerinden alınan uygulamaların meta verilerine dayanan çeşitli örnekler sunularak yeni yöntemler gösterilmiştir [15].

Sercan Türker tarafından yapılan çalışmada makine öğrenmesi tabanlı sistem ile zararlı olan Android yazılımların ait oldukları aile tahmin edilebilmektedir. Tasarlanan sistem farklı sınıflandırma algoritmalarını kullanarak Android yazılımların API çağrılarını, izinlerini tespit etmesiyle beraber zararlı yazılımların sınıflandırılmasını gerçekleştirebilmektedir [19].

D. Klein ve arkadaşları tarafından Context Statik analizi, program kaynak kodunu veya bayt kodunu ayrıştıran tekniklerden yararlanarak program özelliklerini kontrol etmek için program yollarından geçmektedir. Android uygulamalarının güvenliğini değerlendirmek, uygulama klonlarını tespit etmek, test senaryoları oluşturmayı otomatikleştirmek veya performans ile ilgili işlevsel olmayan sorunları ortaya çıkarmak için farklı görevler içeren statik analiz yaklaşımları önerilmiştir [20].

Günümüzde gerçekleşen siber suçlara baktığımızda zararlı yazılımlar geliştirilerek kullanıcının mobil cihazında çeşitli işlemler yapılabilmektedir. Adli soruşturmalarda büyük rol oynayan Android cihazda zararlı yazılımın varlığının tespit edildiği noktada delil olabilecek verilerin; bozulmadan, silinmeden imaj alma, inceleme çalışmalarının uygun adli bilişim yazılımları kullanılarak gerçekleştirilmesi gerekmektedir. Yeterli delillerin elde edilememesi ihtimalinde riskli olmasına karşın Android cihazın manuel olarak incelenmesi gerçekleştirilerek zararlı yazılımın davranışsal analizinin yapılması soruşturmanın açığa kavuşturulmasına katkı sağlayabilmektedir. Bu bağlamda Android cihazlarda zararlı yazılım analizinin incelenmesi gerçekleştirilirken adli bilişim araçlarının performansları açısından yeterli bilgiye sahip olup, uygun araçlar ile incelemenin yapılması gerekmektedir.

2. MOBİL CİHAZLARDA ADLİ BİLİŞİM

Mobil cihazlar, teknolojinin ilerlemesiyle beraber sahip oldukları özellik ile bilgisayarların gerçekleştirdiği işlemleri yapabilmektedir. Aynı zamanda mobil cihazların ebat olarak küçük, taşınabilir olması nedeniyle de kullanıcılar tarafından tercih edilmektedir [4]. Bu cihazlar iletişim kurmak için kullanıldığı gibi internete erişmek, ses ve kamera kaydı yapmak, sosyal ağlar aracılığı ile fotoğraf, video, konum, ses kaydı, herhangi bir not paylaşmak için de kullanılabilmektedir. Genel olarak bakıldığında bir mobil cihaz arama geçmişi, e-posta, kısa mesaj, fotoğraf, video, takvim, hatırlatıcı not, konum bilgisi, uygulama verisi, şifre gibi birçok kişisel veri barındırmaktadır [27].

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

Adli bilişim uzmanlarının, mobil cihazların adli olarak incelenmesini doğru bir şekilde gerçekleştirilebilmeleri için; mobil cihaz türlerini, mobil cihazların işletim sistemlerini, mobil cihazların adli bilişim süreçlerini, mobil cihazlardan veri toplama türlerini, mobil cihazları inceleyen adli bilişim yazılımlarını ve mobil cihazların adli incelemesinde karşılaşabilecek sorunları bilmesi gerekmektediri

2.1. Adli Bilişim

Adli bilişim; adli makamlara başvurulan olayın bilişim yolu aracılığıyla gerçekleştirilmesi durumunda, suçun işlenilmesini sağlayan dijital/elektronik cihazların toplanılması, korunması, tanımlanması, kurtarılması, analiz edilmesi ve belgelenmesi süreci olarak tanımlanmaktadır [21]. Dijital/elektronik delil ise, elektronik cihazların veri depolama birimlerinde tutulan, suçun çözümlenmesine katkı sağlayan kanıt niteliğindeki verilerdir [22]. Kamu ve özel kuruluşlardaki verinin tamamına yakını elektronik ortamlarda saklanmaktadır. Bilgisayar Sistemleri, ağ araçları harddiskler, telefonlar, fotokopi makineleri, hafıza kartları, GPS, flash bellekler, erişim kontrol araçları gibi birçok araç gereç dijital delil niteliğinde olup mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanmaktadır. Elektronik deliller yapılarından dolayı kolayca değişebilmekte ve bozulabilmektedir. Bundan dolayı ele geçirilmiş veya el konulmuş elektronik cihazların korunması büyük önem arz etmektedir [23]. Adli bilişim süreci beş temel aşamadan oluşmaktadır.

Tanımlama: Olay esnasında kullanılan dijital kanıtların bulunduğu elektronik cihazlar incelenmek üzere belgelenir. Kanıt kaynağı olabilecek cihazlar arasında telefonlar, bilgisayarlar, harddiskler gibi araç gereçler sayılabilir.

Koruma: Olay yerini koruyarak, olay yerinin görsel görüntülerinin alınması, delillerin nasıl elde edildiğiyle ilgili bilgilerin belgelenmesi ve elektronik olarak saklanan ilgili bilgileri koruma sürecidir.

İnceleme: Elektronik cihazlarda bulunan kanıt niteliğindeki verilerin korunması, verilerin silinmesi veya kaybolması ihtimaline karşı; elektronik cihazların incelenmesini gerçekleştirebilmek için imaj (adli kopya) alma işleminin yapıldığı aşamadır.

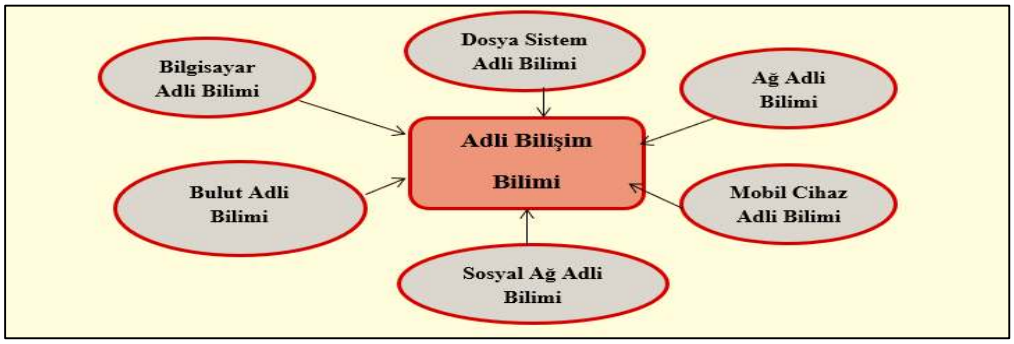
Analiz: Manuel veya adli bilişim araçları ile elektronik cihazdan oluşturulan adli kopya(imaj) dosyası üzerinden incelemelerin yapıldığı aşamadır.

Raporlama: Elektronik cihazın inceleme ve analiz işlemlerinden elde edilen delil niteliğindeki verilerin bilirkişi formatında raporlandırılmasıdır. Rapor dosyası iddialar yerine değerlendirmelerden oluşmalı aynı zamanda raporun anlaşılabilir şekilde yazılması gerekmektedir [22].

2.1.1. Adli Bilişim Türleri

Adli bilişim alanı; yaşanan suç olaylarında kullanılan kriptografik uygulamalar, teknolojilerin gelişmesi, kanunların bu teknolojilerdeki gelişmelere ayak uyduramaması gibi farklı sorunlar ile karşılaşabilmektedir. Adli bilişim bu nedenle; birçok alt disipline sahip, sürekli gelişen bir bilimsel alan olmasıyla birlikte adli bilişim çeşitli alt alanlara ayrılmıştır [24].

Adli bilişimin alanları Şekil 2.1'deki gibi sıralanabilir.



Şekil 2.1. Adli Bilişim Türleri

Bilgisayar Adli Bilişim: Dijital ortamlarda bilgisayarın kullanılmasıyla gerçekleştirilmiş suçların tespit edilmesi, çözümlenmesi bilgisayar adli bilişim türünü ortaya çıkarmıştır. Bilgisayar adli bilişiminde, suçun gerçekleştiği olay mevkisinde bulunan laptop, masaüstü bilgisayar gibi

cihazların korunması sağlanarak, bu cihazlardaki verilerin incelenmesi, analizlerinin gerçekleştirilmesi ve raporlandırılması işlemleri yapılır.

Bulut Adli Bilişim: Bulut sisteminden dijital adli bilgilerin toplanmasını sağlayıp verilerin delillendirilmesi işlemleridir. Bulut adli bilişimde; fiziksel ve sanal sunucuların, depoların, uygulamaların araştırılması gerekmektedir. Canlı sistemden alınan delil niteliğindeki verilerin minimum çaba ve maksimum hız ile alınması gerekir. Canlı sistemden alınan verilerin incelenmesi gerçekleştirilerek, gerekli delil niteliğinde olabilecek veriler mahkemeye sunulur.

Sosyal Ağ Adli Bilişim: Teknolojinin gelişmesiyle beraber sosyal medya uygulamalarındaki işlevsellikte gelişmeye başlamıştır. Sosyal medya araçları ile virüs yayma, dolandırma gibi suç faaliyetlerinin gerçekleştirilmesi sosyal ağ adli bilişim türünü ortaya çıkarmıştır. İşlenilen suçlar kapsamında, sosyal medya uygulamalarının adli bilişim açısından incelenmesi, analiz edilmesi delillerin açığa çıkmasına yardımcı olabilmektedir.

Ağ Adli Bilişim: Suçlular internet ağlarını kullanarak kurumun veya kişinin sistemine zarar verme, sisteme sızma gibi işlemleri yapabilmektedir. Bu nedenle internet ağlarının kullanılmasıyla işlenilen suçları çözümleyebilmek için ağ adli bilişim türü ortaya çıkmıştır. Ağ adli bilişimi; suçlular tarafından sızılmış sisteme ait logların, paketlerin ve bilgisayar sunucularının incelenmesi, analizinin gerçekleştirilmesi ve raporlandırılması aşamalarından oluşmaktadır.

Mobil Adli Bilişim: Mobil cihazların taşıdığı özelliklerin gelişmesiyle beraber, günümüzde mobil cihaz kullanıcı sayısında artış görünmektedir. Mobil cihazların taşınabilir olması, iletişimleri hızlı bir şekilde gerçekleştirebilmesi, fotoğraf/video gibi aktivitelerin yapılabilmesi gibi birçok özelliğe sahip olması nedeniyle kullanıcılar tarafından tercih edilmektedir. Mobil cihazlar tarafından gerçekleştirilen eylemlere ait veriler mobil cihazın depolama alanlarında bulunmakla beraber bu veriler silinip kaybolabilmektedir. Mobil cihazların depolama birimlerindeki verilerin kanıt niteliğinde olması, verilerin kurtarılması ve bu verilerin adli inceleme sürecine dahil olması mobil adli bilişim alanının oluşmasına sebep olmuştur [25].

2.2. Mobil Cihaz

Cep telefonları, tek amaçlı iletişim cihazlarından, kullanıcılarını çok çeşitli görevlerde destekleyen dinamik araçlara dönüşmüştür [26]. Günümüz dünyasında özellikle tablet ve cep telefonu gibi taşınabilir cihazlar her türlü yazılım, donanım ve teknoloji ile geliştirilerek kullanıcılar tarafından tercih edilmektedir [27]. Kullanıcılar tarafından tercih edilen mobil cihazlar ile mesajlaşma, arama yapma, sosyal medya kullanma, farklı uygulamaları indirme, fotoğraf/video çekme, yükleme gibi birden fazla kullanıcıya ait davranışlar gerçekleştirilmektedir. Bundan dolayı mobil cihazlar kullanıcıya ait kişisel bilgileri bünyesinde bulundurmaktadır [23]. Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından açıklanan bildiride Türkiye'de kullanıcıların mobil telefonu daha fazla tercih ettikleri açıklanmıştır. Bu nedenle BTK tarafından açıklanan rapora göre mobil telefonunun

sızma testi 70 milyona ulaşılacağı bildirilmiştir. Mobil cihazların gelişmesi aynı zaman güvenlik sorunlarının da ortaya çıkmasına neden olmuştur [28].

Mobil güvenlik problemleri; mobil cihazların sahip oldukları güvenlik mekanizmalarının yeterli olmaması nedeniyle mobil cihazın siber saldırılara maruz kalması, mobil cihazların siber saldırılardan korumak için gerekli anti virüs uygulamalarının yüklenmemesi, kullanıcıların mobil cihaza yapılacak siber saldırılar hakkında yeterli bilgiye sahip olmamasından dolayı her türlü mesaj, link gibi yerlere bilinçsizce girmeleri, kullanıcılar tarafından mobil cihazın güncellenmemesi, kullanıcılar tarafından yüklenilen uygulamaların virüsleri mobil telefona bulaştırması gibi açıklanabilir [29].

Yukarıda açıklandığı gibi, mobil cihazlar hayatımıza kolaylık sağlarken aynı zamanda güvenlik problemleri ile karşılaşılabilmektir. Bundan dolayı mobil cihazların güvenliğinin sağlanması amacıyla güvenlik mekanizmalarının geliştirilmesi, farklı güvenlik yollarının tespit edilmesi ve uygulanması gibi işlemlerin yapılması gerekmektedir [28].

2.2.1. Mobil Cihaz Türleri

Günümüzde mobil kullanıcılar; akıllı telefonlar, tabletler, akıllı saatler ve diğerleri dâhil olmak üzere çeşitli mobil cihaz türleriyle etkileşime girmektedir [9]. Mobil cihazlar; genel olarak kullanım biçimleri, sahip oldukları donanımlar ve işletim sistemleri bağlamında sınıflandırılmaktadır [9]. Günümüzde kullanılan mobil cihaz türlerinden bazıları aşağıdaki gibi açıklanmıştır.

Akıllı Telefonlar: Akıllı telefonlar; internete bağlanabilen, kullanıcılar tarafından yüklenebilen ve indirilebilen bazı uygulamaları destekleyen mobil cihazları tanımlamak için kullanılmaktadır [9].

Tabletler: Tabletler; telefonların mobil yetenekleri ile bilgisayarların işlem gücünü birleştirerek oluşturulmuş cihazlardır. Tabletlerin sahip oldukları özellikler incelendiğinde, telefon ve bilgisayarların gereksinimlerini yanıtlayabilmek için üretildiği söylenebilir [30].

Taşınabilir Bilgisayarlar: Taşınabilir bilgisayarlar; bir ekran ve klavye içeren bilgisayarların genel adıdır. Genel kullanıcı alışkanlıkları açısından ele alındığında günümüzde taşınabilir bilgisayarların çoğunlukla iş geliştirme süreçlerinde tercih edildiği görülmektedir. Akıllı telefon ve tabletler ile karşılaştıklarında kullanıcıları taşınabilir bilgisayarlara yönlendiren en büyük neden kuşkusuz performans ve işlevselliktir [31].

Giyilebilir Cihazlar: Giyilebilir cihazlar, akıllı sensörlerle oluşturulan vücut hareketlerini takip eden cihazlardır. Giyilebilir cihazlar, Wi-Fi ve mobil internet bağlantısını kullanarak akıllı telefonla kablosuz olarak senkronize olur. Giyilebilir cihazlara kullanıcılar sensörler yardımıyla bağlanır. Google Glass, akıllı saatler, Microsoft HoloLens, gözlükler, etkinlik izleyiciler vb. gibi ürünler giyilebilir cihazlara örnek olarak verilebilir [32].

2.3. Mobil Cihazların İşletim Sistemleri

Mobil işletim sistemleri; kullanıcılar tarafından günümüzde tercih edilen tablet, telefon gibi farklı çeşitlerdeki dijital cihazların yapısından bulunan, bu cihazlar için yazılım kodlarından oluşturulan işletim sistemleri olarak adlandırılmaktadır [33].

Cep telefonları için; kullanıcıların telefonları, kişisel bilgisayarların kullanıldığı şekilde kullanmalarını sağlamak için işletim sistemleri geliştirilmiştir. En iyi bilinen mobil işletim sistemleri Android, iOS, Windows telefon işletim sistemi ve Symbian'dır. Bu işletim sistemlerinin pazar payı oranlarına bakıldığında %47,51 ile Android, %41,91 ile iOS, %3,31 ile Symbian, %2,57 ile Windows phone işletim sistemi tercih edilmektedir. Daha az tercih edilen başka mobil işletim sistemleride bulunmaktadır. Az tercih edilen işletim sistemleri; Java Me Platform, Palm OS, Linux OS ve BlackBerry OS olarak bilinmektedir [34].

2.3.1. Java Me Platform

J2ME platformu, cep telefonları, çağrı cihazları ve kişisel düzenleyiciler gibi küçük cihazlar için geliştirilmiş bir dizi teknoloji, özellik ve kitaplıktır. Java ME, Sun Microsystems tarafından tasarlanmıştır. GNU Genel Kamu Lisansı altında lisanslanmıştır [35].

2.3.2. Palm OS

Palm işletim sistemi; yüksek performans, çoklu dokunma özelliği, parmak etkileşimi gibi özelliklere sahip olup birden çok uygulamanın çalışmasını sağlayan, uygulama uzmanları için üretilmiş Linux çekirdekli işletim sistemidir [33].

2.3.3. Symbian OS

Symbian OS, ARM mimarisinin farklı olarak çalışan 32 bit, küçük endian işletim sistemidir. C++ tabanlıdır. Çok görevli bir işletim sistemidir ve çevre birimlerine çok daha az bağımlıdır. Çekirdek ayrıcalıklı modda çalışır ve hizmetini kullanıcı kitaplıkları aracılığıyla kullanıcı uygulamalarına aktarır [35].

2.3.4. BlackBerry OS

BlackBerry bir akıllı telefon cihazıdır. 1999 yılında Research In Motion (RIM) tarafından piyasaya sürüldü. Piyasaya sürülmesinden bu yana, popülaritesi nedeniyle artmıştır. BlackBerry işletim sistemi, uygulama uzmanları için Windows bilgisayarlar ile uygulama geliştirebilmelerine imkan sağlayan, Java tabanlı işletim sistemidir [36].

2.3.5. Windows Mobile OS

Windows mobile işletim sistemi, Microsoft'un tasarladığı kompakt bir işletim sistemidir. Windows CE 5.2 çekirdeğini temel alan Windows mobile 6.5 sürümü, Microsoft Windows API kullanılarak geliştirilmiş bir dizi temel uygulama içerir. Özellik ve estetik açıdan Windows'un masaüstü sürümlerine benzer olacak şekilde tasarlanmıştır. Windows Mobile için 3. taraf yazılım geliştirme mevcuttur. Windows Mobile şu anda dünya çapında %8,8 paya sahiptir [37].

2.3.6. iOS

Mobil cihazlar için iOS, Apple Inc. tarafından yönetilen ve Apple donanımı için dağıtılan mobil işletim sistemidir. iPhone, iPad, iPod Touch ve Apple TV'ye güç sağlayan işletim sistemidir. Kapalı kaynak kodlu ve tescillidir ve açık kaynaklı Darwin çekirdek işletim sistemi üzerine kuruludur.
iOS, Mac OS X'ten türetilmiştir ve açık kaynaklı bir POSIX uyumlu UNIX OS olan temel Darwin temelini paylaşır. Bu anlamda iOS, UNIX'in bir çeşidi olarak kabul edilebilir. iOS; Şekil 2.2'de gösterildiği gibi Çekirdek işletim sistemi (Core OS), Çekirdek hizmetleri (Core Services), Medya servisleri (Media Services) ve Cocoa Touch olmak üzere dört katmandan oluşmaktadır [38].

