Akıllı Android Telefonlar İçin Fiziksel Adli Imaj Edinim Araçları

(Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones)

Firdous Kausar* and Tadani Nasser Alyahya**

Computer Science Department, Al Imam Mohammad Ibn Saud Islamic University, Riyadh, KSA

Çeviri: Özgür Koca, ensei@tankado.com, v1.0

Özet

Cep telefonları, özellikle de akıllı telefonlar hayatımızda önemli bir rol oynamaktadır. Mobil cihaz pazarının muazzam büyümesiyle, onları suç faaliyetinde kullanma imkânı da sürekli artacak. Android, piyasadaki son derece rekabetçi platformlardan biridir. Birçok üretici tarafından kullanılan Android, farklı modelleri çalıştırmak için kullanılıyor ve bu da güçlü bir çeşitliliğe neden oluyor. Böylece, Android tabanlı akıllı telefonların fiziksel imaj ediniminin zorluğu, özellikle son Android sürümünün kaynak kodu çok geç yayınlanması ile ortaya çıkıyor. Sonuç olarak, en yeni sürüm belleğe sahip mevcut akıllı telefonlar, mevcut akıllı telefon adli araçları kullanılarak edinilemez. Bu yazıda, fiziksel olarak edinme olanağı sunan bazı mobil cihaz adli araçlarının kapsamlı bir perspektifi verilmektedir. Bu araçların karşılaştırmalı analizi, maliyet, bütünlük, veri kurtarma, kullanışlılık, adli veri aşamalarını dışa aktarma yolları ve genelleştirilmiş android akıllı telefonları destekleme yöntemlerini içeren farklı parametrelere dayanarak gerçekleştirilmiştir.

Anahtar kelimeler: *physical image; physical acquisition; Android forensic; forensic tools*

1. Sunuş

Mobil cihazların kullanımı, özellikle akıllı telefonların kullanımındaki artış ile dijital suçlar da arttı. Akıllı telefonların ortaya çıkışı, insanların yaşama, çalışma ve oyun yapma biçimini tamamen değiştirdi. Bununla birlikte, suç işlemede akıllı telefon kullanmanın karanlık bir yanı var. Adli araştırmacılar kanıt elde etmek için zanlıların akıllı telefonlarını onlara karşı mahkemede kullanıyorlar. Akıllı telefonlardan elde edilen kanıtlar, mahkeme salonunda diğer kanıt şekillerinden farklı olarak kabul edilebilmeleri için güvenilir olmalıdır.

Son birkaç yılda Android akıllı telefonları hedef alan önemli miktarda bellek edinimi araştırması yapıldı. Edinme amacı, silinen veriler de dahil olmak üzere yararlı bilgiler toplamak ve daha fazla analiz etmek ve mahkemeye sunmaktır. Adli mobil cihazlar için iki temel edinim yöntemi vardır: fiziksel ve mantıksal. Fiziksel edinme, silinen veriler de dahil olmak üzere tüm fiziksel depolama alanının bit kopyasıdır. Mantıksal edinim, bir dosya sisteminin bir parçası gibi mantıksal depolamayı çıkarır. Yani elde edilen veriler edinim yapılan sistemin dosya sistemi tablosunun sağladıklarıdır. Akıllı telefonlarda saklanan veriler kırılgan olabilir, çünkü veriler üzerine yazılabilir veya silinebilir. Bu nedenle, silinen verileri ayıklamak ve sürdürmek için mantıksal edinim yerine fiziksel edinim kullanma ihtiyacı vardır [1].

Fiziksel edinim araçları, sabitleştirilmiş ve yazılım tabanlı araçlara sınıflandırılmıştır. Donanım tabanlı yöntem, işletim sistemini fiziksel bir aygıtla bypass etmektir. Böylece hedef sistemin dosya yerleşim tablosunun sağlamadığı veriler gibi dez avantajlar ortadan kalkar. Özel bir iletişim portu, dahili belleği kopyalamak için özel bir donanımla açılır [2]. Android akıllı telefonlarda, JTAG test pinleri bir cihazın dahili belleğini almak için kullanılabilir [3]. Bununla birlikte, tüm Android akıllı telefonlarda JTAG test pinleri bulunmamaktadır. Yazılım tabanlı yöntem, dahili belleği elde etmek için bir araç kullanmak veya

tasarlamaktır [2]. Android akıllı telefonlarda bir seçenek de **/dev/mem** aygıtlarından veri edinmektir [3]. Maalesef bu yöntem yalnızca en fazla 896 MB RAM'li akıllı telefonlar için geçerlidir [4]. *Kollar* [5], **fmem** adında fiziksel edinim için /dev/mem aygıtını kullanan yüklenebilir bir çekirdek modülü geliştirdi. Ancak, bu modül tüm Android akıllı telefonlar için geçerli değildir [4].

Android akıllı telefonlardan fiziksel olarak veri edinmek için, genellikle akıllı telefonun, özel önyükleyici, özel kurtarma modu veya kök erişimi olan normal modda [6] önyüklemesi yapılmalıdır. Ardından, donanım cihazına veya sunucusuna (ör. Dizüstü veya masaüstü) imaj verisi göndermek için akıllı telefonda ilgili kodu çalıştırılır [6].

Akıllı telefon işlemci hızları, kullanılan kablo türleri ve aktarılan veri miktarı nedeniyle fiziksel olarak edinme süreci zaman alıcı olabilir. Bazen fiziki edinimin tamamlanması saatler alır. UFED ve Oxygen Forensic gibi ticari araçların çoğu USB üzerinden veri gönderir. Bununla birlikte, kopyalanan verilerin iletim hızı, USB'nin maksimum iletim hızını kullanmaz. Örnek vermek gerekirse, USB 2.0, maksimum 480 Mbps iletim hızına sahiptir, ancak en fazla 320 Mbps alır [7]. 2016'da piyasadaki en büyük Android akıllı telefonlar 128 GB'tır. Akıllı telefonlar büyümeye devam ederken, fiziksel olarak onları edinim süreleri de artacaktır [6].

Bu makalede, Android akıllı telefonlar için birçok farklı fiziksel edinim aracını analiz ettik ve maliyetleri, bütünlüğü, veri kurtarma, kullanışlılık, adli veri aşamalarını dışa aktarma yolları ve genel Android akıllı telefonu destekleme yöntemlerini karşılaştırdık.

Bu yazı şu şekilde düzenlenmiştir: Bölüm 2, Android mimarisini açıklar, Bölüm 3, veri toplama prosedürünün farklı senaryolarını gösterir, Bölüm 4, mevcut bazı fiziksel adli araçları, Bölüm 5, seçilen fiziksel adli veri edinme araçlarının karşılaştırmalı analizini sağlar; Bölüm 6, gelecekte önerilen bazı çalışmalara odaklanır.

2.Android'in Mimarisi

Android'in iç tasarımını ve mimarisini anlamak, Android'in esnekliğinden dolayı adli bir soruşturmada en önemli konulardan biridir. Android platformu, yeni sürümlerle zaman içinde değişiyor. Sürümler arasındaki farklılıklara göre, mimari de farklılaşmaktadır. Bununla birlikte, Android mimarisinin ana çekirdek bileşenleri aynıdır. Android mimarisi, Şekil 1'de gösterildiği gibi dört ana katmandan oluşur:

2.1 Linux Çekirdeği

Android çekirdeğini anlamak en önemli unsurdur, çünkü Android mimarisinin temelini oluşturmaktadır [8]. Bellek, ağ ve süreç yönetimi ve güvenlik gibi temel hizmetleri destekler. Ayrıca neredeyse tüm donanım için çeşitli sürücüler de barındırır [8, 9].

2.2 Kütüphane ve Android Runtime

Android, C/C++ [8] ile yazılmış kütüphaneler seti içerir. Standart CSystem Kütüphanesi, Medya Kütüphaneleri, 3D Kütüphaneler gibi kütüphaneler, sistem bileşenleri tarafından Uygulama Çerçevesi katmanı [9] vasıtasıyla kullanılır. Android çalışma zamanı (runtime) bölümü, Android için özel olarak tasarlanmış ve optimize edilmiş bir tür Java Sanal Makinesi olan Dalvik Sanal Makinesi (DVM) adı verilen önemli bir bileşen sunmaktadır [8]. Ayrıca, geliştiricilerin standart Java programlama dili [8] kullanarak Android uygulamaları yazabilmesini sağlayan çekirdek kütüphaneleri seti de sağlıyor. Çekirdek kütüphanelerin ve DVM'nin bir kümesi, çalışan her uygulamanın DVM'nin kendi örneğini bulundurduğu ve kendi işlemi içinde yürüdüğü bir Android çalışma zamanı oluşturur [9].