Şekil 2.2. iOS İşletim Sistemi Mimarisi [38]

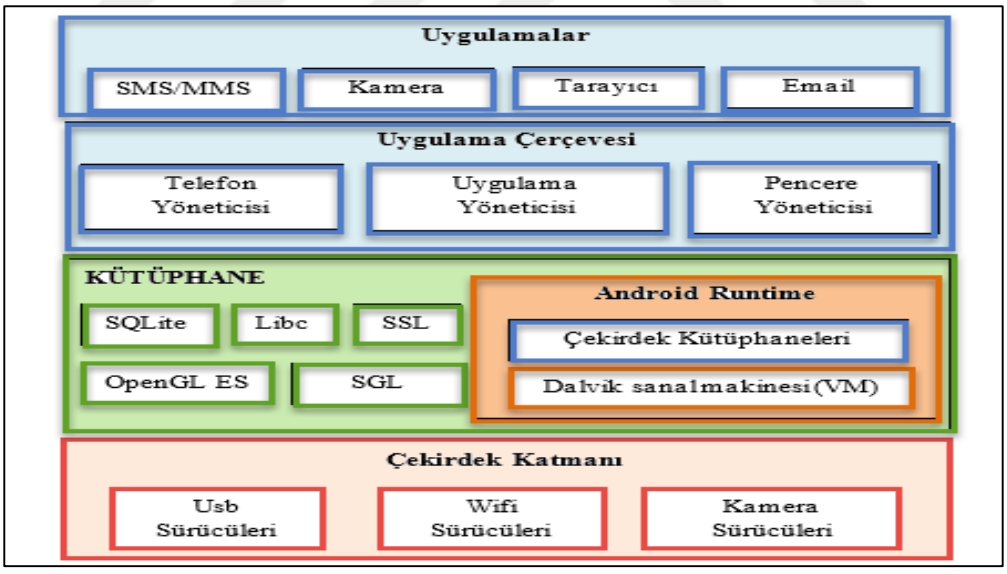
Çekirdek İşletim Sistemi (Core OS) Katmanı: Bu veri katmanı temel düşük seviye özellikler, sistem yönetimi, hafıza yönetimi, genel güvenlik servisleri, şifreleme, ses, görüntü işleme ve donanım yönetimini işlemlerini gerçekleştirir [38].
Çekirdek Hizmetleri (Core Services) Katmanı: Farklı çerçevelerde alt bölümlere ayrılarak temel sistem hizmetleri sunar. C tabanlı arayüzü ile dosya erişimini sağlar. Uygulama servisleri, ağ ve veri yönetimi, konum, takvim, etkinlikler, mağaza satın alma, SQLite ve XML gibi uygulamaların bulunduğu katmandır [38].
Medya Servisleri (Media Services) Katmanı: Uygulamaların ve video, ses gibi kütüphanelerin bulunduğu katmanıdır [38].

Cocoa Touch Katmanı: Kullanıcıya en yakın olan katmandır. Kullanıcı ile görsel iletişimin sağlandığı dokunmatik girişlerin algılandığı, ara yüz görünümlerinin bulunduğu katmandır.

2.3.7. Android OS

Open Handset Alliance'nın geliştirdiği, Google tarafından yönetilen mobil işletim sistemidir. Google, Kasım 2007'de Android dağıtımını açıklamıştır. Android çekirdeğinin çoğu açık kaynak Apache Lisansı altında yayınlanmıştır, ancak cihazlarda çok sayıda yazılım (Play Store, Google Play Hizmetleri, Google Müzik vb.) tescilli ve lisanslıdır [39].

Android işletim sisteminin yapısına bakıldığında uygulamalar, uygulama çerçevesi, kütüphaneler, Android runtime (Android çalışma zamanı) ve çekirdek katmanı olmak üzere 5 katmandan oluştuğu Şekil 2.3'te gösterilmiştir. C programlama dili ile kütüphaneler, API'ler ve katman yazılımları yazılmıştır. Java ile uyumlu kütüphaneleri bulunan uygulama mimarisinde, Apache harmony üzerine kurulu olan uygulama yazılımları çalışmaktadır. Android işletim sistemi, Dalvik sanal makinesi ile derlenmiş Java kodunu çalıştırabilmektedir. Bir milyondan fazla mobil uygulama, Android işletim sistemi tabanlı çalışmaktadır [8].



Şekil 2.3. Android İşletim Sistemi Mimarisi [8]

Linux Çekirdeği: Android, güvenlik, bellek yönetimi, süreç yönetimi ve benzeri gibi temel sistem hizmetleri için Linux'a güvenir [35].

Android Çalışma Zamanı: Java'nın çekirdek kitaplıklarındaki işlevlerin çoğunu destekleyen bir dizi çekirdek kitaplık sağlar. Dalvik VM olarak bilinen Android Sanal Makinesi, bazı temel işlevler için Linux çekirdeğine güvenir [35].

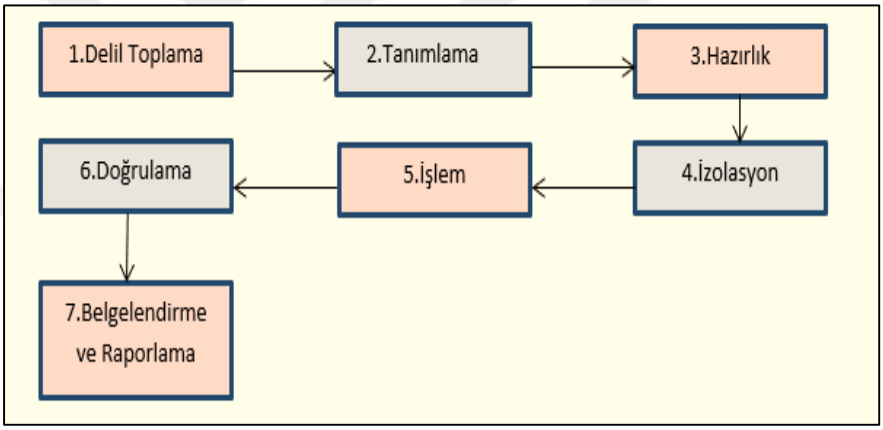
Kitaplıklar: Android, bir dizi C/C++ kitaplığı içerir. Bu kitaplıklar, Android uygulama çerçevesi aracılığıyla geliştiricilere sunulur. Medya kitaplıkları, sistem C kitaplıkları, yüzey yöneticisi, 3B kitaplıklar, SQLite vb. içerirler [35].

Uygulama Çerçevesi: Çekirdek uygulamalar tarafından kullanılan çerçeve API'lerine bir erişim katmanı sağlar. Bileşenlerin geliştiriciler tarafından kullanılmasına izin verir [35].

Uygulamalar: Java dili ile programlanmış Android uygulamalarının bulunduğu katmandır [35].

2.4. Mobil Cihazlarda Adli Bilişim Süreçleri

Dijital ortamlardan elde edilen kanıtların içerdiği verilerin değişmemesi, kanıtların korunması ve elde edilen kanıtların raporlama işlemini başarılı bir şekilde tamamlayabilmek için mobil cihazın adli bilişim aşamalarının belirli bir plan dahilinde gerçekleştirilmesi gerekmektedir [40]. Mobil cihazların adli bilişim aşamaları Şekil 2.4'te gösterildiği gibi yedi adımdan oluşmaktadır.



Şekil 2.4. Mobil Cihazlarda Adli Bilişim Aşamaları [41]

Delil Toplama Aşaması: İnceleme isteğinin işlendiği aşama, delil toplama aşaması olarak adlandırılmaktadır. Bu aşamada istek/talep formu, mobil cihazın suça karıştığı olay, mülkiyet gibi genel bilgilerin belgelenmesi işlemleri yapılmaktadır. İncelemenin bu safhasında incelenen her bir cihaz için inceleme sürecinin dokümantasyonu başlatılmış olur [41].

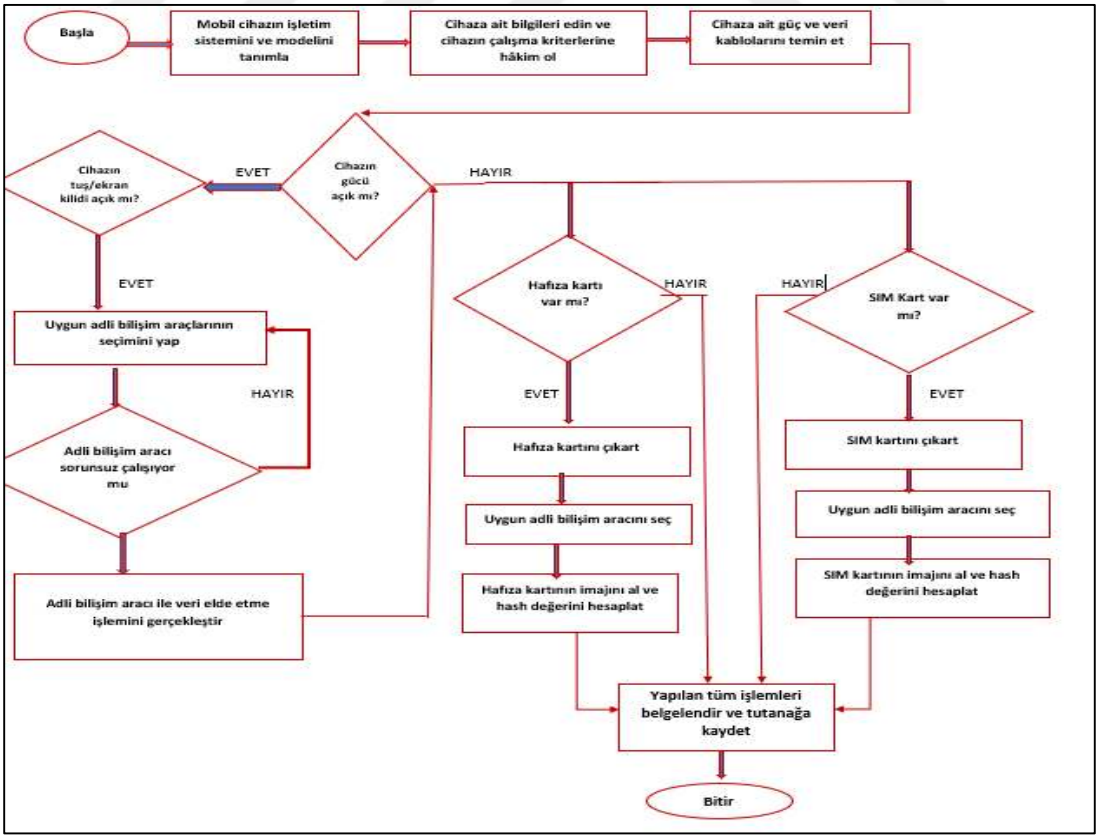
Tanımlama Aşaması: İnceleme uzmanı, her bir mobil cihaz incelemesinde cihazın incelenmesi için yasal yetkisini, inceleme amaçlarını, cihazlar için marka, model ve tanımlama bilgisini, çıkarılabilir ve harici veri saklama alanını tanımlamalıdır [38].

Hazırlık Aşaması: Hazırlık aşamasında, incelenecek mobil cihaz için inceleme sırasında izlenecek metotlar belirlenir ve kullanılacak araçların seçimi yapılır. Bu aşama ayrıca tüm ekipmanların, kabloların, yazılımların ve sürücülerin hazırlanması sürecini de içerir. Eğer kullanılacaksa medya

ve iş istasyonu inceleme için hazır hale getirilir ve kullanılacak araçların mümkünse en son sürümü temin edilir [27].

İzolasyon Aşaması: İzolasyon aşamasında, uzaktan erişim yolu ile delil niteliğindeki verilerin silinmesini, verilerin üzerine yazılmasını, gelen aramaları ve kısa mesajları engellemek gibi mobil cihazın sinyal bağlantılarının kesilmesi işlemi faraday çantaları kullanılarak yapılır [41].

Delil toplama, tanımlama, hazırlık ve izolasyon aşamaları koruma süreci olarak adlandırılmaktadır. İnceleme yerindeki kanıt niteliğindeki verilerin korunması işlemi koruma sürecinin temel hedefidir. Cihaz kullanıcısının parmak izlerinin korunması için analiz edilecek cihaz her zaman eldivenlerle kullanılmalıdır. Cihaz, ele geçirildiği durumda tutulmalıdır. Cihaz kapalıysa, kapalı kalmalıdır. Cihazın kapalı kalması; cihazın uçak moduna alınması, yeni aramaların, SMS'lerin alınmasını, GPS ile yeni güzergâh kayıtları oluşturmasını, analiz sürecinde yanlış pozitiflerin önüne geçilmesini ve hatta verilerin uzaktan silinmesini önlemek için de önemlidir. Aksi hallerde açık durumdaki cihaz kesinlikle kapatılmamalıdır. Cihaz açık durumda ise, cihazın verilerin alınacağı laboratuvara taşınması için bir faraday çantası kullanılmalıdır. Cihazın tüm özellikleri belgelenmeli ve kanıtların korunması sağlanmalıdır [11]. Mobil cihazların adli incelemede verilerin elde edilmesi işlemleri Şekil 2.5'teki adımlarla gerçekleştirilir [42].

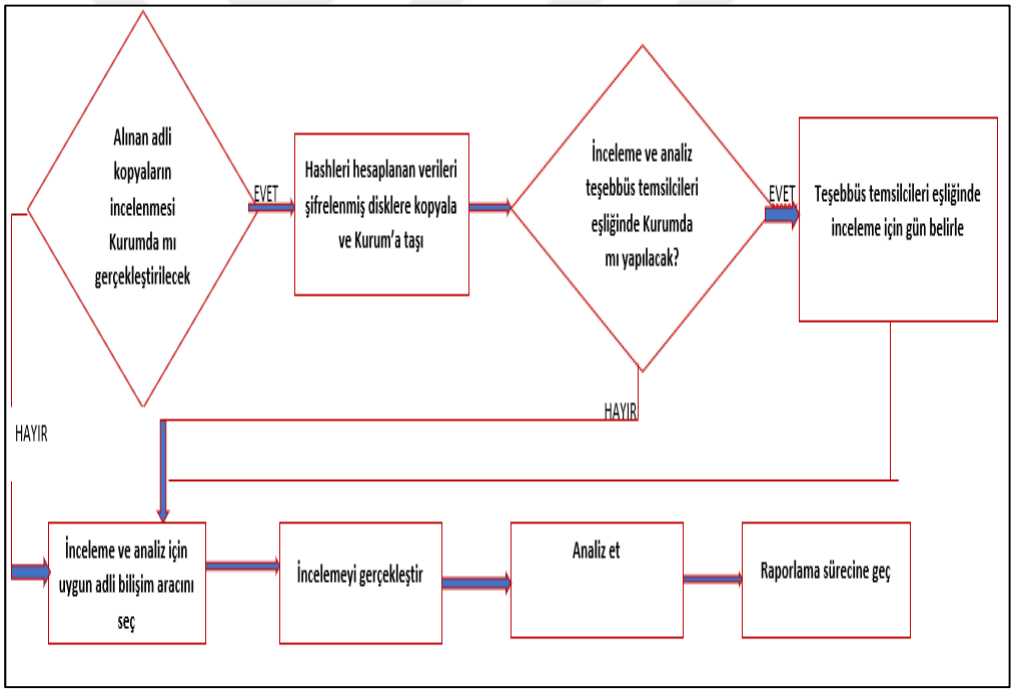


Şekil 2.5. Mobil Cihazlardaki Verilerin Elde Edilme Adımları [42]

İşlem Aşaması: Mobil cihazın izolasyon işlemleri tamamlandıktan sonra mobil cihazın işlenmesi aşamasına geçilir. Bu aşamada arzu edilen verilerin telefondan ayıklanması işlemleri gerçekleştirilir [41]. İşlem aşamasında, mobil cihazdan elde edilmiş olan verilerin özgünlüğünün bozulmaması için, mobil cihazdan elde edilmiş olan adli kopyalar(imajlar) üzerinde işlemlerin gerçekleştirilmesi gerekmektedir [42].

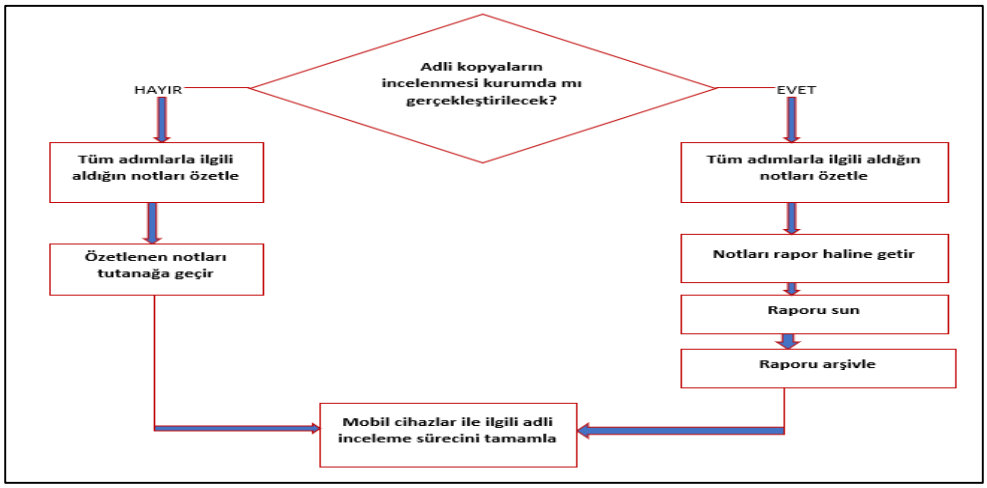
Doğrulama Aşaması: Telefonu işleme aşamasında sonra, inceleme uzmanının telefondan çıkarılan verileri doğrulamak için birtakım düzenlemeleri yapması şarttır. Ne yazık ki, cep telefonu araçlarının yanlışlıkla veya eksik bir şekilde verileri rapor etmesi veya çelişen bilgileri araçlardan birine bildirmesi alışılmadık bir durum değildir. Ayıklanan verilerin doğrulanmasının yapıldığı aşamadır [41].

Mobil cihazların işlem ve doğrulama aşamasında Şekil 2.6'da önerilen adımların izlenilmesi tavsiye edilmektedir [42].



Şekil 2.6. Mobil Cihazlar İçin Önerilen İşlem ve Doğrulama Süreci [42]

Belgelendirme ve Raporlama Aşaması: Mobil cihaz ile ilgili yapılan inceleme ve analiz sonuçlarından elde edilen verilerin raporlandığı aşamadır [13]. Yazılan rapordan elde edilen sonuçların savunabilir ve tekrar edilebilir olması gerekmektedir. Belgelendirme ve raporlama süreci kapsamında Şekil 2.7'deki adımların uygulanması önerilmektedir [42].



Şekil 2.7. Mobil Cihazlar İçin Önerilen Raporlama Süreci [42]

2.5. Mobil Cihazlarda Adli Bilişim Araçlarının Sınıflandırılması

Mobil cihazların adli olarak incelenmesini ve analizini yapabilmek için adli bilişim araçlarının kullanılması gerekmektedir. Mobil cihazın adli incelemesini yaparken yalnızca bir araca bağlı kalmayarak farklı türdeki adli araçların kullanılarak incelemenin yapılması kanıtların bulunmasına katkı sağlamaktadır. Sam Brothers, bu amaçla mobil cihazlar için adli bilişim araç sınıflandırma sistemini Şekil 2.8'de olduğu gibi geliştirmiştir [43].

Şekil 2.8. Mobil Adli Bilişim Araçlarının Sınıflandırılması [43]

2.5.1. Manuel İnceleme (Manual Extraction)

Manuel inceleme yöntemi; cihazın tuş takımı veya dokunmatik ekranı kullanılarak doğrudan telefondaki verileri görüntülemeyi içermektedir. Keşfedilen bilgiler daha sonra fotoğraflı olarak belgelenir. Manuel olarak veri çıkarma işlemi hızlı ve kullanımı kolaydır ve hemen hemen her telefonda çalışır. Bu yöntem, arayüze aşina olmama nedeniyle belirli verilerin kaybolması gibi

sorunlara yol açabilir. Böyle bir durumda silinen bilgileri kurtarmak ve tüm verileri almak mümkün değildir [44].

2.5.2. Mantıksal İmaj Alma (Logical Extraction)

Mobil cihazı, kablolu veya kablosuz bağlantılar ile iş istasyonuyla ilişkisi sağlanarak imaj alma işlemi mantıksal imaj alma olarak adlandırılmaktadır. Farklı bağlantı türleri ve ilgili protokoller verilerin değiştirilmesine (örneğin, okunmamış SMS) veya farklı miktarlarda verilerin çıkarılmasına neden olabileceğinden, incelemeyi yapan kişi belirli bir bağlantı yöntemi seçerken ilgili sorunların farkında olmalıdır. Adli bilişim araçları (Paraben, XRY, UFED vb.) bilgisayardan mobil cihaza kurulan arayüz üzerinden bir dizi komut göndererek mantıksal imaj alma işlemini başlatır. Mobil cihaz, komut talebine göre yanıt verir. Yanıt (mobil cihaz verileri) iş istasyonuna geri gönderilir ve raporlama amacıyla adli tıp denetçisine sunulur [45].

2.5.3. Fiziksel İmaj Alma (Hex Dump)

Hex dump olarak bilinen diğer bir adıyla fiziksel imaj alma yöntemi; mobil cihazı iş istasyonuna bağlayarak, önyükleyiciyi(bootloader) ve işaretlenmemiş kodları mobil cihaza göndererek, mobil cihazın belleğinde bulunan verilerin bilgisayara gönderilmesini sağlar. Fiziksel imaj alma yöntemi, ayrılmamış alanlardaki verilere ulaşarak silinmiş verileri kurtarması ve analistlere kanıt niteliğindeki verileri sağlamasından dolayı tercih edilebilmektedir [44].

2.5.4. Çip Sökme (Chip-Off)

Chip-Off yöntemi, verilerin doğrudan mobil cihazın flash belleğinden fiziksel olarak çıkartılmasını ifade eder. Chip-off yöntemi analistlere ham ikili görüntü sağladığından dolayı tersine mühendislik işleminin yapılması gerekir. Tersine mühendislik işlemleri tamamlandıktan sonra ham görüntü analistler tarafında analiz edilir. Chip-off yöntemindeki sayısız ham veri formatı, yonga türlerinin fazlalığı, çıkarma işlemi sırasında yongaya zarar verilebilme ihtimalinde kaynaklı zor bir yöntemdir. Bu yöntemin başarılı bir şekilde tamamlanabilmesi için analistlere gerekli eğitimlerin sağlatılması gerekir [44].