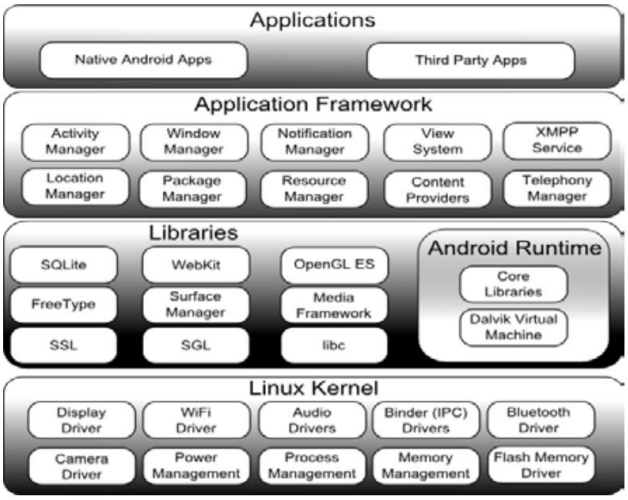
2.3 Uygulama Çerçevesi

Bu katman, Java uygulamalarına istismar edilebilecek birçok üst düzey hizmet sunmaktadır [8, 9]. Uygulama geliştiricileri, Çerçeve tarafından uygulanan güvenlik kısıtlamalarına her zaman saygı duyan geniş bir Uygulama Programlama Arabirimi (API) seti aracılığıyla hizmet sunabilir ve bunları sağlayabilirler [9].

2.4 Uygulama

En üst katman, Java Programlama Dili [10] ile yazılmış bir program demetini (ör. Iletişim yöneticisi, takvim,

SMS programı, web tarayıcısı, bir e-posta istemcisi) içerir.



Şekil 1 - Android Mimarisi

3.Veri Edinim Prosedürü

Adli incelemecilerin benimseyebileceği, Android akıllı telefonlardan veri toplama sürecinin farklı uygulama senaryoları vardır. Uygun prosedürü kullanarak, adli bilişim uzmanları akıllı telefondan maksimum bilgiyi alabilir, böylece elde edilen verilerin mümkün olduğunca daha güvenli ve en az müdahaleci bir şekilde analiz edip belgelendirilebilir. Adli inceleyici, hedef akıllı telefonda kayıtlı verileri korumak için gerekli prosedürleri izlemelidir [11].

3.1 Veri Koruma Prosedürleri

Adli inceleme, hedef akıllı telefonun açık veya kapalı olma durumunu kontrol etmelidir. Akıllı telefon kapalı olduğunda, adli araştırmacı hafıza kartını kontrol eder. Bellek kartı çıkarılmazsa (örn. Dahili bellek), veriler standart USB kart okuyucusu kullanılarak kopyalanabilir. Hafıza kartı çıkarılabilirse, hafıza kartını çıkarın ve korumak için adli bir hafıza kartına kopyalayın. Veriler, usb flash bellek sürücülerinde kullanılanla aynı yaklaşım kullanılarak kopyalanabilir. Bir diğeri, verileri kopyalamak ve daha sonra yinelenen verilerin karma değerlerini oluşturmak için adli araçların kullanılmasıdır. İşlemin sonunda kopyalanan verilerle birlikte adli bellek kartı akıllı telefona geri takılmalıdır.

3.2 Şebeke ve Ağ Bağlantısı Yalıtım Prosedürleri

Verilerin değişimini önlemek için akıllı telefonun şebekeden ayrılması önemlidir. Akıllı telefon, elektromanyetik sinyallerden fiziksel izolasyonu olan bir oda kullanarak izole edilebilir veya akıllı telefonu yalnızca uçuş veya çevrimdışı moda ayarlayabilir. Adli bilişim araştırmacısı akıllı telefonu açtığında, veri iletiminden, çağrıları veya SMS'i almaktan kaçınmak için onu hemen bu tür bağlantısız bir modda yapılandırmalıdır. Akıllı telefon gelen çağrı, SMS veya e-posta gibi bir bilgiyi aldığında, inceleyici, bunu nihai raporda belgeleyip açıklayacaktır. Akıllı telefon telekomünikasyon ağlarından izole edildiğinde, inceleyici, akıllı telefonun bir kimlik doğrulama mekanizması (ör. Şifre veya model) sağlayacak şekilde yapılandırılıp yapılandırılmadığını kontrol etmelidir. Bundan sonra, inceleyici cihaz üzerinde yapılandırılmış olan erişim kontrol mekanizmasına bağlı olarak veri toplama işlemlerini tamamlamalıdır.

3.3 Erişim Kontrolü Prosedürü Olmadan Akıllı Telefonun Veri Edinimi

En basit olan bir durum, çıkarılabilir hafıza kartı ile kilitli olmayan bir akıllı telefonun edinimidir. Daha önce de belirtildiği gibi, inceleyici ilk önce hafıza kartlarından veri çıkardıktan sonra kopyaları alınan adli inceleme kartlarını akıllı telefona tekrar takmalıdır. Ardından inceleyici Android akıllı telefonda süper kullanıcı ayrıcalıklarının durumunu kontrol etmelidir (super su, root). Etkinleştirilirse, inceleyici USB hata ayıklama aracı ADB'yi kullanarak dahili belleğinin bir kopyasını oluşturarak kısıtlama olmaksızın akıllı telefondaki depolanmış verilere erişebilir. Ancak, akıllı telefonda süper kullanıcı ayrıcalıkları devre dışı bırakılırsa, bu durumda bazı Android akıllı telefonlar bootloader modu veya kurtarma modu kullanılarak edinilebilir. İnceleyici, bu teknikleri bu tür akıllı telefonlara uygulama imkânını değerlendirmelidir. İncelemeciler tarafından kullanılabilen mevcut mobil cihaz adli araçları, Cellebrit UFED ve Oxygen Forensic gibi verileri edinmek için kullanıcı ayrıcalıklarını kullanmazlar. Bunun yerine Cellebrit UFED, bootloader modunu kullanır. Dahili belleğin tam bir kopyasını kurtarmak için etkili bir mobil aygıt adli araç seçmek adli bilişim görevlisine kalmıştır.

3.4 Erişim Kontrol Prosedürüyle Akıllı Telefonun Veri Edinimi

Android çalışma zamanı bölümü, Android için özel olarak tasarlanmış ve optimize edilmiş bir Java Sanal Makinesi türü olan Dalvik Sanal Makinesi (DVM) adı verilen önemli bir bileşen sunmaktadır [8]. Ayrıca,

geliştiricilerin standart Java programlama dili [8] kullanarak Android uygulamaları yazabilmesini sağlayan çekirdek kütüphaneleri seti de sağlıyor. Çekirdek kütüphanelerin ve DVM'nin bir kümesi, çalışan her uygulamanın DVM'nin kendi örneğini bulundurduğu ve kendi işlemi içinde yürüdüğü bir Android çalışma zamanı oluşturur [9]. Android akıllı t elefon, bir şifre veya desen gibi erişim kontrolü kullanarak kilitlenebilir. NIST'e göre [12], kilitli akıllı telefonlara erişmenin üç yolu vardır:

1. Araştırmacının olası geçerli parolaları istediği araştırma yöntemi.
2. Araştırmacının akıllı telefona erişmek için yıkıcı olmayan bir prosedürü gerçekleştirmesi gereken donanım yoluyla erişim. Bu yöntem üreticilerin ve yetkili servis merkezlerinin desteğini gerektirmektedir.
3. Yazılımsal erişim yöntemleri, mobil cihaz modeline ve Android sürümüne bağlı olsa da genellikle en kolay yoldur.

İnceleyici kanıttan ödün vermekten kaçınmak için en az müdahaleci yöntemi kullanmalıdır. Akıllı telefon ele geçirildiğinde şifre veya model elde edilmişse, test edilmelidir. İnceleme başarılı olmazsa, akıllı telefonun bir ADB aracı kullanarak USB hata ayıklama bağlantılarını kabul edecek şekilde yapılandırılıp yapılandırılmadığını kontrol etmelidir. Başarılı olursa, son bölümde daha önce bahsedildiği üzere, edinme sürecini devam ettirmek için süper kullanıcı erişim denetimi ayrıcalıkları kazanmaya çalışmaktadır. Akıllı telefona süper kullanıcı erişim kontrolü için herhangi bir ayrıcalık olmadığında bile, denetçi, erişim kontrol sistemini atlamak için ADB aracı aracılığıyla uygulamalar yükleyebilir. Erişim kontrol sistemini atlamak mümkün olmadığı veya USB hata ayıklama erişiminin devre dışı bırakıldığı durumlarda, akıllı telefona takılabilen çıkarılabilir hafıza kartından veriler alınabilir.

3.5 Edinme Dokümantasyonu

Çıkarılan verilerin analizini kolaylaştırmak için kullanılan tüm teknikler ve prosedürler, inceleyici tarafından belgelendirilmelidir. Veri toplama prosedürünün belgelendirilmesiyle, inceleme sonuçlarına daha fazla güvenilecektir. İnceleyici, edinme işlemi sırasında üretilen ve çıkan verilerin hash kodlarını dikkatle kaydetmelidir. Ayrıca, akıllı telefon telekomünikasyon ağlarından izole edilmeden önce bir e-posta veya SMS alması gibi edinim işlemi sırasında karşılaştığı tüm uyarıları belgelemek zorundadır.