2.5.5. Mikro İnceleme (Micro Read)

Mikro inceleme yöntemi, mobil cihazın hafıza yongasında bulunan delil niteliğindeki verilerin, güçlü mikroskoplar aracılığı ile incelendiği, teknik, pahalı ve fazla tercih edilmeyen yöntemdir [42].

2.6. Mobil Adli Bilişimde Veri Toplama Türleri

Dijital/elektronik cihazlardan delil niteliğindeki verilerin farklı yollar kullanılarak görüntülenmesi süreci 'veri elde etme' olarak tanımlanmaktadır. Dijital/ elektronik cihazların türüne göre veri elde etme işlemlerinin zorluk derecesi farklılık göstermektedir. Mobil cihaz türlerinden biri olan cep telefonlarından; fiziksel olarak, mantıksal olarak ve manuel olarak farklı çeşitlerde veri elde etme yöntemleri bulunmaktadır. Kullanılacak olan veri çıkarma türü; dijital cihazdan elde edilmesi beklenen veri türüne ve miktarına göre değişim gösterebilmektedir [44].

2.6.1. Fiziksel Edinim

Mobil cihazların fiziksel olarak elde edilmesi, mobil adli araçlar ve yöntemler kullanılarak gerçekleştirilmektedir. Fiziksel edinim ile belleğe doğrudan erişim yoluyla cihazdan bilgi alınabilmektedir. Bu süreç, bilgisayarların adli inceleme araştırmalarında benimsenen yaklaşıma benzer şekilde, tüm dosya sisteminin bit bit kopyasını oluşturur. Fiziksel bir alım, silinen veriler ve çoğu cihazdaki ayrılmamış alana erişim dâhil olmak üzere bir cihazda bulunan tüm verileri alabilir [44].

2.6.2. Mantıksal Edinim

Cep telefonlarındaki verinin bir bilgisayarla senkronize olarak elde edilmesi işlemi mantıksal edinim olarak tanımlanmaktadır. Mobil adli bilişimde kullanılan adli araçların birçoğu mantıksal edinim işlemini yapabilmektedir. Analistler tarafından mobil cihazdan mantıksal edinim işleminin yapılması kolay olmakla beraber, delil niteliğinde olan verilerin bir kısmına ulaşılabilmektedir. Mantıksal edinim işlemi, delil niteliğinde olabilecek ayrılmamış alandaki silinmiş bulguların elde edilmesini gerçekleştirememektedir [44].

2.6.3. Manuel Edinim

Mobil cihazlardan veri elde işlemleri gerçekleştirilirken genel olarak fiziksel edinim tercih edilmektedir. Fiziksel edinimin gerçekleşmediği durumda ise mantıksal edinim işlemi tercih edilmektedir. Mobil cihazlardan veri elde işleminde en az tercih edilen yöntem olarak manuel edinim işlemi kullanılmaktadır. Manuel edinim işleminde analistler mobil cihazda bulunan verilerin araştırmasını kullanıcı arayüzünü kullanarak yapmaktadır. Manuel edinim ile veri toplama türü diğer veri toplama türlerine göre daha risklidir. Çünkü insan hatasından kaynaklı olarak veriler silinebilmektedir. Manuel edinim işleminin gerçekleştirilmesi kolay olmakla beraber yalnızca görünen olgulara ulaşılabilmektedir [43].

2.7. Mobil Cihazların İncelenmesinde Kullanılan Adli Bilişim Yazılımları

Mobil kullanıcı sayısının artmasıyla beraber, teknolojinin ağırlıklı olarak mobil cihazlar üzerinde geliştiği söylenebilir. Bu nedenle adli incelemelerde mobil cihazın önemi gün geçtikçe artmaktadır. Mobil cihazlar, içerdikleri farklı database tiplerine sahip sayısız uygulamalar, sahip oldukları değişik tipte çip setler ve daha birçok farklı parametreden ötürü incelenmesi açısından bilgisayarlara göre çok daha karmaşıktır. Bu sebeple bu tip cihazların sürekli kendini geliştiren, aynı zamanda da kullanıcı dostu özel yazılımlarla incelenmeleri gerekmektedir [43].

2.7.1. Oxygen Forensic

Oxygen Forensic yazılımı günümüzde mobil adli bilişim araçlarından biri olarak; şifrelenmiş dosyaları, medya verilerini, bulut depolama verilerini, arama kaydı verilerini, sms verilerini, sosyal medya uygulamalarının verileri gibi birçok delil niteliğindeki verileri, Android, iOS, Windows Mobile gibi birçok işletim sistemine sahip mobil cihazların incelenmesi, analiz edilmesi ve raporlanması gibi işlemlerinin yapıldığı adli araç olarak kullanılmaktadır. Oxygen Software tarafından üretilen yazılım mobil cihazlardan veri ayıklama ve adli analiz/raporlama işlerinde yaygın olarak kullanılmaktadır. Yazılımın en güçlü yanları gelişmiş ve detaylı raporlama özellikleri ve birçok farklı donanıma ve mobil işletim sistemine destek vermesidir. Yazılım temel olarak, çalışan cihaz üzerinde ve cihazın daha önceden alınmış disk görüntüsü üzerinde analiz ve raporlar gerçekleştirmektedir. Oxygen Forensic yazılımı 8000'den fazla mobil cihazdan veri ayıklayabilmekte ve analizin yapabilmektedir [46].

2.7.2. Cellebrite

Mobil cihazların adli bilişim incelemelerinde; adli bilişim uzmanları, analistler, kolluk kuvvetleri gibi birçok sektör tarafından tercih edilen, Cellebrite şirketi tarafından piyasaya sürülmüş olup günümüzde mobil adli bilişim aracı olarak kullanılmaktadır. Farklı işletim sistemlerine sahip mobil cihazları destekleyerek cihazdan fiziksel ve mantıksal olarak imajlarının alınması, mobil cihazdaki verilerin ayıklanması, verilerin analizlerinin yapılması gibi birçok işlevi bulunmaktadır [42].

2.7.3. XRY

Mobil cihazlardaki olguların elde edilmesini sağlayan, Windows işletim sistemlerinde çalıştırılabilen mobil adli bilişim aracıdır. XRY sistemi hem mantıksal incelemelere (cihaz işletim sistemiyle doğrudan iletişim) hem de fiziksel incelemelere (işletim sistemini atlayarak ve kullanılabilir belleği boşaltarak) izin verir. Verilerin mantıksal olarak kurtarılması genellikle daha fazla cihaz için daha iyi desteklenirken, fiziksel incelemeler ise SMS metin mesajları, görüntüler ve arama kayıtları vb. gibi daha fazla silinmiş bilgiyi kurtarma yeteneği sunmaktadır [47].

2.7.4. Paraben

Paraben, farklı işletim sistemlerine sahip mobil cihazların fiziksel ve mantıksal olarak imaj alma, inceleme, verileri ayıklayabilme, analiz edebilme gibi birçok işleve sahip olup Paraben şirketi tarafından piyasaya sürülen, mobil adli bilişim aracı olarak günümüzde kullanılmaktadır [48].

2.7.5. Encase

EnCase, en popüler adli araçlardan biridir. Sadece akıllı telefonlar için değil, genel dijital adli tıp için kullanılır. Bu araç bir Android görüntüsünü inceleyebilmesine rağmen, araştırmacının ihtiyaç duyduğu izleri bulmak için mücadele etmesi gerekmektedir. Bunun nedeni, EnCase'in özellikle yüklü uygulamalara ve bunların taşıyabilecekleri kanıtlara değil, yalnızca dosya sistemine odaklanmasıdır. Ayrıca EnCase, doğrudan cihaz üzerinde kullanılabilir. Yani, bir aracı kurarak, mobil cihaz hakkında belirli bilgilerin alınmasını mümkün kılar. Olumsuz tarafı ise bu bilgiler sınırlıdır ve uygulama yapılarını içermemektedir [16].

2.7.6. Magnet AXIOM

Magnet AXIOM; akıllı telefon, bilgisayar gibi elektronik cihazlardan, delil niteliğinde olan ilgili verileri toplamak için hazırlanmış adli araçlardan biridir. Adli soruşturma uzmanları tarafından delilleri aramak için kullanılan Magnet AXIOM, verileri görselleştirebilir, analiz edebilir, verileri doğrulayabilir ve diğer araçlarla elde edilen görüntüleri incelemek üzere tek bir vaka dosyasında birleştirebilme gibi özelliklere sahiptir [48].

2.7.7. AccessData Mobile Forensic

Mobil cihazlardan elde edilen dijital delillerin detaylı olarak incelemesini sağlaması, filtreleme gibi özelliklerini kullanması nedeniyle analiz yeteneğindeki gücünün fazla olması, bilgisayar ile elde edilen dijital delillerle bağlantı kurabilmesi, kolay kullanıma sahip olması nedeniyle adli bilişim uzmanları tarafından tercih edilen mobil adli bilişim aracıdır.

2.7.8. MOBILEdit Forensic

Farklı işletim sistemlerine sahip mobil cihazlardan; arama kayıtlarının verileri, sms verileri, medya verileri, uygulamalara ait veriler gibi kullanıcının kişisel verilerinin ayıklanması, incelenmesi, analiz edilmesi gibi işlevleri yerine getiren mobil adli bilişim aracı olarak günümüzde kullanılmaktadır [49].

2.7.9. SAFT

SAFT; arama günlükleri, SMS/MMS günlükleri, kişi listesi, dosya tarayıcı günlükleri, tarayıcı geçmişi, yer imleri, facebook ve twitter günlükleri, youtube ve instagram günlükleri, Whatsapp ve Skype günlükleri, e-posta mesajları, konum geçmişi ve takvim gibi cihazdan değerli bilgileri çıkarmak için kullanılan kullanımı kolay mobil adli inceleme yazılımıdır. Sadece Android cihazların analizini yapabilmektedir. Microsoft Word formatında rapor oluşturma olanağına sahiptir [50].

2.8. Mobil Adli Bilişimde Karşılaşılan Zorluklar

Mobil cihazların adli inceleme açısından önemini bilerek, adli bilişim uzmanlarının karşılaştığı mevcut bilinen zorlukları bilmek gerekmektedir. Ulusal Adalet Enstitüsü Elektronik Suçlar Araştırması hibesinden sağlanan fonu kullanarak, mevcut cep telefonu ortamına ilişkin bir anket gerçekleştirilmiş olup; taşıyıcılar ve üreticiler, veri koruma, güç ve veri konektörleri, işletim sistemleri ve iletişim protokolleri, güvenlik mekanizmaları ve benzersiz veri biçimleri olmak üzere altı genel zorluk kategorisi üretilmiştir [6].

Taşıyıcılar ve Üreticiler: Bir cep telefonu soruşturmasında, ilk işlem telefonun kimliğinin tespit edilmesi olmalıdır. Birden fazla ağ taşıyıcısı ve cihaz üreticisi olduğu düşünüldüğünde, eğitimli araştırmacılar için bile bir telefonu tek başına tespit etmek son derece zordur. Tek bir donanım üreticisinden belirli bir model, çeşitli taşıyıcılardan birçok farklı isim kullanılarak pazarlanabilmektedir. Mobil cihazların işletim sistemleri, sahip oldukları donanımlar, mobil cihazların boyutları ve özellikleri teknoloji ilerledikçe gelişim gösterip değiştiği için farklı mobil cihaz türleri piyasaya sürülmektedir. Mobil cihaz türlerindeki çeşitlilik olması nedeniyle adli incelemelerde, analistlerin kullandığı adli bilişim araçlarının sürekli olarak güncel olması gerekmektedir [13].

Veri Koruma: Bir cep telefonu araştırması için, cihazın daha fazla veri veya sesli iletişim almasını engellemek önemlidir. Metin mesajları "İlk Giren İlk Çıkar" düzeninde saklandığından, yeni gelen herhangi bir metin mesajı, saklanan eski metin mesajlarını silebilir. Benzer şekilde, gelen aramalar arama geçmişi günlüklerini silebilir ve bazı cihazlar (RIM BlackBerry gibi) gelen iletişimlerden korunmazlarsa tüm verilerden uzaktan silinebilir. Bu nedenle, ilk edinim üzerine, bu cep telefonları bir tür kablosuz koruma kabına yerleştirilmelidir. Bunun için çeşitli başarı seviyelerinde birden fazla teknoloji kullanılabilir [13].

Güç ve Veri Konektörleri: Adli bilişim uzmanlarının karşılaştığı bir diğer zorluk, telefonun gücünü nasıl koruyacağıdır. Yeterince uzun bir süre fişe takılı kalmazsa, telefonun pili sonunda tüm gücünü kaybeder. Birçok cep telefonu bilgileri geçici bellekte sakladığından, tam bir güç kaybı, bilgi kaybı, dolayısıyla önemli kanıtların kaybı anlamına gelebilir. Bu nedenle, bir telefonun şarj durumunda

tutulması arzu edilir. Günümüzde cep telefonları için güç gereksinimleri için bir standart yoktur. Bu güç standartları eksikliği, kablo konektörleri için de bir standart olmaması gerçeğiyle birleşmektedir. Mobil cihazların artması nedeniyle adli bilişim uzmanlarının, mobil cihaz üzerinden adli kopya(imaj) oluşturma ve inceleme aşamalarını başarılı bir şekilde tamamlayabilmesi için, mobil adli inceleme donanımlarının ve yazılımlarının bulunması gerekmektedir [13].

İşletim Sistemleri ve İletişim Protokolleri: Mobil cihazların; IOS, Android, Windows Mobile, Palm OS, Symbian gibi farklı işletim sistemi türleri bulunmaktadır. Adli bilişim uzmanlarının mobil cihaz üzerinden inceleme gerçekleştirirken, işletim sistemlerindeki çeşitlilik nedeniyle, bu işletim sistemleri hakkında yeterli bilgiye hâkim olması gerekmektedir [13].

Güvenlik Mekanizmaları: Mobil cihazlarda teknolojinin ilerlemesiyle beraber kullanıcıya ait kişisel bilgileri koruyabilmek için güvenlik mekanizmaları geliştirilmektedir. Adli bilişim uzmanları tarafından incelenen mobil cihazın sahip olduğu güvenlik özelliklerindeki şifreleme mekanizmaları, adli incelemede gerekli olguların elde edilmesinde sorun teşkil edebilmektedir. Bundan dolayı adli bilişim uzmanının mobil cihazdan gerekli olguları alabilmesi için güvenlik mekanizmalarını çözmesi gerekmektedir [13].

Benzersiz Veri Formatları: Bir telefonun taşıyıcısının ve üreticisinin tanımlanabileceğini, telefonun kablosuz aktiviteden korunabileceğini, doğru güç ve veri konektörü kablolarının bulunabileceğini ve bilgilerin şifreli olarak saklanmadığını varsayarsak, teorik olarak mümkündür. Ancak geriye bir engel daha kalıyor. Modern bir cep telefonunu oluşturan diğer bileşenlerde olduğu gibi, bir araştırmacı tarafından istenen bilgilerin çoğu için ne standart bir biçim ne de standart bir konum vardır. Veri dosyaları birkaç yerde saklanabilir. Daha önce de belirtildiği gibi, telefonun SIM kartında bulunan bellekte bazı bilgiler saklanabilir. Cep telefonu donanımı ayrıca, geçici (bilgiyi tutmak için elektrik yükü gerektirir) veya geçici olmayan (bilgiyi elektrik yükü olmadan tutar) olarak bölümlere ayrılabilen rastgele erişim belleği (RAM) içerir. Adli yazılım araştırmacıları ve üreticileri, bilgilerin tüm bu tür belleklerde saklanıyor olabileceğinin farkında olmalıdır. Birçok cep telefonunda ayrıca salt okunur bellek (ROM) bulunur. Ancak, ROM tipik olarak telefonun işletim sistemini depolamak için kullanılır ve son kullanıcı tarafından kolayca değiştirilemez. ROM'un içeriği kolayca değiştirilemediği için, burada saklanan dosyalar muhtemelen bir araştırmacının pek ilgisini çekmez. Telefon numaraları, adres defterleri, e-posta mesajları ve metin mesajları gibi metinsel bilgiler özel dosya formatları kullanılarak saklanır. Adli yazılım araçlarının yapımcılarının, bu dosyaları insanlar tarafından kolayca anlaşılabilecek bilgilere dönüştürecek yazılımlar yazabilmeleri için bu formatlardan haberdar olmaları gerekecektir. Bu tescilli dosya biçimlerinin bir istisnası, tipik olarak ortak JPG ve MPEG biçimlerinde depolanan görüntü ve video dosyaları içindir [13].

3. ANDROİD CİHAZLARDA ZARARLI YAZILIM

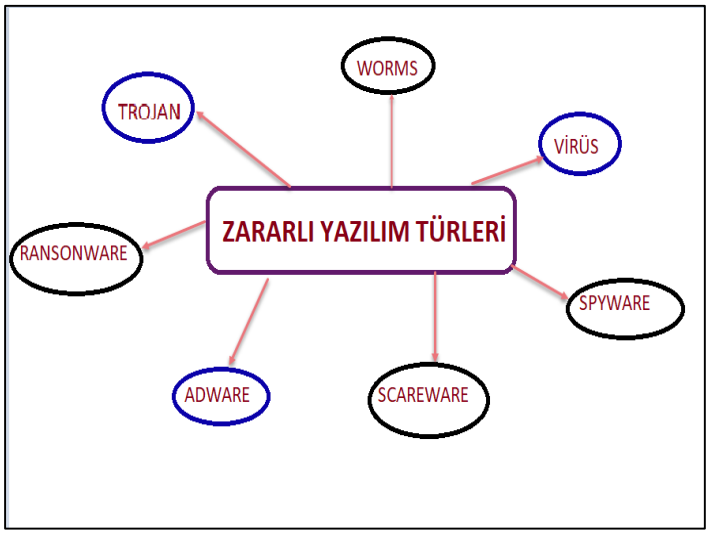
Günümüzde saldırganlar tarafından kullanıcıların kullandığı mobil cihazlar hedef odağı olmaktadır. Mobil cihaz türlerinden pazar payı oranı yüksek olan Android cihazlar, saldırganın cihazda depolanan, cihaz tarafından aktarılan verilere yetkisiz erişim elde etmeye çalıştığı birçok potansiyel saldırı vektörüne sahiptir. Saldırı Vektörleri, saldırganların mobil cihaz tarafından kullanılan işletim sistemlerinde veya uygulamalarda bulunan güvenlik açıklıklarından yararlanmasına olanak tanımaktadır. Saldırganlar, mobil cihazlara bulaşmak için kötü amaçlı bir uygulama geliştirerek zararlı uygulamayı uygulama mağazasından yayınlayabilmekle beraber orijinal uygulamaları taklit ederek zararlı uygulamaları sosyal mühendislik gibi çeşitli yollarla kullanıcıların cihazına yüklemesini sağlamaktadır. Zararlı uygulama kullanıcının cihazına yüklenildiği takdirde saldırgan tarafından cihaz kontrolü ele geçirilebilmektedir. Ransonware, trojan, virüs, adware, scareware, worm gibi çeşitli zararlı yazılım türleri bulunmaktadır [14].

Saldırganlar tarafından kötü amaçlı bir uygulamadan veya veri kaybından etkilenmeyi önlemek için Android cihazlarda güvenliğin sağlanması gerekmektedir. Bu bağlamda; Android cihazlarda root işlemi yapılmamalıdır. Bununla birlikte Android cihazlarda; kullanıcılarının farkındalığının arttırılması, antivirüs uygulamalarının yüklenmesi, işletim sisteminin güncel tutulması, doğrudan Apk dosyalarının indirilmemesi, uygulamaların yalnızca resmi Android mağazasından yüklenilmesi, yedeklemenin gerçekleştirilmesi gibi çeşitli işlemler yapılarak önlemler alınabilmektedir [15].

Adli vakalarda delil niteliği olan Android cihazlara zararlı uygulamaların yüklenilmesi muhtemeldir. Bu sebeple siber güvenlik uzmanlarının, adli bilişim uzmanlarının zararlı yazılım türlerini bilmekle beraber Android cihaza bulaşmış zararlı uygulamanın analiz edilmesiyle ilgili teknikler hakkında bilgi sahibi olması gerekmektedir.

3.1. Android Cihazlarda Zararlı Yazılım Türleri

Android cihazlara farklı yöntemler ile bulaşabilen ve kullanıcıya ait bilgilere zararlı yazılımın amacına bağlı olarak farklı şekillerde zarar veren zararlı yazılım türleri bulunmaktadır. Android cihazlarda; Ransonware (Fidye yazılımı), Trojan (Truva Atı), Adware (Reklam yazılımı), Scareware (Korku yazılımı), Virüs, Spyware (Casus yazılım) gibi çeşitleri zararlı yazılım türleri bulunmaktadır. Zararlı yazılım türleri Şekil 3.1'de gösterilmiştir.



Şekil 3.1. Zararlı Yazılım Türleri

3.1.1. Ransonware (Fidye Yazılım)

Android cihazlarda Ransonware (fidye yazılımı), mobil cihazları hedef alan zararlı yazılım çeşidi olarak bilinmektedir. Android Ransonware ile saldırganlar, kullanıcıların Android cihazlarına zararlı yazılımı yükleyerek kullanıcıya ait verileri çalmakla beraber verileri şifreleme işlemini yapabilmektedir. Saldırganlar böylelikle kullanıcının cihaza olan erişimini engelleyerek kullanıcının tekrardan cihaza olan erişimini sağlayabilmesi için fidye istemektedir. Ransonware (fidye yazılımı) yazılımları üçüncü taraf web siteleri, e-posta ekleri, sosyal medya platformları, üçüncü taraf uygulama mağazaları ile dağıtılan virüslü uygulamalar gibi çeşitli şekillerde Android cihaza bulaşabilmektedir. Saldırganlar tarafından kullanılan Ransonware yazılımlarından Android cihaza güvenlik yazılımları yükleyerek, üçüncü taraf uygulamaları indirmeden önce gerekli dokümanı okuyarak, bilinmeyen bağlantılara tıklarken ve uygulamaları indirirken dikkatli olarak, uygulama ve izinlere dikkat ederek, yedekleme işlemi gibi çeşitli güvenlik önlemleri alınarak Android Ransonware yazılımından korunabilmektedir. MalLocker.B ve Koler.a gibi yaygın kullanılan Android Ransonware örnekleri bulunmaktadır [51].

3.1.2. Trojan (Truva Atı)

Trojan (Truva atı), mobil cihazları hedef alan zararlı yazılım çeşitlerinden biri olarak bilinmektedir. Saldırganlar tarafından sıklıkla tercih edilen Trojanlar programın kendisi olmakla beraber, Android cihaz üzerinde kendisini çoğaltmamaktadır. Trojanlar, Android sisteminde yetkisiz bir şekilde erişim elde ederek kullanıcıya ait veriler üzerinde silme, engelleme, değiştirme, kopyalama gibi çeşitli eylemleri yapabilmektedir [52]. Trojanlar bir uygulama gibi görünüp e-posta ile gönderilerek Android cihaz üzerinde yükleme işleminin tamamlanmasıyla birlikte bulaşabilmektedir. Kullanıcı

tarafından Android cihaz üzerinde gerçekleştirilen her eylem Trojan yazılımı tarafından belirlenen sunucuya gönderilmektedir. Bu bağlamda saldırganlar tarafından kullanılan Trojan yazılımlarına karşı kullanıcının; güvenli web sitelerinden programları yüklemesi, e-posta eklerine dikkat etmesi, bilinmeyen kaynaklardan indirilen programı cihaz üzerinde çalıştırmaması, yazılımları güncel tutması gibi işlemlerin yapılması Android cihazı Trojan yazılımlarından koruyabilmektedir [14]. ExoCompact, SharkBot, Octo gibi çeşitli Android Trojan yazılımları bulunmaktadır [53].

3.1.3. Virüs

Android virüsler, yürütülebilir dosyalara meşru programlara eklenmiş olan zararlı yürütülebilir kod olarak tanımlanmaktadır. Virüsler dosyalara eklenip çoğalabilmektedir. Dağıtılması ve oluşturulması zordur. Saldırganlar tarafından genellikle MS Office programlarını kullanarak e-mail aracığıyla kullanıcının cihazına gönderilmektedir. Kullanıcının programı yürütmesiyle beraber saldırgan hedefine ulaşmaktadır. Bu nedenle; Android cihaza güvenlik yazılımları yüklenerek, e-mail ile gönderilen bağlantılara dikkat edilerek, gönderilen dosyaların virüs total gibi programlarda çalıştırılıp gerekli bilgiler edinildikten sonra çalıştırılması gibi durumlarda kullanıcı Android cihazını virüsten koruyabilmektedir [54].

3.1.4. Adware (Reklam Yazılımı)

Adware (Reklam yazılımı) genellikle pop-up, banner vb. reklamların kullanıcının cihazında görünmesini gerçekleştiren yazılımlar olarak tanımlanmaktadır. Saldırganlar gelir yaratmak amacıyla Adware yazılımını kullanabilmektedir. Reklamlar indirilebilmekle beraber ücretsiz programlarda bulunabilmektedir. Adware yazılımı, Android cihaz ekranında gösterilen hizmetlerle ilgili reklamları görüntülemek için kullanıcının hangi tür web sitelerini kullandığını analiz etmek için kullanılabilmektedir [55].

3.1.5. Scareware (Korku Yazılımı)

Scareware (Korku yazılımı), Android kullanıcıyı korkutma işlemini gerçekleştirerek sosyal mühendislik yöntemleri ile sahte yazılımları satın almanızı veya indirmenizi gerçekleştiren zararlı yazılım olarak bilinmektedir [56].

3.1.6. Spyware (Casus Yazılım)

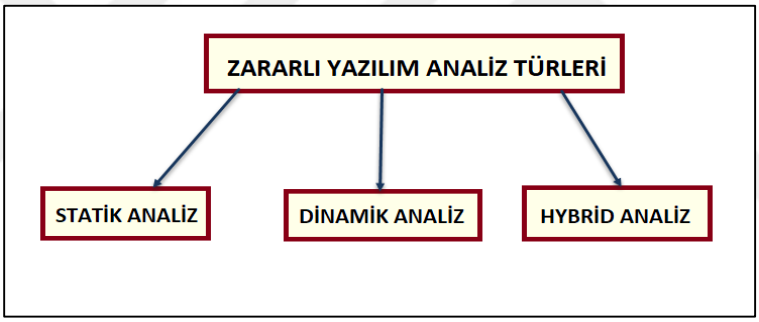
Spyware (Casus yazılım) yazılımı kullanıcının izni olmadan Android cihaz üzerinden bilgi toplayabilen zararlı yazılım olarak bilinmektedir. Saldırganlar spyware yazılımı ile kullanıcının kimlik doğrulama bilgilerini, e-posta adreslerini, tuş vuruşlarını, kullanıcı aktivitelerini ve birçok kişisel bilgiyi ele geçirebilmektedir [57].

3.1.7. Worms (Solucanlar)

Worms (Solucanlar) yazılımı, yayılmalarını gerçekleştirmek için programların parçası olmasını gerektirmeyen, cihazların güvenlik açıklarından yararlanmak için üretilmiş, kendi kendine çoğaltabilen program olarak bilinmektedir. Worm yazılımları kendi kendine çoğaldıklarından dolayı ağ trafiğini yavaşlatabilmektedir [58].

3.2. Android Cihazlarda Zararlı Yazılım Analiz Türleri

Siber güvenlik uzmanları tarafından zararlı yazılımlar statik, dinamik ve hybrid olmak üzere üç şekilde analiz edilmektedir. Zararlı yazılım analizi şüpheli bir dosyanın, URL'nin veya programın davranışını ve amacını anlama süreci olarak bilinmektedir. Analizin çıktısı ile potansiyel tehdidin tespit edilmesine ve azaltılmasına yardımcı olabilmektedir [59]. Zararlı yazılım analiz türleri Şekil 3.2'de gösterilmiştir.



Şekil 3.2. Zararlı Yazılım Analiz Türleri

3.2.1. Statik Analiz

Statik analiz uygulamanın kodunu, altyapıyı, kitaplıkları veya paketlenmiş dosyaları inceleyerek zararlı yazılımın belirtileri, ne amaçla yapıldığı konusunda incelemeler yapılabilmektedir. Android cihazı zarara uğratmadan zararlı yazılımın analizi yapılabildiği için statik analiz yöntemi tercih edilebilmektedir. Siber güvenlik uzmanları tarafından; decompilerlar, weaving, metedata çıkarıcılar, Androguard, apktool, JEB Decompiler gibi çeşitli statik analiz araçları kullanılmaktadır [19].

3.2.2. Dinamik Analiz

Dinamik analiz yöntemi ile zararlı yazılım cihaz üzerinde yürütülerek yazılımın sistem üzerinde ne gibi değişiklikler oluşturduğu, dosya dizin üzerindeki eylemleri, ağ ile ilgili, sistem üzerinde tesir

altına almış olduğu etki alanı ile ilgili çeşitli bilgiler edinilebilmektedir. Dosyaların salt okunur izole ortam kullanılarak aktarılması gerekmektedir. Statik analiz yöntemi kod üzerinden gerçekleştirilen şifreleme yöntemlerinden etkilenebilmektedir. Dinamik analiz yöntemi ise kod üzerinden gerçekleştirilen şifreleme yöntemlerinden etkilenmemektedir. Bu bağlamda dinamik analiz yöntemi ile daha doğru sonuçlara ulaşılabilmektedir. Siber güvenlik uzmanları tarafından; wireshark, sandbox, Windbg, FakeDNS, Olly Debugger gibi çeşitli dinamik analiz araçları kullanılmaktadır [17].

3.2.3. Hybrid Analiz

Hybrid analiz yöntemi, statik ve dinamik analiz yöntemlerini birleştirilmesi olarak tanımlanmaktadır. Hybrid analiz ile zararlı yazılım kodu algılanabilmekle, bilinmeyen tehditlerin tespit edilmesine yardımcı olabilmektedir. Siber güvenlik uzmanlarına bu bağlamda statik ve dinamik analiz tekniğine göre daha iyi bir yaklaşım sağlamaktadır [59].

3.3. Android Zararlı Yazılımlarına Karşı Alınabilecek Önlemler

Kullanıcıya ait kişisel verileri bulunduran Android cihazların saldırganlar tarafından ele geçirilmesini önlemek için aşağıda belirtilen işlemler yapılarak Android cihazların zararlı yazılıma karşı güvenliğinin alınması sağlanabilmektedir.

Kullanıcıların farkındalığı arttırılarak bilinmeyen kaynaklardan e-postalara dikkat etmesi gerekmektedir.

Android cihaza root işlemi yapılmamalıdır.

Uygulamaların yalnızca resmi Android mağazasından indirilmeli ve Android paket dosyaları (apk) doğrudan indirilmemelidir.

Uygulamalar cihaza yüklenirken verilen izinlere dikkat edilmelidir.

Android işletim sistemi ve yazılımları güncel tutulmalıdır.

Android cihazdaki verilerin yedekleme işlemi yapılmalıdır.

Cihaz üzerine antivirüs uygulaması yüklenilmelidir.

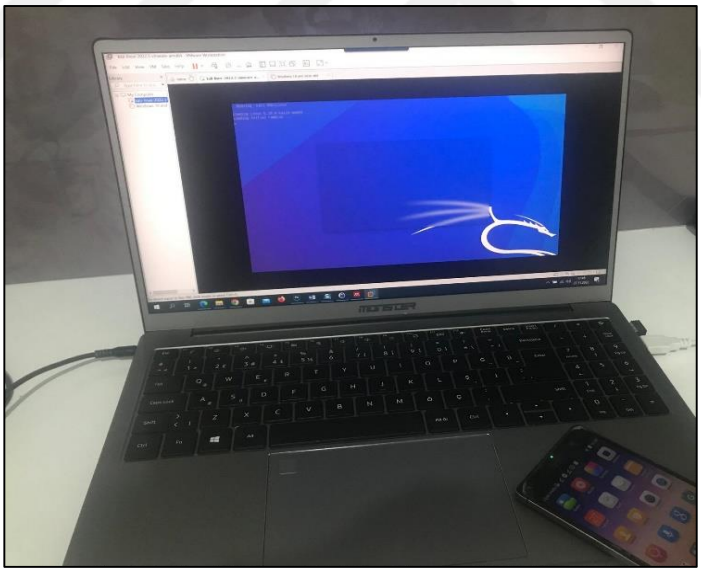
Android paket dosyaları (apk) doğrudan indirilmemelidir.

X-Ray gibi Android vulnerability scanner araçları kullanılabilir. Google Play Protect kullanılarak verilerin gizliliğiyle beraber uygulamaların güvenliği sağlanmalıdır [60].

4. ANDROİD CİHAZLARDA ZARARLI YAZILIM ANALİZİ

Tez çalışmasının amacı; Android işletim sistemine sahip Android cihaz üzerinde zararlı yazılım analizinin adli bilişim bakımından incelenmesini gerçekleştirmektir. Bu nedenle Android işletim sistemine sahip cihaz üzerinde çeşitli zararlı yazılımlar (Ransonware, trojan) oluşturularak sızma testi işlemi gerçekleştirilmiştir. Android kullanıcı çeşitli yollarla kandırılmış olup zararlı Android uygulamalar cihaz üzerine indirilmiştir.

Saldırı aşamaları tamamlandıktan sonra mobil adli bilişim yazılımı kullanılarak Android cihazın mantıksal ve fiziksel imajları üzerinde inceleme yapılmakla beraber manuel inceleme yapılarak da cihazdaki zararlı yazılımın adli bilişim bakımından analizi gerçekleştirilmiştir. Yapılan incelemeler sonucunda manuel inceleme, mantıksal imaj ve fiziksel imaj ile elde edilen bulgular tablo halinde sunulmuştur. Tez çalışmasının gerçekleştirildiği cihazlar Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Tez Çalışmasının Gerçekleştirildiği Cihazlar

4.1. Android Cihazda Zararlı Yazılım Oluşturulması İçin Kullanılan Donanım ve Yazılımlar

Android 4.4.2 işletim sistemi yüklü Huawei P7-L10 16 GB modeline sahip akıllı telefon üzerinde zararlı Android uygulamalar yüklenilmiş olup incelemeler gerçekleştirilmiştir. Android 4.4.2 işletim sistemi yüklü Huawei P7-L10 16 GB modeline sahip akıllı telefon ile birlikte Windows 10

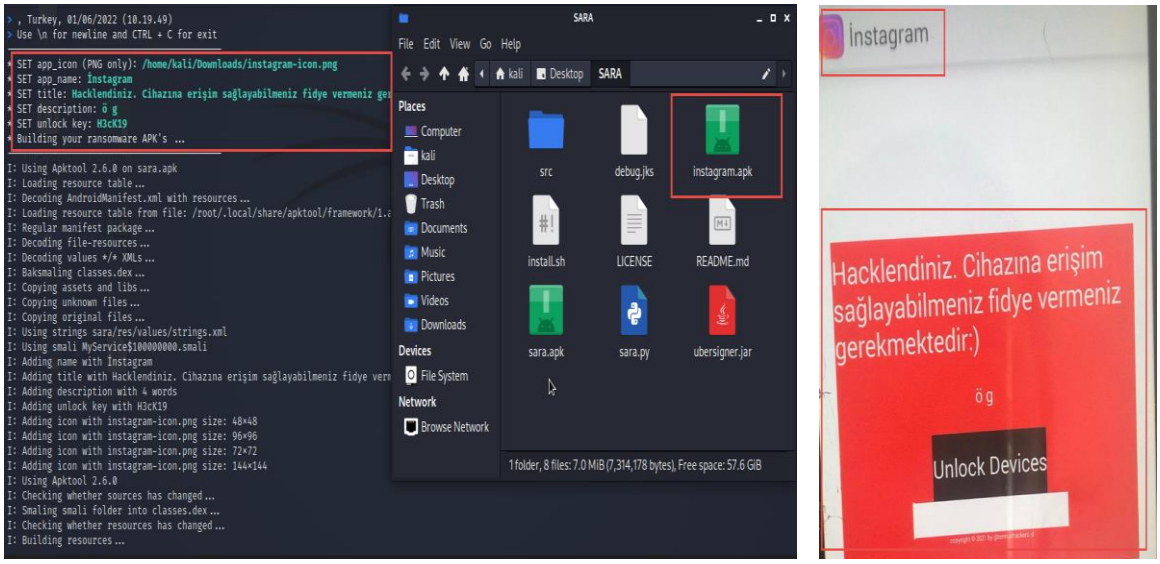
Pro yüklü 64 bit işlemcili 16 GB RAM sahip Monster bilgisayar donanımları kullanılmıştır. Tez çalışmasının gerçekleşebilmesi için VMWare sanal ortam üzerinde Kali Linux işletim sisteminde Android cihazlar için kullanılan zararlı yazılım toolları kullanılarak zararlı apk dosyaları oluşturulmuştur. Apktool aracı ile uygulamaların decompile/compile işlemleri gerçekleştirilmiştir. Tez çalışmasında kullanılan donanım ve yazılımlar Tablo 4.1'de gösterilmiştir.

Tablo 4.1. Zararlı Yazılım Oluşturulması İçin Kullanılan Donanım ve Yazılımlar

Kullanılan Donanım ve Yazılımlar	Kullanım Amacı
Huawei P7-L10 16 GB Android 4.2.2	İncelenecek Cihaz
Windows 10 Pro, 64 bit işlemci, 16 GB RAM Monster Bilgisayar	İş İstasyonu
TURKCELL SIM Kart	SIM Kart
Kali Linux	Sızma Testi İçin Kullanılacak Sistem
Apktool	Uygulamaları Oluşturma Aracı

4.1.1. Android Ransonware Zararlı Yazılımın Oluşturulması ve Sızma Testinin Gerçekleştirilmesi

SARA Ransonware aracı, Kali Linux işletim sistemi üzerinde yüklenme işlemi gerçekleştirildikten sonra zararlı apk dosyası oluşturmaktadır [61]. SARA aracı ile oluşturulan apk dosyası Android kullanıcısına Google Drive ile zararlı instagram.apk uygulaması gönderilmiştir. Kullanıcının Google Drive üzerinde instagram.apk dosyasını indirip cihazı üzerinde çalıştırmasını gerçekleştirdiğinde cihazına tekrar giriş yapabilmesi için şifre talep edilmiştir. Kullanıcı tarafından şifre girilmediği takdir de Android kullanıcı cihazını kullanamaz hale gelmiştir. Şifreyi tekrar elde edebilmesi için karşılığında fidye talep edilerek Ransonware zararlı yazılım aracı hedefine ulaşmıştır. Şekil 4.2a'da görüldüğü gibi SARA Ransonware aracının kurulumu gerçekleştirilir. 'app_icon' seçeneği ile oluşturulan apk uygulamasının iconu seçilir. 'app_name' seçeneği ile uygulamanın ismi belirlenir. 'title' seçeneği ile kurban uygulamayı başlattığında hacklendiğine dair fidye talep edilir. 'description seçeneği ile istenilen tanımlama yapılır. 'unlock key' seçeneği ile Ransonware için şifre belirlenir. Zararlı instagram.apk dosyası oluşturulur. Şekil 4.2b'de kullanıcının instagram uygulamasını çalıştırdığında cihazının kilitlendiği görülmektedir. SARA zararlı yazılım aracının kurulum ve zararlı instagram.apk dosyasının oluşturulması ve sızma testinin gerçekleştirilmesi Şekil 4.2'de gösterilmiştir.