4. Android için Fiziksel Edinim Araçları

4.1 Linux Bellek Çıkarıcı (LiME)

LiME aracı 2012'de J. Sylve ve diğerleri tarafından piyasaya sürülmüştür. [4]. Android'den, uçucu belleği elde (RAM) etmek için kullanılan açık kaynaklı bir adli araçtır. LiME, bellek sayfalarını adli olarak sağlam bir şekilde elde edebilen **dmd** adlı yeni bir yüklenebilir çekirdek modülünü temel almaktadır. Akıllı telefondaki SD'ye veya ağ üzerinden hafızayı almayı destekler. Dmd modülü aşağıdaki gibi çalışır: sistem RAM'inin fiziksel bellek adres aralıklarını öğrenmek, her bellek sayfasında fiziksel adresleri sanal adreslere çevirmek, tüm bellek sayfalarını okumak ve TCP soketinin SD'sine yazmak için çekirdek yapısını ayrıştırmak. LiME aracı önemli özellikler sunar [13]: edinme için hedef cihaza aktarmak için sadece dmd modülü gereklidir, bellek dökümü için çok az sayıda çekirdek işlevi gereklidir, dmd modülünün yüklenmesi asgari ayak izi gerektirir ve kullanıcı alanı ile minimum etkileşim gereklidir. Yazarlar, sayfaların yaklaşık %99.46'sının TCP bağlantısı üzerinden doğru olarak yakalandığını ve sayfaların % 99.15'i SD karta doğru yazıldığını gösteriyor. Önerilen modül tüm Android cihazlarını destekliyor ancak yine de genel bir modül olarak değerlendirilmiyor. Ayrıca, Wächter [14], modelin belirlenmesi, Android sürümünün belirlenmesi, ekranı kilitleme, süper kullanıcı yetki istismarı, kaynakların kullanılabilirliği, çekirdek konfigürasyonu ve kanıt erozyonu nedeniyle LiME aracının kollukta adli olmasının pek çok nedenden dolayı mümkün olmadığı sonucuna varmıştır.

4.2 Android Fiziksel Döküm (APD)

APD, S. Yang ve ark. Tarafından geliştirilmiştir. [15]. Bu araç, Android akıllı telefonların bellenim güncelleme protokollerini analiz etmeye dayanmaktadır. Bu nedenle, Android cihazların önyükleme yükleyicisinin Android güncelleme protokolleri aracılığıyla dahili belleğe erişir. Hem bölüm hem de tüm belleğin dökümünü almayı destekliyor. APD'yi kullanarak edinilen verilerin biçimi, akıllı telefon adli analiz araçları aracılığıyla analiz edilebilen ham verilerdir. Yazarlar, önerilen yöntemin edinilen verilerin bütünlüğünü garanti

ettiğini ispatladı. APD'nin veriyi yüksek hızda aldığını gösterdiler; UFED 4PC ortalama 120 dakika sürerken, 32 GB belleğin dökümünü almak yaklaşık 30 dakika aldı. APD, ekran kilidi nedeniyle kısıtlamaya rağmen yürütülebilir; Normal önyükleme modundan ziyade telefonu kapatarak ve bellenim güncelleme modunda yeniden başlatarak. APD aracı, en yeni Android modellerinin 80'inden fazlasını destekler. Bununla birlikte, yöntemin en büyük dezavantajı, yeni Android akıllı telefonlar her başlatıldığında üretici yazılımı güncelleme protokolünü analiz etmeyi gerektirmesidir.

4.3 Hawkeye

Hawkeye, Guido ve ark. Tarafından 2016 yılında fiziksel edinim amaçları için önerildi. [6]. Hawkeye'nin amacı, fiziksel edinim sırasında aktarılması gereken veri miktarını ve gereksiz verileri azaltmaya odaklanıyor. Böylece, toplam edinim süresini azaltır. Hawkeye, Android akıllı telefonları fiziksel döküm elde etmek için özel açılış veya kurtarma kipinde çalıştırıyor. Araç, tescilli marka aracını geçici olarak hedef akıllı telefonun RAM belleğine yükler. Araç temel hash ve bölümlerin bir listesini de sağlar. Araç, daha sonra USB aracılığıyla arka uç PMF mimarisine gerekli veri bloklarını belirleyip gönderecektir. Yazarlar birkaç nedenden ötürü PMF'yi seçtiler: resimleri otomatik olarak geri yazarak ham formata çevirme. Araç, bir bölümü veya akıllı telefonun dahili belleğini tam olarak alabilir. Hawkeye 16GB boyutunda dahili belleği 7 dk içinde başarıyla elde edebildi.

4.4 Android Memory Extractor (AMExtractor)

AMExtractor [3], Android cihazlardan uçucu hafıza (RAM) elde etmek için kullanılan bir araçtır. AMExtractor çekirdek alanında kod yürütmek için /dev/kmem aygıtını kullanır. Bu, yüklenebilir çekirdek modülünün kısıtlamasını önleyecek ve herhangi bir değişiklik yapmadan en son stok ROM'larda çalışma olanağı sağlayacaktır. AMExtractor hedef akıllı telefonun kaynak koduna ihtiyaç duymaz ve çoğu Android işletim sistemi sürümüyle uyumludur. Diğer araçların aksine AMExtractor, hedef akıllı telefonlar üzerinde minimum etkiye sahip olduğu için çekirdek modunda çalışır. Ayrıca, cihazı çekirdek modunda çalıştırmak, veri kopyalamayı en aza indirir ve gizli verileri kullanıcı modunda iken inceler. H. Yang ve ark. [3], AMExtractor kullanılarak elde edilen verilerin, LiME'yi kullanarak elde edilen verilerle neredeyse aynı olduğunu gösterdi.