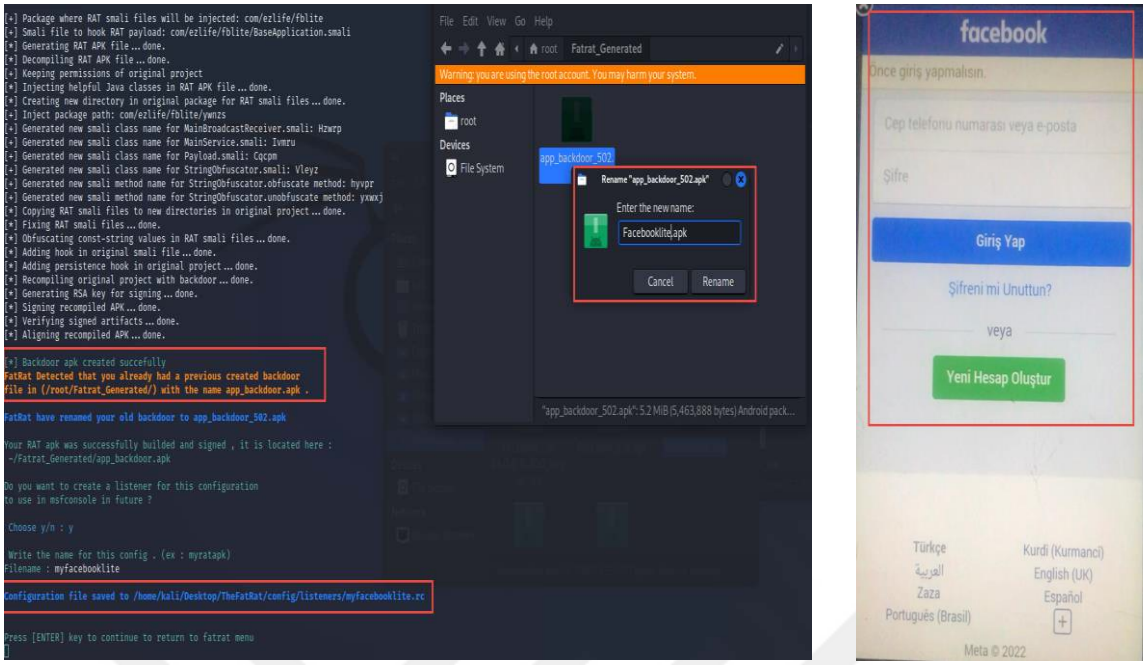


(a) **(b)**

Şekil 4.2. Ransonware Apk Uygulamasının Oluşturulması. **(a)** uygulamanın oluşturulma adımları ve **(b)** sızma testinin gerçekleştirilmesi

4.1.2. Orijinal Apk Dosyasına Backdoor Yerleştirilerek Zararlı Yazılım Oluşturulması ve Sızma Testinin Gerçekleştirilmesi

Kali Linux işletim sistemi üzerinde TheFatrat aracı kullanılarak zararlı yazılım oluşturulabilmektedir. TheFatrat aracı ile Android, Windows, Mac cihazları için zararlı trojan, RAT oluşturarak kullanıcının kullandığı cihaz üzerinde saldırı gerçekleştirilmektedir. TheFatrat aracının sahip olduğu payloadlar ile oluşturulan zararlı yazılımlar Antivirüs taramalarını atlatabilmektedir. TheFatrat aracı ile orijinal FacebookLite apk dosyasına backdoor yerleştirilerek zararlı apk dosyası oluşturulmuştur. Google Drive aracılığı ile kullanıcının Android cihazına indirilmiştir. Oluşturulan zararlı apk ile saldırı aşaması gerçekleştirilmiştir. Şekil 4.3a'da görüldüğü gibi TheFatRat aracının kurulumu gerçekleştirilir. Orijinal apk dosyasının backdooring işlemleri gerçekleştirilerek ayarlar tamamlanır. Zararlı Facebooklite.apk dosyası oluşturulur. Şekil 4.3b'de görüldüğü gibi kullanıcının cihazından zararlı Facebook Lite uygulaması çalıştırılarak sızma testi işlemi gerçekleştirilir. Zararlı Facebooklite.apk dosyasının oluşturulması ve sızma testinin gerçekleştirilmesi Şekil 4.3'te gösterilmiştir.

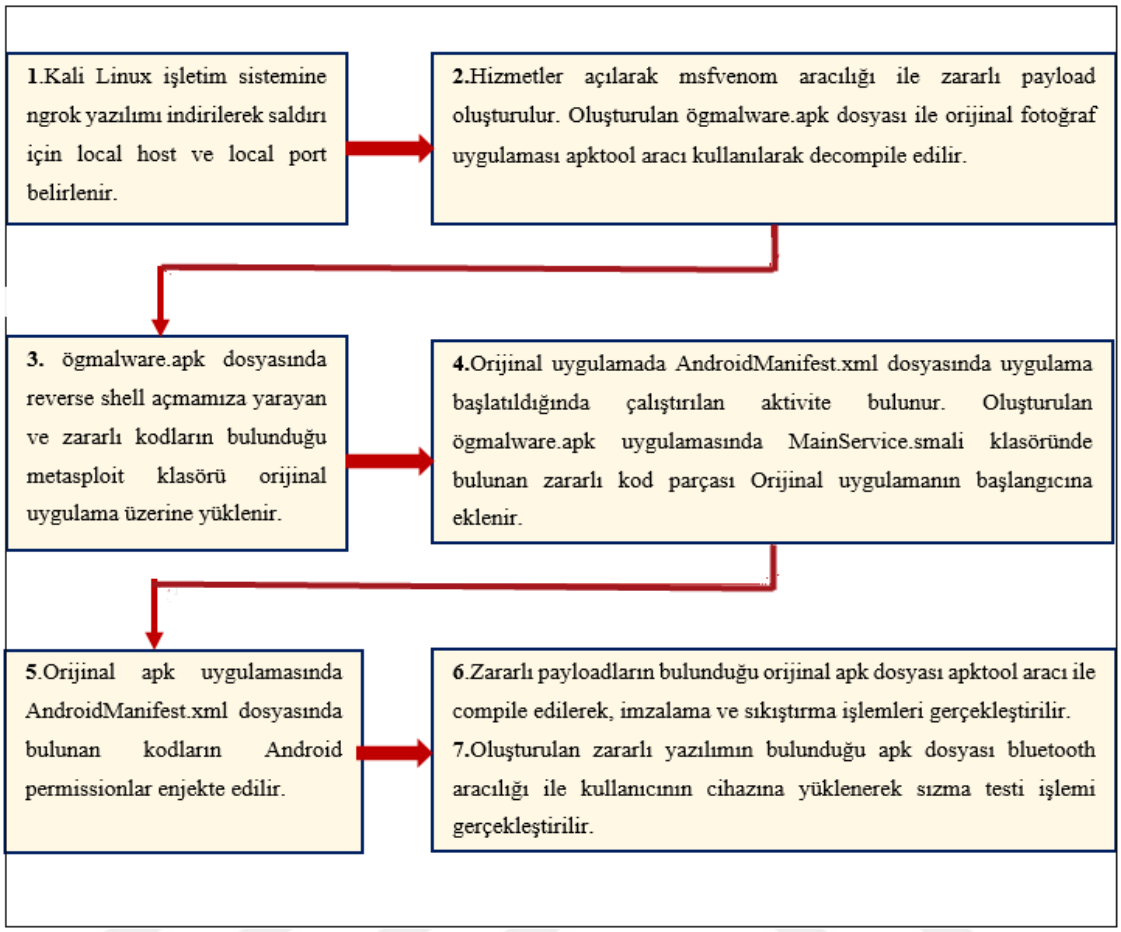


(a) **(b)**

Şekil 4.3. Orijinal Apk Dosyasına Backdoor Yerleştirilerek Zararlı Yazılım Oluşturulması. **(a)** uygulamanın oluşturulma adımları ve **(b)** sızma testinin gerçekleştirilmesi

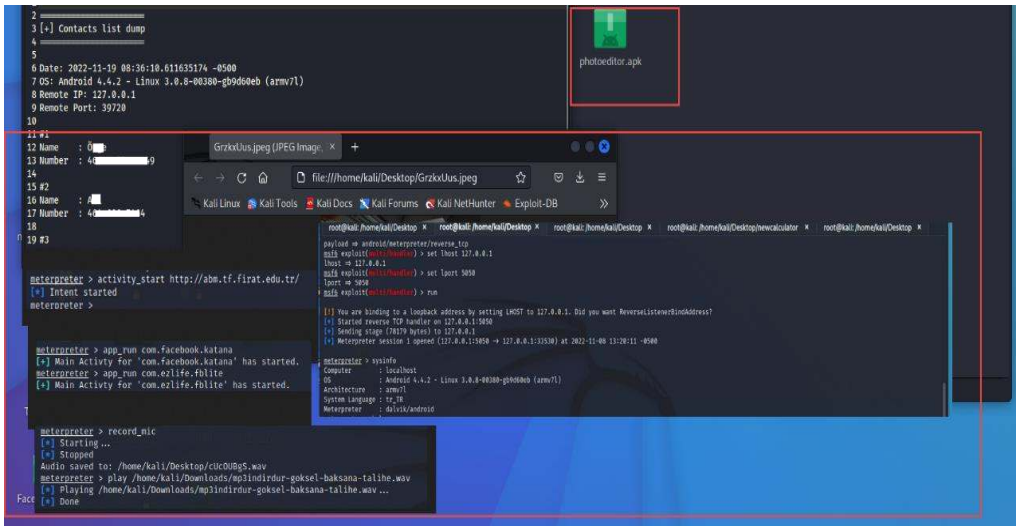
4.1.3. Manuel Olarak Android Uygulamaya Zararlı Payload Enjekte Edilerek Zararlı Yazılım Oluşturulması ve Sızma Testinin Gerçekleştirilmesi

Orijinal Android uygulamasına manuel olarak zararlı payload enjekte edilerek zararlı yazılım oluşturulabilmektedir. Manuel olarak zararlı payload; metasploit frameworkün parçası olanı msfvenom kullanılarak oluşturulabilmektedir. Orijinal fotoğraf uygulamasına manuel olarak zararlı payload enjekte edilerek apk dosyası yeniden derlenebilmektedir. Derlenen zararlı apk dosyası Bluetooth aracılığı ile kullanıcının cihazına yüklenerek cihaza zararlı yazılım bulaştırılmış olup Android cihaz üzerinde sızma testi işlemi gerçekleştirilmiştir. Manuel olarak orijinal apk dosyasına zararlı payload enjekte adımları Şekil 4.4'te gösterilmiştir.



Şekil 4.4. Manuel Android Uygulamaya Zararlı Payload Enjekte Edilerek Zararlı Yazılım Oluşturulması ve Sızma Testinin Gerçekleştirilmesi

Manuel olarak zararlı payload enjekte edilen photoeditor.apk dosyası ile sızma testinin örnekleri Şekil 4.5'te gösterilmiştir.



Şekil 4.5. Photeditor.apk Dosyası ile Sızma Testi Örnekleri

Zararlı uygulamalar oluşturularak gerçekleştirilen sızma testi senaryosunda başarılı ve başarısız gerçekleştirilen eylemler Tablo 4.2'de gösterilmiştir.

Tablo 4.2. Sızma Testi ile Gerçekleştirilen Eylemlerin Başarı Durumu

Sızma Testinde Gerçekleştirilen Eylemler	Başarım Durumu
Sistem Bilgilerini Elde Etme	+
Kullanıcıyı Gerçek Zamanlı Olarak İzleme	-
Cihazdaki Uygulama Listesini Elde Etme	+
Cihaza Apk Dosyası Yükleme	+
Cihaz Üzerinde Apk Dosyası Silme	+
Cihazda Uygulama Çalıştırma	+
Cihazdaki Web Kameralarının Listesini Görme	+
Ön Kamera veya Arka Kamera ile Görüntü Çekme	+
Cihazdaki Ekran Görüntüsünü Alma	-
Cihazın Yerel Tarih ve Saatini Görüntüleme	+
Ses Kaydetme	+
Cihazda Müzik Dosyası Çalıştırma	+
SMS Gönderme	-
SMS'leri Okuma	+
Arama Kaydı Listesini Elde Etme	+
Kişi Listesini Kaydetme	+
Shell Alma	+
Cihazda İstediğin URL Adresini Başlatma	+
Uygulama Simgesini Başlatıcıda Gizleme	+
Görüntülü Sohbet Başlatma	-
Konum Belirleme	+
Post Modülü Çalıştırma	-
Root Olarak Çalışıp Çalışmadığını Tespit Etme	+

4.2. Android Cihazda Zararlı Yazılımın Adli Bilişim Bakımından Analizi

Tez çalışmasının amacının gerçekleşebilmesi için incelenmesi yapılacak Android 4.2.2 işletim sistemi yüklü Huawei P7-L10 16 GB modeline sahip Android telefona, zararlı apk dosyaları yüklenilerek, uygulamalar çalıştırılmıştır. Android işletim sistemine sahip akıllı telefonun adli incelemesini gerçekleştirmek için mantıksal ve fiziksel imajların alınarak adli kopya üzerinden incelenmesi gerekmektedir. İncelenecek cihazın imaj alma, verileri ayıklama, analiz etme ve rapor oluşturma işlemlerini yapan açık kaynak ve ticari olan Magnet AXIOM adli aracı kullanılmıştır. Manuel inceleme işlemi için Android cihaz USB kablo aracılığı ile bilgisayara aktarılarak analiz

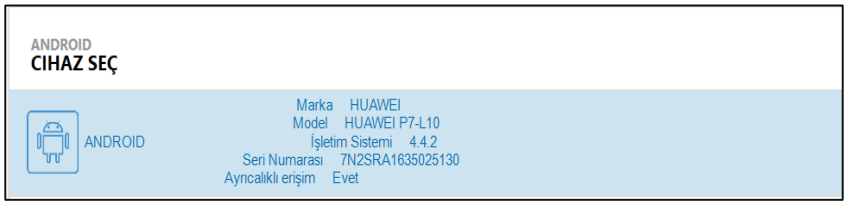
edilmiştir. Zararlı olduğu düşünülen apk dosyalarının analizi apktool aracı kullanılarak gerçekleştirilmiştir. Android cihazın adli analizinde kullanılan yazılımlar Tablo 4.3'te gösterilmiştir.

Tablo 4.3. Android Cihazın Analizinde Kullanılan Yazılımlar

Kullanılan Yazılım	Kullanım Amacı
Apktool 2. 6.0	İnceleme Aracı
Magnet AXIOM 3.0.0	İnceleme Aracı
Kingo ROOT	Cihazı Root Etme Aracı

4.2.1. Magnet AXIOM 3.0.0 Aracı ile Zararlı Uygulamaların Adli Analizinin Gerçekleştirilmesi

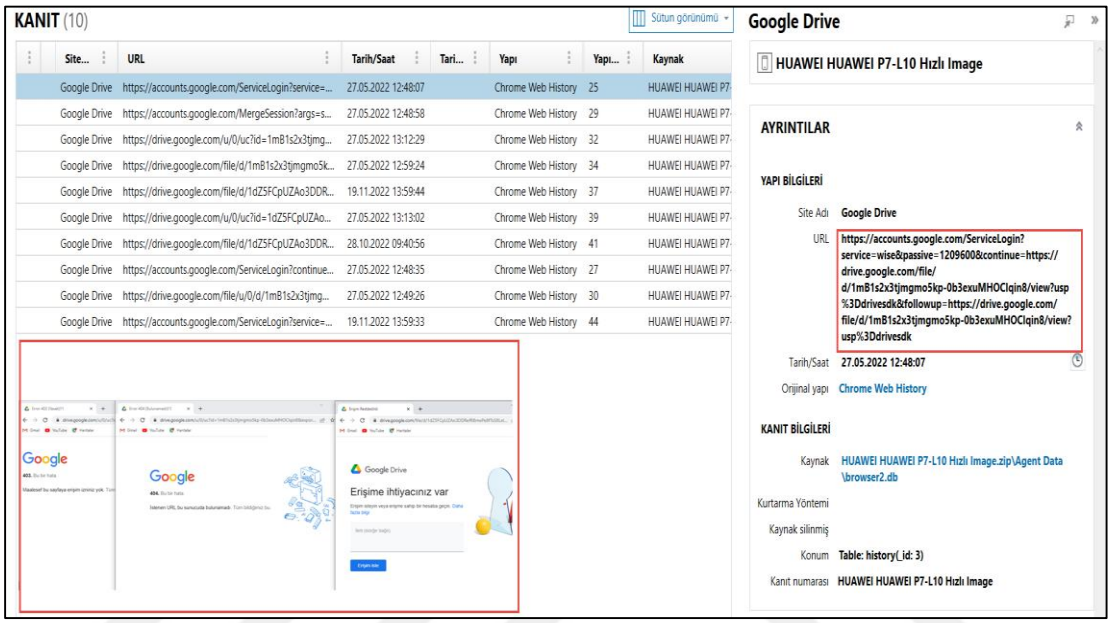
Magnet Axıom; akıllı telefon, bilgisayar veya bulut gibi tüm veri kaynaklarından en ilgili kanıtları toplamak için kullanılmaktadır. Magnet Axıom, verileri akıllıca görselleştirebilir ve analiz edebilir, verileri doğrulayabilir ve diğer araçlarla elde edilen görüntüleri incelemek üzere tek bir vaka dosyasında birleştirebilme özelliklerine sahiptir. Magnet Axıom 3.0.0 aracının imajı alınacak cihazı seçme ekranı Şekil 4.6'daki gibidir.



Şekil 4.6. Magnet Axıom Aracı ile İmajı Alınacak Cihazı Seçme Ekranı

Android 4.2.2 işletim sistemi yüklü Huawei P7-L10 16 GB modeline sahip akıllı telefonun öncelikle Magnet AXIOM 3.0.0 adli aracı ile mantıksal imajı alınmıştır. Daha sonra Android işletim sistemine sahip akıllı telefona Kingo ROOT aracı kullanılarak root işlemi gerçekleştirilip fiziksel imajı alınmıştır. Mantıksal ve fiziksel imajlar alınarak Android işletim sistemine sahip akıllı telefon analiz edilmiştir.

Browser.db ile elde edilen kanıtlar incelendiğinde belirli tarih ve saatlerde Google Drive Url adreslerinin bulunduğu tespit edilerek, URL adresleri virüstotal gibi platformlarda incelenerek zararlı olduğuna dair tespitler yapılmıştır. Fakat ilgili Url adreslerine erişilmek istediğinde Şekil 4.7'de görüldüğü gibi hata kodlar tespit edilmiştir.



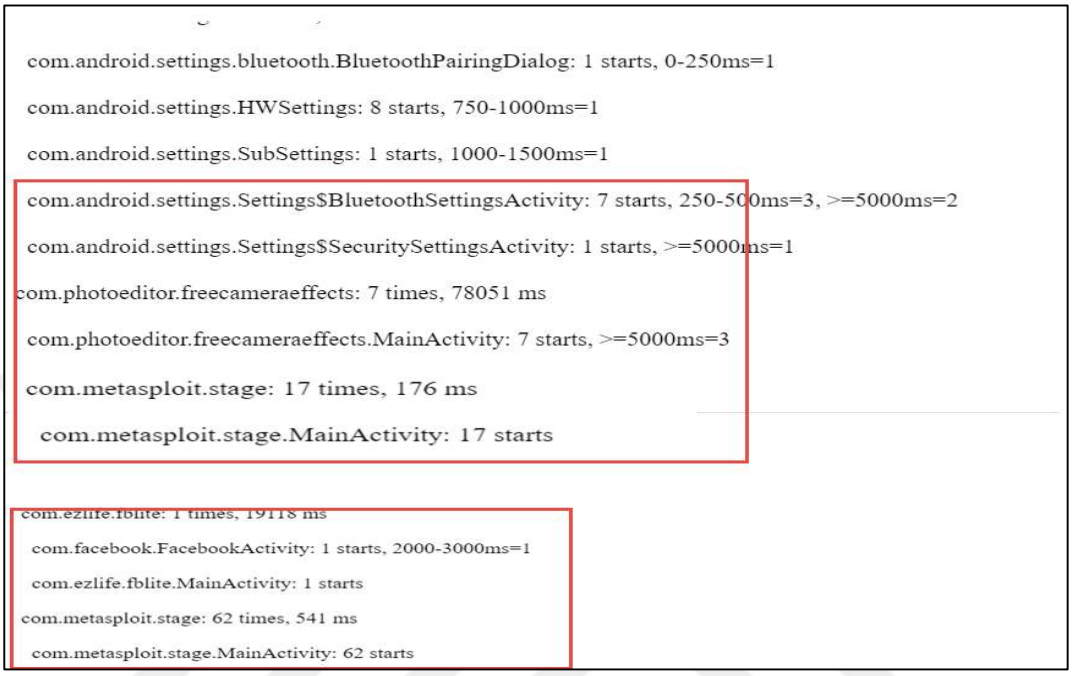
Şekil 4.7. Google Drive URL Adresleri Bulguları

Chrome Web Geçmişine dair kanıtlar incelendiğinde, Google drive yardiminstagram.apk uygulaması indirilirken indirme uyarısı aldığı Şekilde 4.8'de görüldüğü gibi tespit edilmiştir.

URL	Son Ziyaret...	Başlık	Ziya...	Türü
https://www.vodafone.com/	19.05.2022 10:20:48	Home	1	
http://ab.tek.firat.edu.tr/	27.05.2022 12:47:59	ab.tek.firat.edu.tr	2	
https://accounts.google.com/ServiceLogin?service=...	27.05.2022 12:48:07	Google Drive: Oturum Açın	3	
https://accounts.google.com/ServiceLogin?continue...	27.05.2022 12:48:35	Google Drive: Oturum Açın	2	
https://accounts.google.com/MergeSession?args=s...	27.05.2022 12:48:58	Google Drive: Oturum Açın	5	
https://drive.google.com/file/u/0/d/1mB1s2x3tjmg...	27.05.2022 12:49:26	yardiminstagram.apk - Google Drive	2	
https://drive.google.com/u/0/uc?id=1mB1s2x3tjmg...	27.05.2022 13:12:29	Google Drive - İndirme uyarısı	5	
https://drive.google.com/file/d/1mB1s2x3tjmgmo5k...	27.05.2022 12:59:24	yardiminstagram.apk - Google Drive	6	
https://drive.google.com/file/d/1dZ5FCpUZAo3DDR...	19.11.2022 13:59:44	Google Drive: Oturum Açın	5	
https://drive.google.com/u/0/uc?id=1dZ5FCpUZAo...	27.05.2022 13:13:02	Google Drive - İndirme uyarısı	1	
https://drive.google.com/file/d/1dZ5FCpUZAo3DDR...	28.10.2022 09:40:56	Web sayfası yok	1	
http://abm.tf.firat.edu.tr/	19.11.2022 14:58:21	Web sayfası yok	2	
https://accounts.google.com/ServiceLogin?service=...	19.11.2022 13:59:33	Google Drive: Oturum Açın	4	
http://cep.vodafone.com.tr		Vodafone Web Sitesi	0	
http://m.vodafone.com.tr		Vodafone Self Servis	0	
http://Forum.vodafone.com.tr		Vodafone Forum	0	

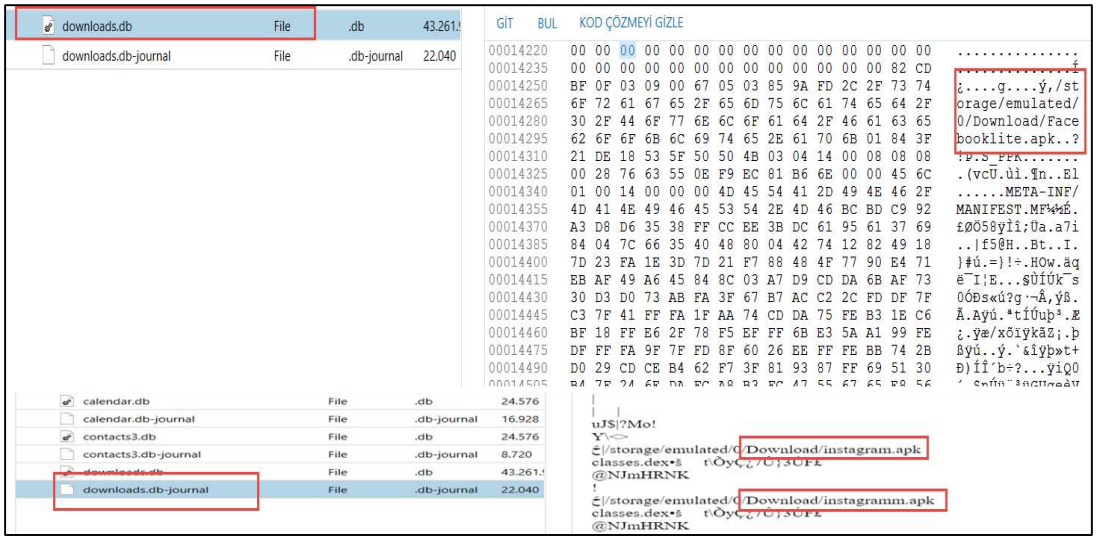
Şekil 4.8. Google Drive İndirme Uyarısı

Usage.txt dosyasındaki bulgular incelendiğinde FacebookLite, photeditor uygulamalarından sonra Şekil 4.9'da görüldüğü gibi metasploit'in çalıştırıldığı tespit edilmiştir.



Şekil 4.9. Uygulamalardan Sonra Metasploit Çalıştırıldığına Dair Bulgu

Carvied archieved dosyaları incelendiğinde instagram.apk, Facebooklite.apk dosyalarının Şekil 4.10'da görüldüğü gibi indirildiği tespit edilmiştir.



Şekil 4.10. Carvied Archieved Uygulamaların İndirildiği Dair Bulgular

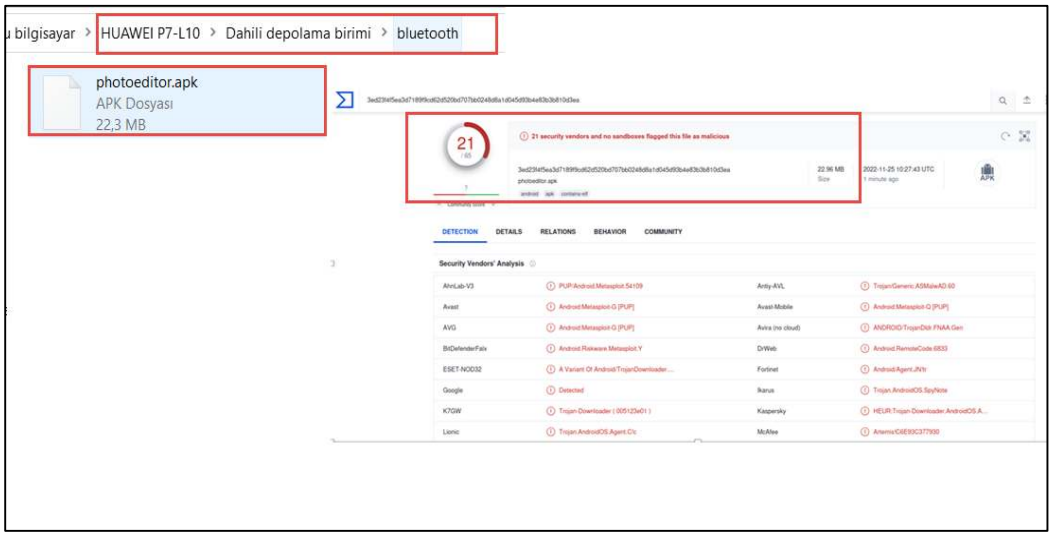
Magnet AXIOM ile gerçekleştirilen mantıksal ve fiziksel imaj inceleme sonuçlarında zararlı yazılımlara ilişkin elde edilen kanıtlar Tabloda 4.4'te gösterilmiştir.

Tablo 4.4. Magnet Axiom Aracı ile Yapılan Zararlı Uygulamalar İle İlgili Elde Edilen Veriler

Zararlı Uygulamalar İle İlgili Elde Edilen Deliller	**Fiziksel İmaj**	**Mantıksal İmaj**
Google Drive Linkleri	+	+
Bluetooth İle Yüklenilen Uygulamalar	+	+
Zararlı Uygulamanın Çalıştırıldığına Dair Bulgu	+	+
Silinen Uygulamalar	+	-
Uygulamanın Kim Tarafından Gönderildiğine Dair Bulgu	-	-
Metasploitin Çalıştırıldığı Konuma Ait Bulgu	-	-
Web Tarayıcı Geçmişi	+	+
Uygulamaların Analizi	-	-
Ransonware Uygulamasına Dair Bulgu	+	+

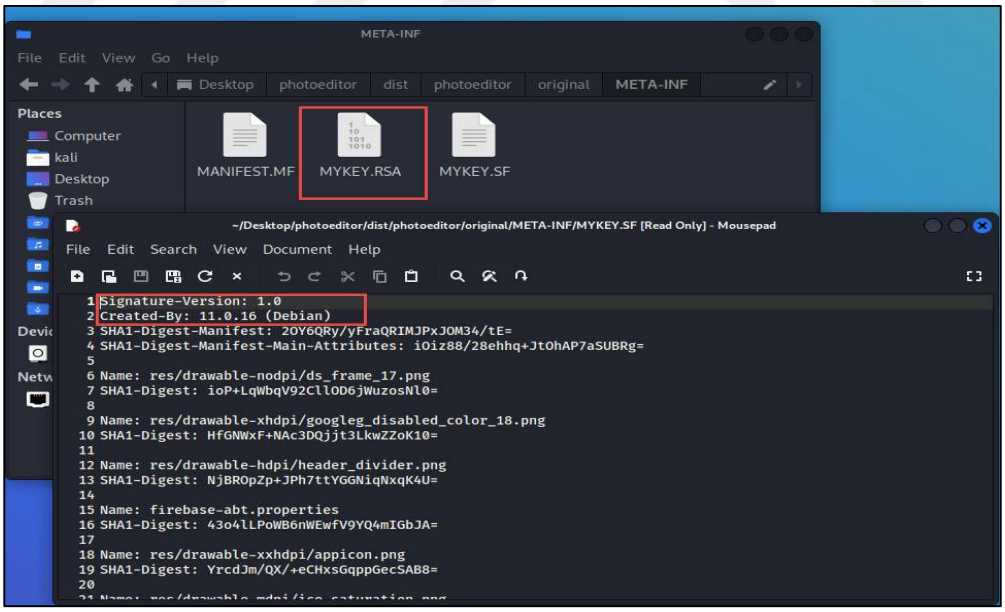
4.2.2. Manuel İnceleme ile Adli Analiz Gerçekleştirilmesi

Android 4.4.2 işletim sistemi yüklü Huawei P7-L10 16 GB modeline sahip akıllı telefon USB kablo aracılığı ile bilgisayara aktarılmıştır. Cihazın dahili depolama biriminde bulunan klasörler manuel olarak incelenmiştir. Bluetooth klasöründe Şekil 4.11'de görüldüğü gibi photoeditor.apk dosyası tespit edilmiştir. Virüstotal sitesi üzerinde photoeditor.apk dosyası yüklenilerek antivirüsler tarafından zararlı olarak tespit edildiği görülmüştür. Photoeditor.apk dosyasının bulunduğu klasör ile antivirüsler tarafından yapılan analiz sonuçları şekilde gösterilmiştir.



Şekil 4.11. Manuel İnceleme İle Bluetooth Aygıtı Aracılığıyla Yüklenilen Uygulama

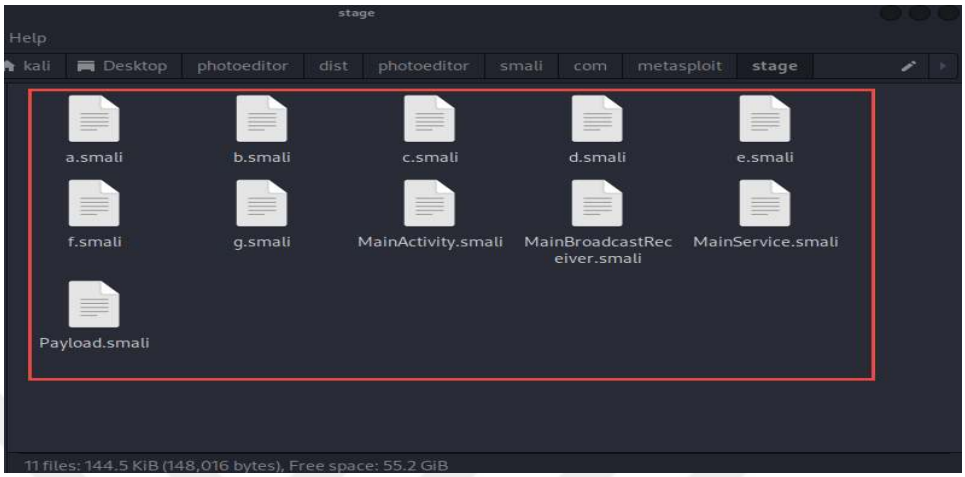
Apktool aracı ile photeditor.apk dosyası decompile edilerek dosyanın analizi gerçekleştirilmiştir. META-INF klasörü imza, apk dosyasının Metadata verilerini içermektedir. META-INF klasörü incelendiğinde apk dosyasının Debian 11.0.6 tarafından yaratıldığı Android uygulamanın Google Play tarafından imzalanmadığı Şekil 4.12'de görülmektedir.



Şekil 4.12. photoeditor.apk META-INF Dosya Analizi

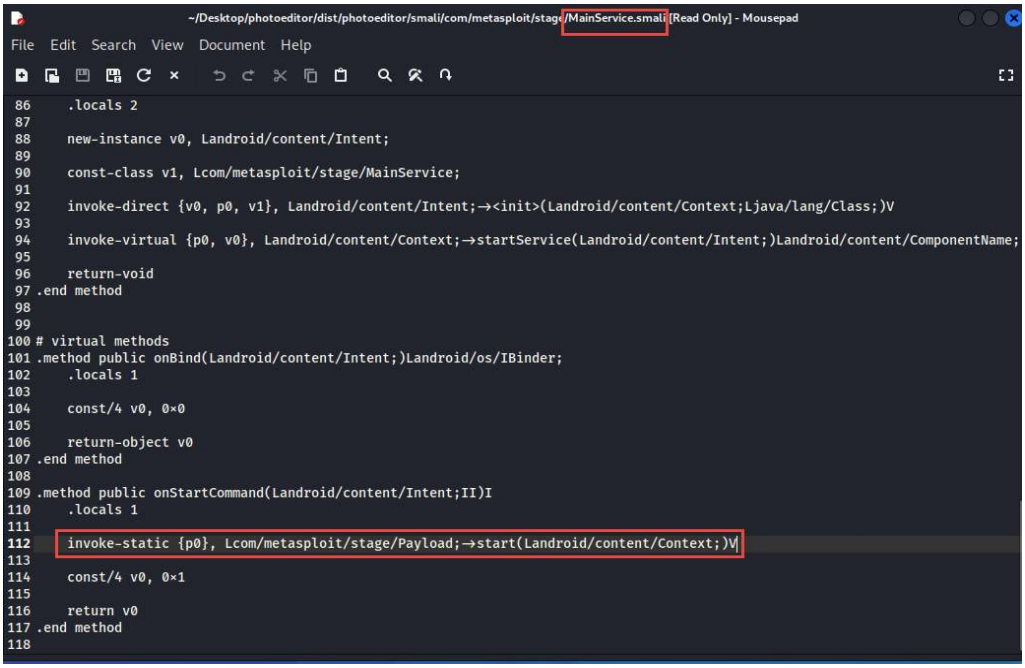
Decompile edilen photoeditor.apk dosyasında smali klasörü bulunmaktadır. Apk Android uygulama arşivlerinde saklanan dex uygulaması yürütülebilir dosyaları yeniden derlenmesi için smali klasörü programcılar tarafından kullanılmaktadır. Smali klasörü içerisinde Şekil 4.13'te görüldüğü gibi metasploit klasörü tespit edilmiştir. Payload.smali reverse shell'in alınmasını

sağlayan shell code bulunmaktadır. Bu dosyaların orijinal photoeditor.apk'ya dahil edildiği tespit edilmiştir.



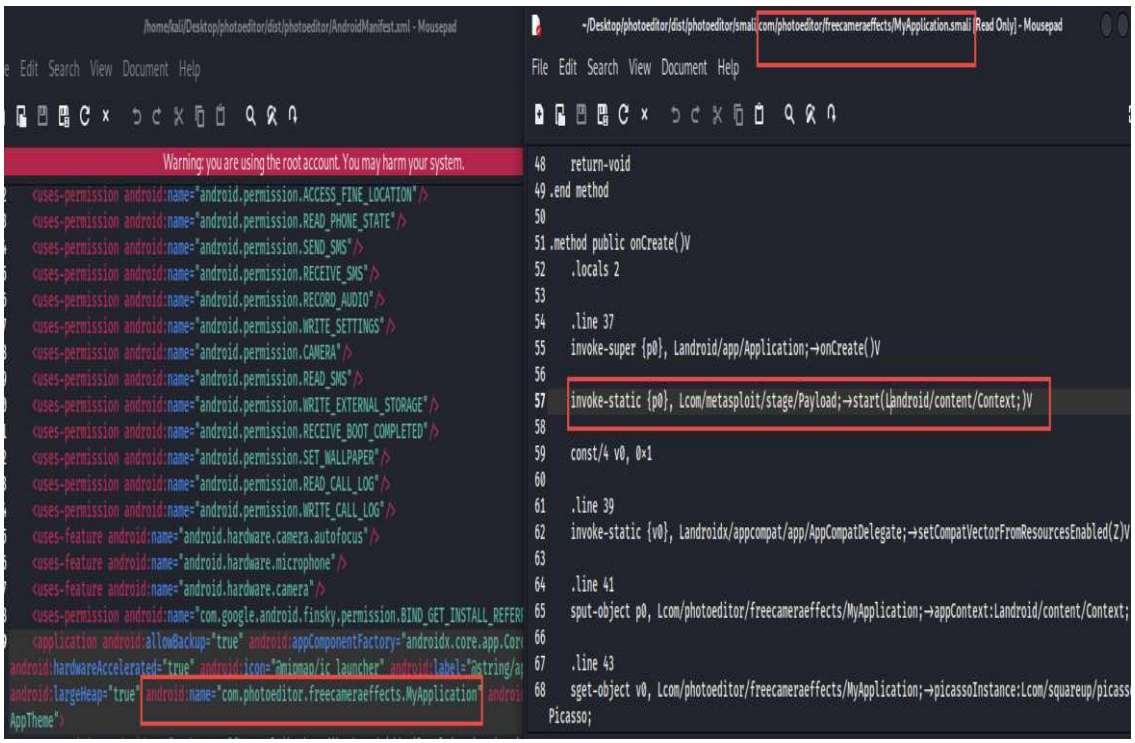
Şekil 4.13. Photoediotr.apk Smali Klasörü Analizi

Mainservice.smali dosyası içerisinde tüm uygulamalar tarafından erişilebilir public metota dair komut tespit edilmiştir. Şekil 4.14'te görüldüğü gibi komut incelendiğinde payload'ı çalıştırdığı görülmektedir.



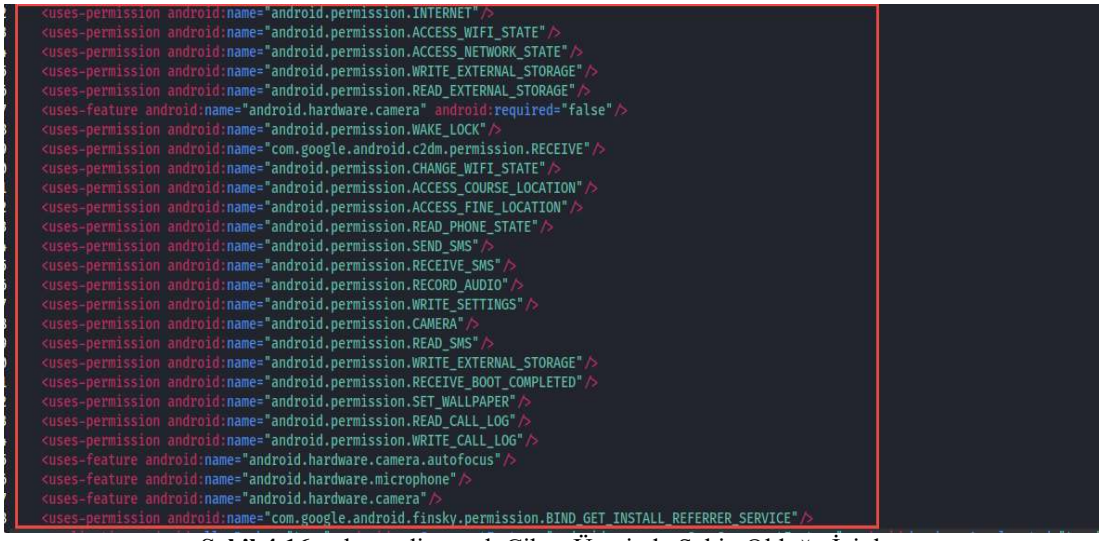
Şekil 4.14. hotoeditor.apk Payload Çalıştıran Komut Tespiti

Androidmanifest.xml dosyası içerisinde paketin adının bulunduğu yol takip edildiğinde MyApplication.smali dosyasında Şekil 4.15'te görüldüğü gibi payload'ı çalıştırmaya yarayan komutun uygulamanın başlangıcına eklendiği tespit edilmiştir.



Şekil 4.15. photeditor.apk Komutun Uygulamanın Başlangıcına Eklendiğine Dair Bulgul

Uygulamanın yüklenildiği takdirde Androidmanifest.xml dosyasında Şekil 4.16'da görüldüğü gibi cihaz üzerinde; telefonun durumunu/kimliğini okuma, SMS mesajlarının alma/okuma/gönderme, resim çekme, görüntü kaydetme, ses kaydetme, GPS ve ağ tabanlı konuma erişim, arama günlüğünü okuma/yazma mesajları okuma, SD kartın içeriğini okuma/değiştirme/silme, ağ bağlantılarını görüntüleme, ağ erişimi, başlangıçta çalıştırma, telefonun uykuya geçmesini önleme, duvar kağıdını ayarlama, sistem ayarlarını değiştirme gibi çeşitli izinlere sahip olduğu tespit edilmiştir.

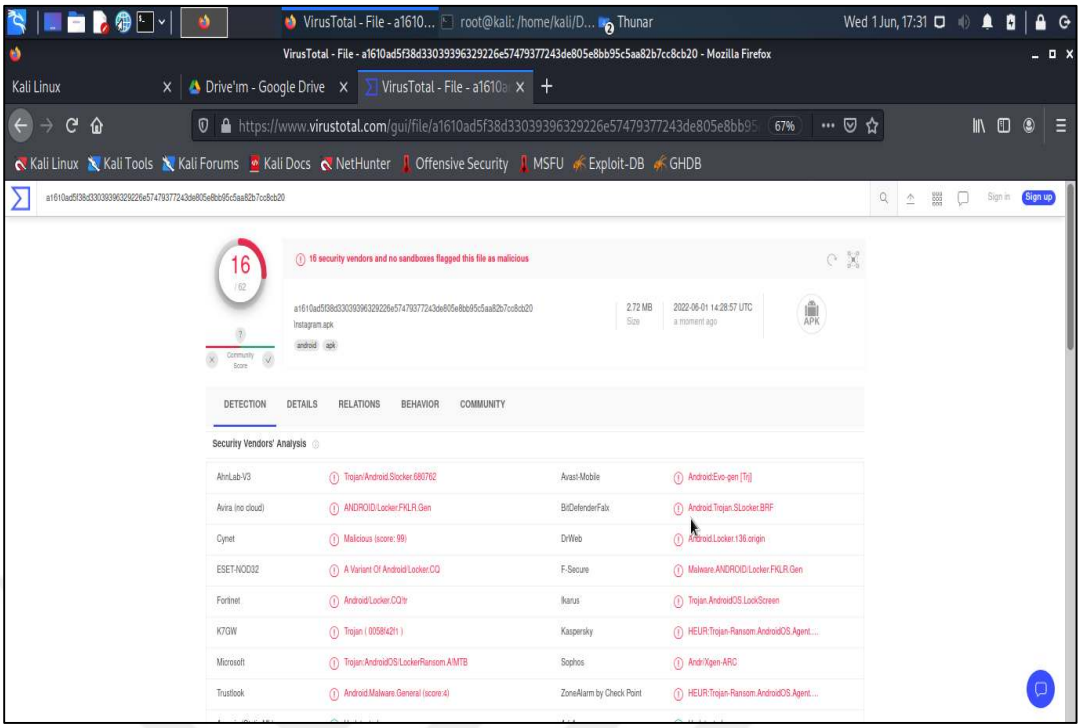


Şekil 4.16. photoeditor.apk Cihaz Üzerinde Sahip Olduğu İzinler

Cihazın manuel olarak incelenmesi gerçekleştirilirken indirilenler klasöründe çeşitli apk dosyaları bulunmaktadır. İndirilenler klasörünüde bulunan apk dosyaları Şekilde 4.17'de gösterilmiştir.