4.5 ANDROPHSY

ANDROPHSY, 2015 yılında I. Akarawita ve ark. tarafından geliştirilen açık kaynaklı bir araçtır. [16]. Dijital adli süreçlerin tüm safhalarını destekleyen ilk açık kaynak araçtır. ANDROPHSY mimarisi dört ana modülden oluşur: vaka işleme, edinme, analiz desteği ve raporlama modülü. Vaka işleme modülünde, özel durum için vaka oluşturma ve yedek arşiv işlevleri sağlanmaktadır. Edinim modülü fiziksel ve mantıksal edinim sağlar. Analiz modülünde, çıkarılan verilerin tam bir inceleme ve analizi. Ve son olarak raporlama modülü, PDF formatında bir rapor oluşturmayı sağlar. Bu aracı kullanmak için tek bir .jar dosyası ve yapılandırma komut dosyası ayrı ayrı kurulmalıdır. Bu araç ile fiziksel edinime odaklanan yazarlar, dd ve Android Debug Bridge (adb) komutları gibi düşük seviyeli Linux ve Android dahili adli işlevlerini ağırlıklı olarak kullanmışlardır. Adb komutları, Android akıllı telefonu ve USB üzerinden bağlı iş istasyonu arasındaki bağlantı ve iletişim süreçlerini yönetmek ve gerçekleştirmek için kullanılır. Dd komutu, ham görüntüleri fiziksel sürücülerden kurtarmak için kullanılan yerleşik bir komut satırı yardımcı programıdır. ANDROPHSY, veri değişimini en aza indirgemek için Linux çekirdeğini kök erişimi kazanmak için kullanır. Kimlik doğrulama ve gizlilik için kullanıcı erişim kontrolü ve vaka yönetimi sağlar. SD kartı edinim hedefi olarak kullanmaz. Bunun yerine, veriler TCP bağlantısı üzerinden aktarılır.

4.6 Android Digital Autopsy (ADA)

ADA, 2016 yılında R. Fasra ve diğerleri tarafından geliştirilen, açık kaynak kodlu bir dijital adli araçtır. [17]. Araç, fiziksel, mantıksal ve dosya sistemi edinimi gerçekleştirir. Yazarlar multimedya kartı (MMC) bölüm düzenine sahip bir cihaz kullandılar. Fiziksel edinme sürecini otomatikleştirmek için geliştirilmiş bir komut dosyası yazıldı. Komut dosyası veri bloklarını tanımlar, daha sonra kök erişimini kazandıktan sonra blokların RAW görüntülerini elde etmek için dd komutunu kullanır. Elde edilen veriler, daha sonra harici bir hafıza kartına, yani SD karta depolanmaktadır. Önerilen araçla birlikte, yazarlar ADA Analiz Aracı'nı geliştirdiler, ancak ne yazık ki bu mantıksal edinim içindir.

4.7 Cellebrite UFED

Cellebrite UFED [18], Android gibi çeşitli cihazlar ve platformlarda fiziksel, mantıksal, dosya sistemi ve şifre alımını gerçekleştiren ticari bir adli araçtır. Ayrıca, çözme, analiz ve raporlama da gerçekleştirir. UFED, tüm Android işletim sistemi sürümlerinden veri edinebilir.

4.8 Oxygen Forensic Suite

Oksijen Forensic Suite [19], çok çeşitli akıllı telefonları destekleyen önde gelen adli tıp araçlarından biridir. Bu, tüm dünyada 50'den fazla ülkede Yasa Uygulayıcılar, ordu, polis departmanlrı ve diğer hükümet yetkilileri tarafından kullanılır. Araştırmacılar, Android akıllı telefonlarının fiziksel olarak edinilmesini, gelişmiş incelemesini ve akıllı telefondan çıkarılan ham görüntülerin ve cihaz görüntülerinin analizini yapmalarını sağlar. Desteklenen akıllı telefonların tamamen otomatik bir şekilde edinilmesi ve analiz edilmesine olanak tanır. Yaklaşık 45 dakika içinde 16 GB akıllı telefon edinebilir. Akıllı telefon faaliyetlerini özetleyen denetmen için iyi tanımlanmış bir rapor sunar.