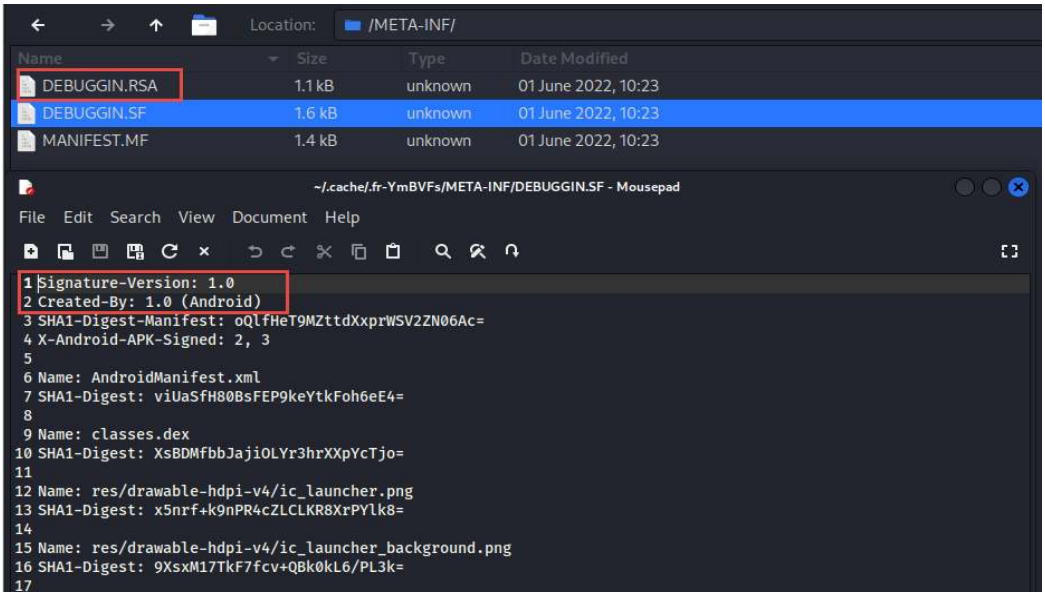
Şekil 4.17. Manuel İnceleme İle Download Klasöründe Tespit Edilen Uygulamalar

İndirilenler klasöründe bulunan instagram.apk dosyasının antivirüsler tarafından analizi Şekil 4.18'de gösterildiği gibi zararlı olarak tespit edildiği görülmektedir.



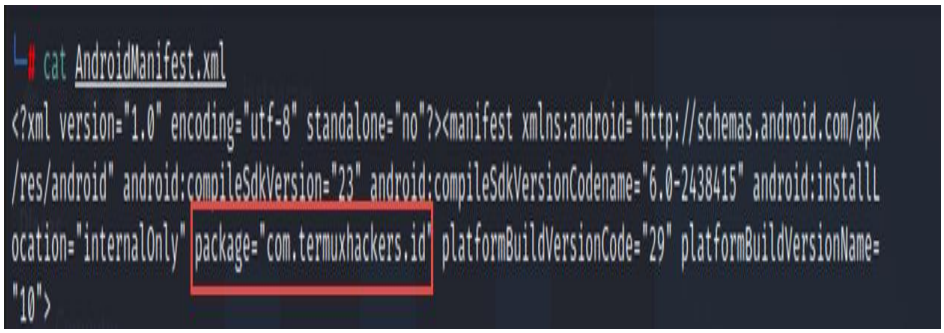
Şekil 4.18. instagram.apk Virüstotal Analizi

İnstagram.apk dosyası apktool aracı ile decompile edilmiştir. META-INF klasörü incelendiğinde instagram.apk dosyasının Android 1.0 tarafından yaratıldığı fakat Android uygulamasının Google Play tarafından imzalanmadığı Şekil 4.19'da görülmektedir.



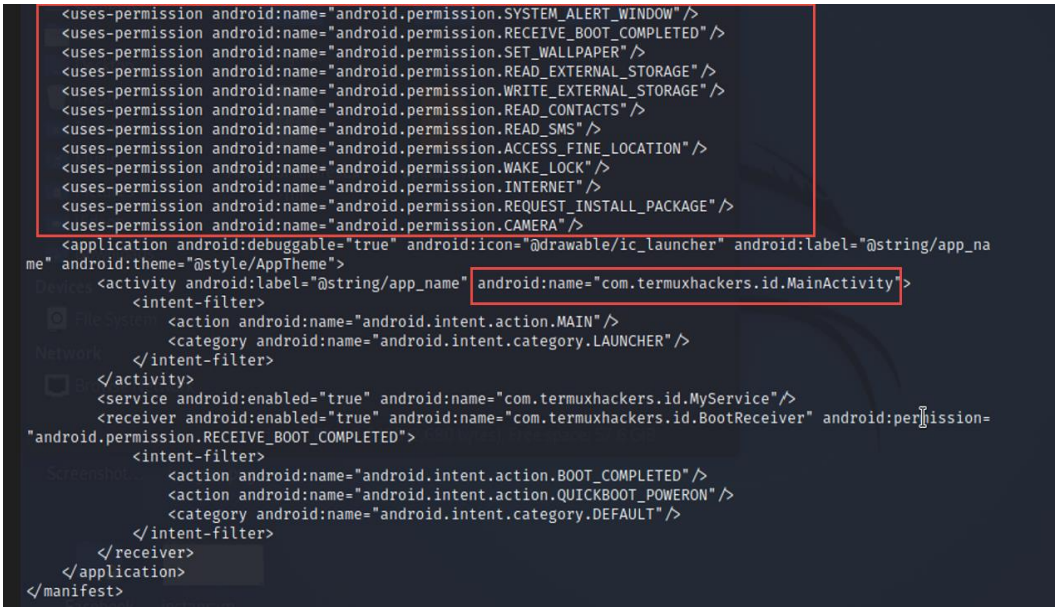
Şekil 4.19. İnstagram.apk META-INF Klasörü Analizi

Androidmanifest.xml dosyası incelendiğinde paket adının ‘com.termuxhackers.id’ olduğu Şekil 4.20’de görüldüğü gibi tespit edilmiştir.



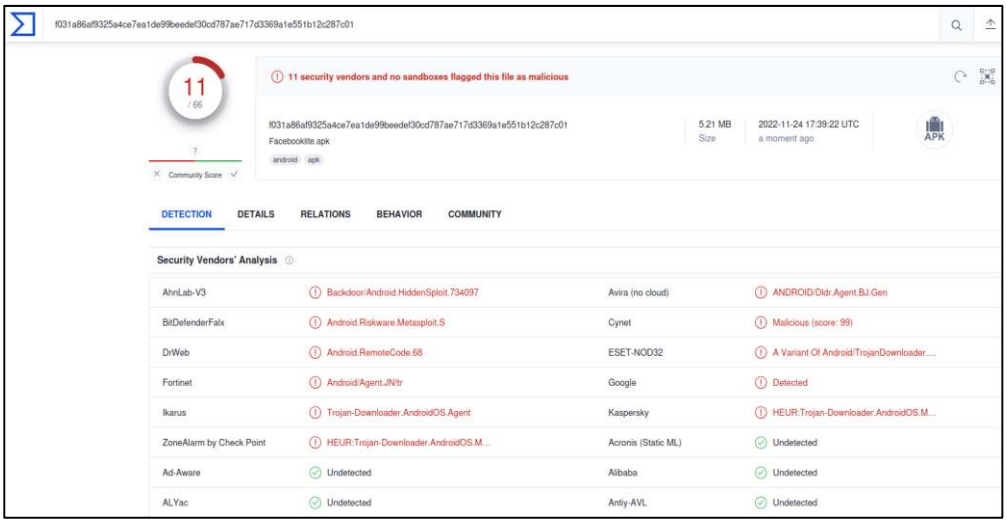
Şekil 4.20. instagram.apk Uygulama Paket Adı

Uygulamanın yüklenildiği takdirde Androidmanifest.xml dosyasında Şekil 4.21’de görüldüğü gibi cihaz üzerinde; mesajları okuma, resim çekme, görüntüyü kaydetme, konuma erişim, kişileri okuma, SD kartın içeriğini okuma/değiştirme/silme, ağ erişimi, uygulamaları sürükleme, başlangıçta çalıştırma, telefonun uykuya geçmesini önleme gibi çeşitli izinlere sahip olduğu tespit edilmiştir



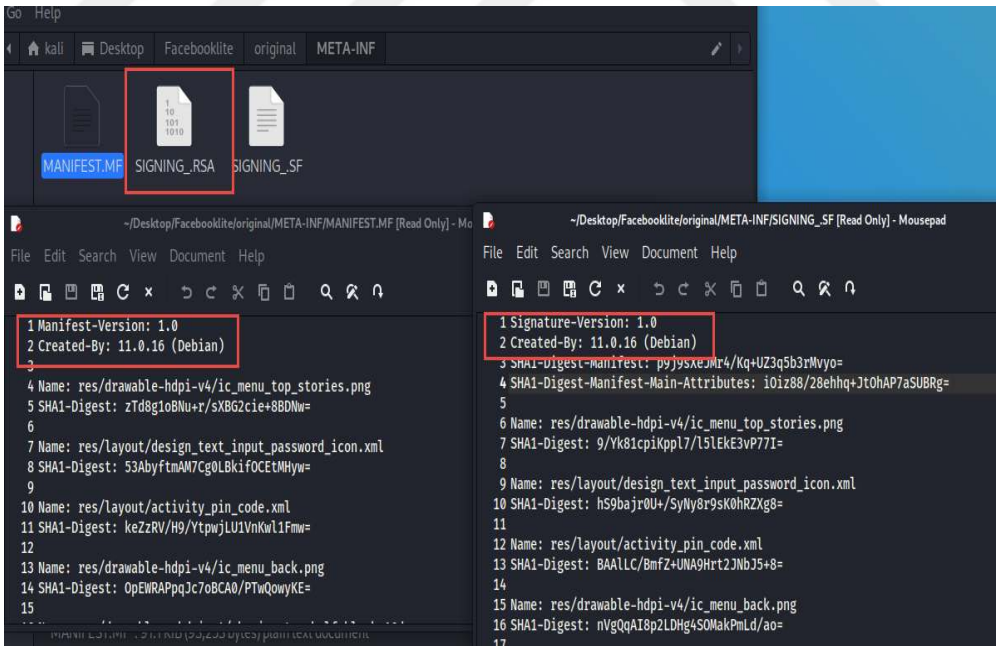
Şekil 4.21. instagram.apk Uygulamasının Cihaz Üzerinde Sahip Olduğu İzinler

İndirilenler klasöründe Facebooklite.apk dosyasının antivirüsler tarafından Şekil 4.22’de görüldüğü üzere zararlı olarak tespit edildiği görülmektedir.



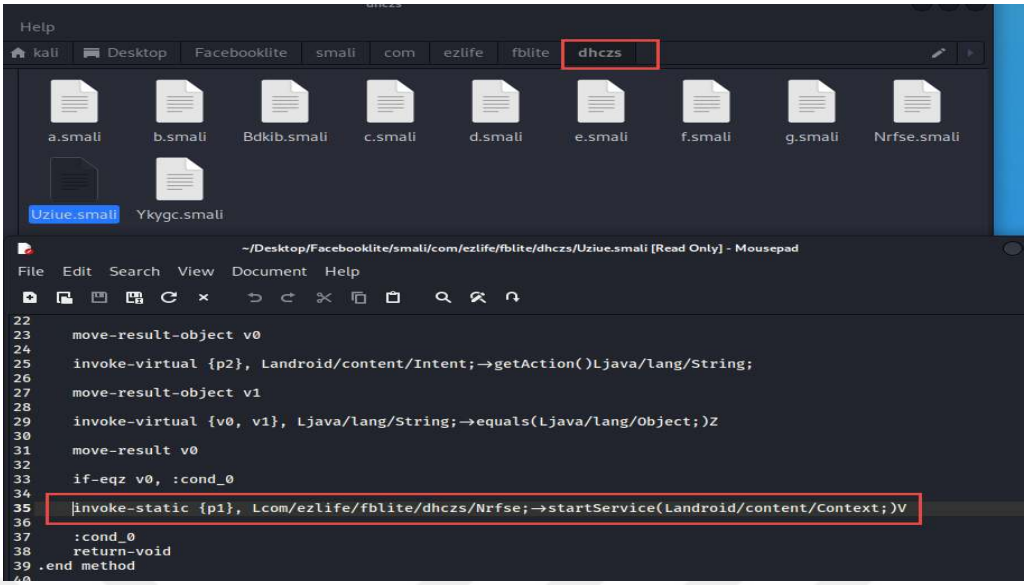
Şekil 4.22. Facebooklite.apk Virüstotal Analiz Sonuçları

Facebooklite.apk dosyası apktool aracı ile decompile edilmiştir. META-INF klasörü imza, apk dosyasının Metadata verilerini içermektedir. META-INF klasörü incelendiğinde Facebooklite.apk dosyasının Debian 11.0.6 tarafından yaratıldığı Android uygulamanın Google Play tarafından imzalanmadığı Şekil 4.23'te görülmektedir.



Şekil 4.23. Facebooklite.apk META-INF Klasörü Analizi

Activity altında bulunan ilgili yol takip edildiğinde 'dhczs' adlı klasör altında metasploit aracının oluşturduğu smali dosyaları tespit edilmiştir. Smali dosyaları incelendiğinde reverse shell'in alınmasını sağlayan shell code bulunmuştur. Payload'ı çalıştıran komut Şekil 4.24'te gösterilmiştir.



Şekil 4.24. Facebooklite.apk Payload Çalıştıran Komut

Androidmanifest.xml dosyası incelendiğinde uygulamanın yüklendiği taktirde cihaz üzerinde; Şekil 4.25'te görüldüğü gibi GPS ve ağ tabanlı konuma erişim, SD kartın içeriğini okuma/değiştirme/silme, ağ erişimi, ağ bağlantılarını görüntüleme, internetten veri alma, başlangıçta çalıştırma, titreşimi denetleme, telefonun uykuya geçmesini önleme gibi çeşitli izinlere sahip olduğu tespit edilmiştir.

Şekil 4.25. Facebooklite.apk Cihaz Üzerinde Sahip Olduğu İzinler

Manuel inceleme sonuçlarında zararlı yazılımlara ilişkin elde edilen kanıtlar Tabloda 4.5'te gösterilmiştir.

Tablo 4.5. Manuel İnceleme Sonucunda Zararlı Uygulamalar İle İlgili Elde Edilen Veriler

Zararlı Uygulamalar İle İlgili Elde Edilen Deliller	**Manuel İnceleme**
Google Drive Linkleri	+
Bluetooth İle Yüklenilen Uygulamalar	+
Zararlı Uygulamanın Çalıştırıldığına Dair Bulgu	-
Silinen Uygulamalar	-
Uygulamanın Kim Tarafından Gönderildiğine Dair Bulgu	-
Metasploitin Çalıştırıldığı Konuma Ait Bulgu	-
Web Tarayıcı Geçmişi	+
Uygulamanın Kendisine Ait Dosya	+
Ransonware Uygulamasına Dair Bulgu	+
Uygulamaların Analizi	+

5. BULGULAR VE TARTIŞMA

Tez çalışmasında, Android işletim sistemine sahip Android cihazda oluşturulan zararlı uygulamalar adli bilişim araçları ile incelenmiştir. Android işletim sistemine sahip cihazdaki delillerin bütünlüğünü bozmamak için öncelikle incelenen cihazın adli kopyası(imaj) alınarak imaj dosyası üzerinden analizler gerçekleştirilmiştir. Adli bilişim araçlarıyla öncelikle mantıksal imajlar alınmıştır. Mantıksal olarak imaj alma yönteminde; mobil işletim sistemleri verilerin bir kısmına erişim izni vermektedir. Mantıksal imaj ile elde edilen delil niteliğindeki veriler genel olarak; arama kayıtları, SMS, fotoğraflar, videolar, ses dosyaları gibi verilerdir. Fiziksel imaj ise mantıksal imajın aksine Android cihazın tüm belleğinin birebir kopyasını almaktadır. Fiziksel imaj ile kullanıcının erişebildiği alanlarla birlikte ayrılmamış alandaki veriler ve silinmiş verilerde bulunabilir. Fiziksel imaj ile elde edilen delil niteliğindeki veriler; arama kayıtları, SMS, fotoğraflar, videolar, silinmiş mesajlar, silinmiş arama kayıtları, e-postalar, uygulama verileri ve daha fazla elde edilebilecek veri tipleridir. Fiziksel imaj ile mantıksal imaja göre daha fazla kapsamlı inceleme yapılarak, delil niteliğindeki silinmiş verilere, ayrılmış alandaki verilere ulaşılabilir. Mantıksal ve fizikse imaj ile yapılan zararlı yazılım analizi sonucunda yeterli delilin elde edilememesi noktasında manuel inceleme gerçekleştirilebilmektedir. Manuel inceleme ile verilerin kaybolabilmesi gibi riskler bulunmaktadır. Fakat mantıksal ve fiziksel imaj ile export edilemeyen apk dosyalarının statik ve dinamik analizi manuel inceleme yöntemi ile analiz edilebilmektedir. Manuel inceleme yönteminde silinen verilere, cihazdaki tüm verilere ulaşılamamaktadır.

Adli kopyalar; Magnet AXIOM mobil adli inceleme aracı kullanılarak analiz edilmiştir. Yapılan analiz sonucunda Android işletim sistemine sahip Android cihazı incelemek için kullanılan adli araçların; adli inceleme araçlarının sürümleri, mobil cihazın işletim sistemi, modeli, markası, uygulamaların sürüm versiyonu gibi nedenlere bağlı olarak veri elde etme performansları değişiklik gösterebilmektedir. Android işletim sistemine sahip Android cihazda zararlı yazılımların incelenmesi sonucunda bu uygulamalara ait detaylı bulgular elde edilememektedir. Aynı zamanda mobil adli incelemeyi yapan adli bilişim araçlarının yazılım arayüzleri anlaşır ve kolay kullanıma sahip olduğu sonucuna varılabilmektedir Elde edilen analiz sonuçları incelendiğinde; daha kapsamlı verilere (silinmiş veriler, ayrılmamış alanlardaki veriler vb.) ulaşabilmek için fiziksel imaj alınarak analiz yapılması gerekmektedir. Fiziksel imaj alınamaması durumunda (cihaza root yetkisi verememe vb) mantıksal imaj alınarak incelemeler gerçekleştirilebilir. Android cihazda zararlı uygulamaların statik ve dinamik analizinin yapılabilmesi noktasında manuel olarak inceleme gerçekleştirilebilmektedir.

Sonuç olarak Tablo 5.1'e bakıldığında Android cihazda zararlı yazılım incelenmesi için mantıksal imaj, fiziksel imaj ve manuel inceleme performanslarına bakıldığında üç inceleme yönteminde zararlı uygulamaların varlığı tespit edilmiştir. Saldırgan tarafından yapılan eylemlerin neler olduğu konusunda üç inceleme yöntemi ile bulgu bulunamamıştır. Zararlı uygulamaların yüklenip çalıştırıldığı noktada metasploit'in ne kadar çalıştırıldığı konusunda mantıksal ve fiziksel imaj yöntemi ile elde edilebilirken manuel inceleme yönteminde metasploit'in çalıştırılma sayısına dair bulgu bulunamamıştır. Silinmiş uygulamalara ait bulgulara fiziksel imaj yöntemi ile erişilebilirken, mantıksal ve manuel inceleme yöntemi ile tespit edilememiştir. Uygulamaların statik ve dinamik analizi mantıksal ve fiziksel imaj yöntemleri ile gerçekleştirilemiyorken manuel inceleme yöntemi ile gerçekleştirilmiştir.

Tablo 5.1. Mobil Adli Bilişim Araçları ile Zararlı Yazılımlara Ait Bulguların Karşılaştırılması

Zararlı Uygulamalar İle İlgili Elde Edilen Deliller	**Manuel İnceleme**	**Fiziksel İmaj**	**Mantıksal İmaj**
Google Drive Linkleri	+	+	+
Bluetooth İle Yüklenilen Uygulamalar	+	+	+
Zararlı Uygulamanın Çalıştırıldığına Dair Bulgu	-	+	+
Silinen Uygulamalar	-	+	-
Uygulamanın Kim Tarafından Gönderildiğine Dair Bulgu	-	-	-
Metasploitin Çalıştırıldığı Konuma Ait Bulgu	-	-	-
Web Tarayıcı Geçmişi	+	+	+
Uygulamaların Analizi	+	-	-
Ransonware Uygulamasına Dair Bulgu	+	+	+

6. SONUÇLAR

Yapılan tez çalışmasında; Android cihaz için Ransonware uygulaması, tool ile orijinal apk dosyasına backdoor yerleştirilerek trojan ve manuel olarak orijinal uygulamaya payload enjekte edilerek trojan oluşturulmuştur. Oluşturulan zararlı apk dosyaları Google Drive ve Bluetooth aygıtı aracılığıyla Android cihaza yüklenerek sızma testi senaryosu gerçekleştirilmiştir. Android cihazda zararlı yazılım analizinin adli bilişim bakımından gerçekleştirilmesi noktasında mobil adli bilişim araçlarının(manuel inceleme, fiziksel imaj, mantıksal imaj) karşılaştırılması yapılmıştır.

Teknolojinin ilerlemesiyle birlikte günümüzde mobil cihazların kullanımı gün geçtikçe artmaktadır. Mobil cihaz kullanıcı sayısının artmasıyla birlikte mobil işletim sistemleri güncellenmekte ve farklı işletim sistemlerine sahip cihazlar piyasaya sürülmektedir. Bu nedenle siber suçların gerçekleştirilmesinde mobil cihazlar büyük rol oynamaktadır. Adli bir soruşturmada mobil cihazlardan elde edilen delillerin soruşturmanın açığa kavuşturulmasındaki öneminden bahsedilmiştir.

Siber suçların artmasıyla birlikte, bilişim yolu kullanılarak işlenilen suçlar adli bilişim kavramını ortaya çıkarmıştır. Adli bilişimin genel bir tanımı yapılarak adli bilişim süreçlerinde kullanılan tanımlama, koruma, inceleme, analiz ve raporlama aşamalarından bahsedilmiş olup cihazların çeşitliliği ve farklı özelliklere sahip olması nedeniyle adli bilişimin farklı alt dallara ayrıldığına değinilmiştir.

Mobil cihazların adli olarak incelenmesinin doğru bir şekilde gerçekleştirebilmek için; mobil cihaz türleri(akıllı telefonlar, tabletler, giyilebilir cihazlar vb.), mobil cihazların sahip olduğu işletim sistemleri(Palm OS, Windows Mobile OS, IOS, Android OS VB.),mobil cihazların adli bilişim süreç aşamaları, mobil cihazlardan veri toplama türleri(fiziksel edinim, mantıksal edinimi, manuel edinim), mobil cihazları inceleyen adli bilişim yazılımlarını(Cellebrite, Oxygen Forensic, Paraben, Magnet AXIOM, MOBILEdit Forensic, SAFT vb.) ve mobil cihazların adli incelemesinde karşılaşabilecek sorunlardan bahsedilmiştir.

Günümüzde saldırganlar tarafından kullanıcıların kullandığı mobil cihazlar hedef odağı olmaktadır. Mobil cihaz türlerinden pazar payı oranı yüksek olan Android cihazlar, saldırganın cihazda depolanan, cihaz tarafından aktarılan verilere yetkisiz erişim elde etmeye çalıştığı birçok potansiyel saldırı vektörüne sahiptir. Saldırı vektörleri olan zararlı yazılım türlerinden (Ransonware, trojan,scareware,virüs,worm vb.) bahsedilmiş olup zararlı yazılım analiz teknikleri (statik analiz, dinamik analiz, hybrid analiz) hakkında bilgi verilmiştir. Mobil cihazdaki zararlı yazılımlardan korunmak için alınabilecek önlemlere değinilmiştir.

Son olarak Android işletim sistemine sahip Android cihaz için Ransonware ve trojan içeren zararlı uygulamalar oluşturularak sızma testi senaryosu gerçekleştirilmiştir. Sızma testi işlemi tamamlandıktan sonra Android cihazda zararlı yazılım analizinin adli bilişim bakımından

incelenmesi gerçekleştirilmiştir. Android cihazda zararlı yazılımların analizi Magnet AXIOM adli bilişim yazılım ile mantıksal ve fiziksel imaj dosyaları üzerinden analizi yapılmıştır. Manuel inceleme yöntemi ile zararlı uygulamaların statik ve dinamik analizi gerçekleştirilmiştir.

Yapılan incelemeler sonucunda Android cihazda zararlı yazılım incelenmesi için mantıksal imaj, fiziksel imaj ve manuel inceleme performanslarına bakıldığında üç inceleme yönteminde zararlı uygulamaların varlığı tespit edilmiştir. Saldırgan tarafından yapılan eylemlerin neler olduğu konusunda üç inceleme yöntemi ile bulgu bulunamamıştır. Zararlı uygulamaların yüklenip çalıştırıldığı noktada metasploit'in ne kadar çalıştırıldığı konusunda mantıksal ve fiziksel imaj yöntemi ile elde edilebilirken manuel inceleme yönteminde metasploit'in çalıştırılma sayısına dair bulgu bulunamamıştır. Silinmiş uygulamalara ait bulgulara fiziksel imaj yöntemi ile erişilebilirken, mantıksal ve manuel inceleme yöntemi ile tespit edilememiştir. Uygulamaların statik ve dinamik analizi mantıksal ve fiziksel imaj yöntemleri ile gerçekleştirilemiyorken manuel inceleme yöntemi ile gerçekleştirilmiştir.

Bu nedenle Android cihazda zararlı yazılım analizinin adli bilişim bakımından gerçekleştirilmesi noktasında en az iki adli bilişim yazılımı ile mantıksal ve fiziksel imaj yöntemi ile incelenmesi yapılabilir. Zararlı uygulamalara ait bulguların tespit edildiği noktada manuel inceleme yöntemi tercih edilerek uygulamaların statik ve dinamik analizinin gerçekleştirilmesi gerektiği gözlemlenmiştir.

ÖNERİLER

Android cihazların işletim sistemlerini ve uygulamalarını sürekli güncelleştirmelerinden dolayı mobil adli bilişim araçlarına devamlı olarak güncelleştirme işlemlerinin yapılması gerekmektedir.
Mobil cihazları inceleyen analistlerin, mobil adli inceleme araçları hakkında yeterli donanım ve tecrübeye sahip olmaları, aynı zamanda gerekli kanıtları elde edebilmek ve verilerin teyit edilmesi işlemini gerçekleştirebilmek için en az iki adli bilişim aracını kullanması gerekmektedir.
Siber suçların gerçekleştirilmesinde rol oynayan mobil cihazların adli bilişim süreçlerine genel bir çerçeve çizilmesi, tecrübelerin aktif olarak bir platform üzerinden paylaşılması ve eğitimlerin gerçekleşmesi gerekmektedir.
Mobil cihazların incelemesini gerçekleştiren adli araçların lisans satın alınarak yapılması, bu alanda yetişecek uzman sayısını kısıtlamaktadır. Bu nedenle mobil cihazlardan veri elde edebilmek için manuel olarak veri elde etme konusunda gerekli eğitimlerin verilmesi önerilmektedir.

KAYNAKLAR

[1] Y. Korkmaz, A. Boyaci, F. Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği Bölümü, Dergisi Science and Eng, J Fırat Univ. 30 (2018) 329–343.

[2] R. Benzer, C. Aliusta, Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, (2019). https://doi.org/10.18640/ubgmd.512829.

[3] B. Önel, E. Irmak, Adli bilişim ve dijital delillerin Windows işletim sistemi üzerinde incelenmesi Computer forensics and examination of digital evidence on windows operating system, J. Polytech. (2021). https://doi.org/10.2339/politeknik.860163.

[4] G. Karatas, A. Akbulut, A.H. Zaim, Mobil Cihazlarda Güvenlik Tehditler ve Temel Stratejiler, Istanbul Commer. Univ. J. Sci. (2016).

[5] Y. Bal, N. Arici, Ü. Eml, M.E. Bakanlığı, E. Bilgisayar, E. Bölümü, G. Üniversitesi, T. Ankara, Mobil Öğrenme Materyali Hazırlama Süreci, Bilişim Teknol. Dergisi. (2011) 7. www.yasinbal.com/moodle (accessed June 3, 2021).

[6] K.D. Lutes, R.P. Mislan, Challenges in mobile phone forensics, IMETI 2008 - Int. Multi-Conference Eng. Technol. Innov. Proc. 1 (2008) 348–352.

[7] V. Rao, V. Cse, J. Kakinada, I.A.S.N. Chakravarthy, Survey on Android Forensic Tools and Methodologies, Int. J. Comput. Appl. 154 (2016) 975–8887.

[8] V.E. Platformlar, Mobil Öğrenme Uygulamalarının Geliştirilmesinde Yöntemler ve Platformlar, (2016).

[9] Y.D. Özdemir, Yeni Medya Ortamlarında Akıllı Telefonlar Üzerine Düsünmek, (n.d.). https://www.researchgate.net/publication/323075023_Yeni_Medya_Ortamlarinda_Akilli_Telefonlar_Uzerine_Dusunmek (accessed June 5, 2021).

[10] S. Krishnan, B. Zhou, M.K. An, Smartphone Forensic Challenges, Int. J. Comput. Sci. Secur. (2019) 183. https://www.researchgate.net/publication/336221775.

[11] C.M. da Silveira, R.T. de Sousa, R. de Oliveira Albuquerque, G.D.A. Nze, G.A. de Oliveira Júnior, A.L.S. Orozco, L.J.G. Villalba, Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware, Appl. Sci. 10 (2020). https://doi.org/10.3390/app10124231.

[12] S.S.G. Punja, R.R.P. Mislan, Mobile Device Analysis, Small Scale Digit. Device Forensics Jourrnal. 2(2008)1,16.,http://www.researchgate.net/profile/Rick_Mislan/publication/228374981_Mobile_device_analysis/links/543920e80cf24a6ddb954572.pdf.

[13] K.D. Lutes, Challenges in Mobile Phone Forensics, (n.d.).

[14] H. Abualola, H. Alhawai, M. Kadadha, H. Otrok, A. Mourad, An Android-based Trojan Spyware to Study the NotificationListener Service Vulnerability, Procedia Comput. Sci. 83 (2016) 465–471. https://doi.org/10.1016/J.procs.2016.04.210.

[15] P. Teufl, M. Ferk, A. Fitzek, D. Hein, S. Kraxberger, C. Orthacker, Malware detection by applying knowledge discovery processes to application metadata on the Android Market (Google Play), Secur. Commun. Networks. 9 (2016) 389–419. https://doi.org/10.1002/SEC.675.

[16] D. Kasiaras, N. Clarke, T. Zafeiropoulos, G. Kambourakis, Android Forensic Data Analyzer (Afda): An Opensource Tool to Automatize Event Correlation Analysis on Android Devices, (2014).

[17] K. Chumachenko, Y. Korkmaz, C. Sakarya, M.C. Co, K. Enstit, A. Dal, B. Dal, T. Dan, M. Sokol, J. Ernstsson, A.M. Bahaa-Eldin, E.E.E. Eldessouky, H. Dag, S.I. Sor, A. Pektaş, T. Acarman, Y. Falcone, J.C. Fernandez, Ç. YÜCEL, Android platformunda zararli yazilim analïzi ïçïn hïbrit kum havuzu geliştïrïlmesï yüksek lisans tezi, Proc. 21st Pan-Hellenic Conf. Informatics - PCI 2017. 2018-Janua (2019) 93. http://www.fit.vutbr.cz/info/szz/%0Awww.bth.se.

[18] F. Tong, Z. Yan, A hybrid approach of mobile malware detection in Android, J. Parallel Distrib. Comput. 103 (2017) 22–31. https://doi.org/10.1016/J.JPDC.2016.10.012.

[19] S. Türker, ZararliAndroid Yazilimlarinin Makine Öğrenmesi Aïlelerïne Göre Siniflandirilmasi, (2019).

[20] L. Li, T.F. Bissyandé, M. Papadakis, S. Rasthofer, A. Bartel, D. Octeau, J. Klein, L. Traon, Static analysis of android apps: A systematic literature review, Inf. Softw. Technol. 88 (2017) 67–95. https://doi.org/10.1016/J.INFSOF.2017.04.001.

[21] M.A. Caloyannides, N. Memon, W. Venema, Digital forensics, IEEE Secur. Priv. 7 (2009) 16–17. https://doi.org/10.1109/MSP.2009.34.

[22] Ö.G. Özen M, Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), Ankara Barosu Derg. (2015).

[23] M.V. Dülger, Adli Bilişim ve Ülkemizde Uygulaması (Forensic Informatics and Its Application in Our Country), SSRN Electron. J. (2021). https://doi.org/10.2139/ssrn.3790772.

[24] A. Emekci, E. Kuğu, M. Temiztürk, Adli Bilişim Ezberlerini Bozan Bir Düzlem Bulut Bilişim, Uluslararası Bilgi Güvenliği Mühendisliği, (2016) 8–14.

[25] F. Süleyman Berber Danışman Doç Ecir Uğur Küçüksille, Mobil Adli Bilişim Yazılımı Geliştirilerek Adli Bilişim Yazılımı Geliştirilerek Elde Edilen Veriler ile Kullanıcılar Arası İlişkilerin Değerlendirilmesi, (2018).

[26] A.K. Singh, A.K. Prajapati, V. Kumar, S. Mishra, Usage Analysis of Mobile Devices, in: Procedia Comput. Sci., 2017. https://doi.org/10.1016/j.procs.2017.11.420.

[27] İ. İlhan, Dicle Üniversitesi Mühendislik Fakültesi mühendislik dergisi, (n.d.).

[28] B. Mühendisliği Bölümü, M.-M. Fakültesi, G. Üniversitesi, Mobil Ortamlarda Bilgi ve Haberleşme Güvenliği Üzerine Bir İnceleme, Şeref Sağıroğlu ve Hülya Bulut, Fak. Der. J. Fac. Eng. Arch. Gazi Univ. Cilt. 24 (2009) 499–507.

[29] M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE Commun. Surv. Tutorials. 15 (2013). https://doi.org/10.1109/SURV.2012.013012.00028.

[30] A. Kavramlar, Yeni iletişim teknolojileri (n.d.).

[31] J. Gardner, Personal Portable Computers and the Curriculum, (n.d.). https://www.researchgate.net/publication/247166813_Personal_Portable_Computers_and_the_Curriculum (accessed June 5, 2021).

[32] S.Wilson,Wearable,Technology:Present,and,Future,(n.d.). https://scielo.conicyt.cl/pdf/formuniv/v10n2/art09.pdf (accessed June 4, 2021).

[33] B. Os, Mobil işletim sistemleri, (n.d.).

[34] O.O. O, A.O. T, G.R. A, O.C. A, Mobile Operating Systems and Application Development Platforms: A Survey, Int. J. 2201 (2014) 2195–2201.

[35] T. de Lanerolle, Mobile Operating Systems, Comput. Handbook, Third Ed. (2014) 1–28. https://doi.org/10.1201/b16812-69.

[36] Rim, Blackberry operating system, Blackberry. (2010).

[37] S. Allen, V. Graupera, L. Lundrigan, Windows Mobile, Pro Smartphone Cross-Platform Dev. (2010) 65–80. https://doi.org/10.1007/978-1-4302-2869-1_5.

[38] T.H.E. Effect, O.F. Diversity, O.F. The, B. Of, I. Decision, F. Decision, D. Policy, T.O. Company, Impact Factor : International Scientific Journal Theoretical & Applied Science The Effect Of Diversity Of The Nationality, Board Of Director, Investment Decision, Financing Decision, and Impact Factor :, (2000) 164–168. https://doi.org/10.15863/Tas.

[39] K. Barmpatsalou, T. Cruz, E. Monteiro, P. Simoes, Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence, IEEE Access. 6 (2018). https://doi.org/10.1109/ACCESS.2018.2875068.

[40] O.F. Yakut, F. Ertam, A digital forensics analysis for detection of the modified COVID-19 mobile application,in:5th Int. Conf. Comput. Sci. Eng. UBMK 2020, 2020. https://doi.org/10.1109/UBMK50275.2020.9219416.

[41] F.G. ERİŞ, Sosyal Medya Uygulamalarının Adli Analizi, Fatma Güneş Eriş. (2018).

[42] F. Ciroğlu, Mobil Cihazlarda Adli Bilişim İncelemeleri ve Rekabet Hukukundaki, (n.d.).

[43] U. Akalin, Ç. Uluyol, Mobil Cihazlar , Mobil Adli Bilişim ve Önerilen Süreç Modeli, (2015).

[44] Rohit Tamma, Practical Mobile Forensics, (n.d.).

[45] R. Ayers, S. Brothers, W. Jansen, NIST Special Publication 800-101 Revision 1 Guidelines on Mobile Device Forensics, (n.d.). https://doi.org/10.6028/NIST.SP.800-101r1.

[46] Ö. Koca, Mobil Cihazlarda Adli Bilişim İncelemesinin Yapılması (Oxygen Forensic), (n.d.). https://www.academia.edu/20842883/Mobil_Cihazlarda_Adli_Bilişim_İncelemesinin_Yapılması_Oxygen_Forensic_ (accessed June 8, 2021).

[47] D.Trivedi,CSL Assignment Mobile Forensics Tools, (2015) 1–7. https://doi.org/10.13140/RG.2.2.14945.63842.

[48] M. Yates, Practical Investigations of Digital Forensics Tools for Mobile Devices, 2010.

[49] R. Ayers, W. Jansen, L. Moenner, NISTIR 7387 Cell Phone Forensic Tools: An Overview and Analysis Update, (n.d.). https://doi.org/10.6028/NIST.IR.7387.

[50] V. Rao, A. S., Survey on Android Forensic Tools and Methodologies, Int. J. Comput. Appl. 154 (2016) 17–21. https://doi.org/10.5120/ijca2016912182.

[51] Infosec, Android Fidye Yazılımı Nedir ve Kendinizi Ondan Nasıl Korursunuz - InfoSec Insights, (n.d.). https://sectigostore.com/blog/what-android-ransomware-is-how-to-protect-yourself-from-it/ (accessed May 30, 2022).

[52] Trojan atları nedir ve türleri nelerdir? | Kaspersky, (n.d.). https://www.kaspersky.com.tr/resource-center/threats/trojans (accessed May 30, 2022).

[53] SharkBot: a “new” generation Android banking Trojan being distributed on Google Play Store – NCC Group Research, (n.d.). https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/ (accessed May 30, 2022).

[54] M. Ulu, Zararlı Yazılımlar, (n.d.).

[55] S. Yilmaz, S. Zavrak, Adware : a review, (2016).

[56] C. Seifert, J.W. Stokes, C. Colcernian, J.C. Platt, L. Lu, Robust scareware image detection, ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc. (2013) 2920–2924. https://doi.org/10.1109/ICASSP.2013.6638192.

[57] US-CERT, Spyware, (2005) 1–8.

[58] U. Sarwar, S. Ramadass, R. Budiarto, A framework for detecting Bluetooth mobile worms, Proceeding - 2007 IEEE Int. Conf. Telecommun. Malaysia Int. Conf. Commun. ICT-MICC 2007. (2007) 343–347. https://doi.org/10.1109/ICTMICC.2007.4448656.

[59] F. Tong, Z. Yan, A hybrid approach of mobile malware detection in Android, J. Parallel Distrib. Comput. 103 (2017) 22–31. https://doi.org/10.1016/J.JPDC.2016.10.012.

[60] İ. Kara, (pdf) Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama ve Hukuki Boyutunun Değerlendirilmesi(n.d.),https://www.researchgate.net/publication/338774682_turkiyede_zararli_yazilimlatla_mücadelenin_uygulama_ve_hukuki boyutunun_değerlendirilmesi (accessed October 18, 2021).

[61] E. Dushku, M. Rabbani, M. Conti, L. V Mancini, S. Ranise, Sara: Secure Asynchronous Remote Attestation for IoT Systems, IEEE Trans. Inf. Forensic Secur. 15 (2020) 2020. https://doi.org/10.1109/TIFS.2020.2983282.

interpretation of basin, TPAO internal report, Ankara

ÖZGEÇMİŞ

Özge GÜNAY

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

AKADEMİK FAALİYETLER

Bildiriler:

1. Gunay, Ertam, O. (2022). Adli bilişim inceleme yazılımlarının android cihazlar üzerinde karşılaştırılması, International Informatics Congress(IIC2022), Batman, Turkey.