4.9 XRY Physical

MSAB [20], özütleme, analiz etme ve raporlama için ürünler sağlar. XRY Fiziksel araç, hedef cihazı değiştirmeden dahili belleğin ve çıkarılabilir medyanın çıkarılmasını destekler. Ayrıca, kullanıcıların bellek imajının karma değerlerini ve ayrıca tek tek çözülen dosyaları oluşturmalarına olanak tanır. XRY Fiziksel, işletim sistemini atlayarak hedef akıllı telefondan ham verileri kurtarır ve silinen verileri hedef akıllı telefondan daha derinlemesine gidip kurtarma şansı sunar. Fiziksel özütleme iki ayrı aşamaya ayrılır: ilk veri tabanı, ham veriler akıllı telefondan alınır ve kod çözme aşaması, burada araç veriyi otomatik olarak anlamlı bilgiler haline getirir. Çıkarılan veriler XAMN Spotlight tarafından görüntülenebilir.

4.10 Device Seizure

DS [21] fiziksel, mantıksal, dosya sistemi ve şifre elde etmeyi desteklemektedir. Edinilen tüm veriler hakkında eksiksiz bir analiz ve rapor sunar. Geniş platform ve cihaz yelpazesini destekler. Android için 4.4.2'ye kadar fiziksel imaj alımlarını destekler (sürüm 3 hariç). DS minimum sistem gereksiniminin düşük olması nedeniyle herhangi bir cihazda çalışabilir. Önemli kanıtlar için akıllı telefonun bellek dökümünü arayabilir [22].

4.11 MOBILedit! Forensic

MOBİLedit! Forensic [23], birkaç tıklamayla akıllı telefonda saklanan silinmiş veriler de dahil olmak üzere tüm verileri almak, aramak ve görüntülemeye izin verir. Bu araç, Android ve iOS tarafından desteklenen tüm akıllı telefonları destekleyebilir. Sıklıkla güncellenir ve daha fazla akıllı telefonu desteklemek için yeni özellikler eklenir. Araç, bu kanıtların elde ediliş şekli ve sunulması biçimini değiştirmiştir. *Mahkeme salonunda sunulmaya hazır ayrıntılı adli raporlar üretir*. Rapor herhangi bir dilde üretilebilir.

4.12 ViaExtract

ViaExtract [24] ViaForensics tarafından oluşturulan fiziksel ve mantıksal bir çıkarma aracıdır. Android akıllı telefonlar için rehberli veri toplama, güçlü analiz ve esnek raporlama özellikleri sunar. ViaExtract, yalnızca bir düğmeyi tıklatarak çoğu akıllı telefonun kök erişimini elde etmek için cihaz root'lama sihirbazını kullanır. Bu araç, incelemecilerin dahili ve harici depolamadan veri çıkarmak için şifreyi kırmalarına izin verir. Hızlı ve kullanımı kolay bir global arama özelliği sunar. Bu özellik, denetleyicinin, halihazırda açık olan tüm incelemelerde çıkarılan tüm içerik türlerini bir kerede aramasına izin verir. ViaExtract popüler Android akıllı telefonların çoğunda çalışır.

4.13 Cep Telefonu Examiner Plus (MPE +)

MPE + [25] gelişmiş akıllı telefon edinme ve analiz özelliklerine sahip bir mobil cihaz inceleme aracıdır. Geniş platform ve cihaz yelpazesini desteklemektedir. İncelemecilerin veriyi hızlı bir şekilde toplamasına, kolayca tespit etmesine ve etkili bir şekilde elde etmesine izin verir. DS gibi, MPE + da önemli bir kanıt için bir akıllı telefonun bellek dökümünü arayabilir [22]. Piyasada bulunan diğer araçlardan %30 daha hızlı iOS ve Android cihazlarından veri edinebilir. MPE +, sağlam ve üstün bir analiz araçları kümsesi içerir. Fiziksel edinimi gerçekleştirmek için, hedef telefona takılması gereken boş bir adli SD kartı, MPE + 'nın ajanını geçici olarak saklar. Root yetkisi kazanmak için 3. Parti araçlara ihtiyaç duyar.

5. Karşılaştırmalı Analiz

Bu yazıda fiziksel adli araçlar maliyet, kullanıcı dostu, ekran kilidi ile veri kurtarma, veri bütünlüğü, bölüm veri kurtarma, verilerin dışa aktarılma yolları, adli aşamaların desteklenmesi ve genel Android akıllı telefonların desteklenmesi açısından karşılaştırılmıştır. Tablo 1, değerlendirilen adli araçların bir değerlendirmesini göstermektedir.

5.1 Açık Kaynak

Oksijen, UFED ve MSAB XRY gibi en güçlü mobil aygıt adli araçlar pahalı olduklarından kişisel kullanım için uygun değildir. Ticari araçların yanı sıra, ticari araçların birçoğuyla rekabet edebilecek düzeyde (örneğin desteklenen cihazlar, edinilmiş veriler, bütünlük, güvenilirlik) iyi sonuçları elde etmek için LiME, AMExtractor, ADA ve ANDROPHSY gibi ücretsiz açık kaynak kodlu mobil cihaz araçları bulunmaktadır.

5.2 Kullanıcı Dostu

Hemen hemen tüm ticari araçlar kullanıcılara veri çıkarma, analiz etme ve raporlama için kullanımı kolay bir arayüz sağlar. Gezinmek için basit bir arayüz ve kullanıcıları tüm süreç boyunca yönlendiren bir sihirbaz ile birlikte tasarlanmıştır. Bazıları, Cellebrite UFED ve Oxygen gibi çok dilli kullanıcı arabirimini desteklemektedir. ANDROPHSY, kullanıcılara kolay arayüz sağlayan tek açık kaynaklı adli araçtır.

5.3 Ekran Kilidi Atlatmak

Tüm Android akıllı telefonlar, desen veya şifre kullanarak kilitlenebilir ve güvenlik nedenlerinden ötürü USB hata ayıklama devre dışı olarak elde edilebilirler.

Forensic Aracı	Açık Kaynak	Kullanıcı Dostu	Ekran Kilitli Cihazdan Kurtarma	Bütünlük	Bölüm	Dışarı Veri Aktarma	Adli Bilişim Süreçleri Uyumu	Genel Amaçlı
LiME	E	H	Bilgi yok	Yüksek	H	TCP SD Kart	H	H
AMExtractor	E	H	H	Yüksek	H	TCP	H	H
APD	H	H	E	E	E	Bilgi yok	H	H
Hawkeye	H	H	H	E	E	Bilgi yok	H	H
ANDROPHSy	E	H	E	E	E	TCP	E	E
ADA	E	E	H	E	H	SD Kart	H	H
UFED	H	H	E	E	H	SD Kart, USB Flash Bellek	E	H
Oxygen	H	E	E	E	H	USB bağlantısı, Bluetooth	E	H
MSAB XRY/XACT	H	E	E	E	H	USB Bağlantısı	E	H
DS	H	E	E	E	H	USB Bağlantısı	E	H
MOBILedit!	H	E	H	E	H	USB Kablo, TCP	E	H
ViaExtract	H	E	E	Bilgi Yok	H	Bilgi Yok	E	H
MPE+	H	E	E	H	H	Kablolar, Infrared, Bluetooth	E	H

Tablo -1: Adli Bilişim Araçlarının Karşılaştırmalı Tablosu

Bu nedenle, mevcut edinim yöntemlerini uygulamak için USB hata ayıklamasının etkinleştirilmesi gerekir. MOBILedit gibi adli araçların çoğu fiziksel imaj için ADB protokolünü kullanır. Bununla birlikte, ADB protokolünü kullanmak ve edinme yöntemlerini uygulamak için USB hata ayıklamasının etkinleştirilmesi gerekir. ADB aracı, akıllı telefonu kapattıktan ve yazılım güncelleme modunda yeniden başlatıldıktan sonra fiziksel olarak edinme gerçekleştirerek bu sorunun üstesinden gelir [15].

USB hata ayıklamanın etkinleştirilip etkinleştirilmediğine veya cihazın root'lu bir durumda olmasına bakılmaksızın MPE +, Android 2.3.4 veya 2.3.5 destekli Samsung Galaxy S II ailesinden ekran kilitlerine atlayabilir ve fiziksel görüntüler elde edebilir [25]. ANDROPHSY, DS ve MSAB XRY Android akıllı telefonların ekran kilidini atlatmayı destekler [19, 20, 21]. UFED ve viaExtract, her türlü kilidi atlayabilir ve yalnızca USB Hata Ayıklama etkinleştirilmişse veri aktarabilir [18, 24]. Oxygen, bazı Samsung Galaxy Note ailesi akıllı telefonları için fiziksel imajlar oluşturabilir ve kilit ekranını bypass edebilir [19].

5.4 Veri Bütünlüğü

Kanıtların bütünlüğü, kanıtların edinim ve analiz esnasında ayrılmaması ve değiştirilmemesi gerekliliğini tanımlayan, adli bilişim alanında önemli bir boyuttur. Bazı mobil cihaz adli bilişim araçları, doğal olarka bir akıllı telefonun deposunda değişiklik yapan fiziksel görüntüler elde etmek için normal moda başlatılması gerekebilir. ADB aracı, birçok fiziksel edinim denemesinden sonra dahi cihazın bütünlüğünü garanti eden bellenim güncelleme modunda hedef akıllı telefonu önyükleme yaparak bütünlüğü korudu [15]. Bütünlük, sağlama değer toplamı (hash) aracılığıyla doğrulanabilir. DS, MOBILedit! Forensic, UFED, Oxygen, MSAB XRY, ADA,Hawkeye ve ANDROPHSY üretilen görüntüler arasında hash değerlerini (ör. MD5, SHA-1, SHA-256, SHA-512) hesaplayarak veri bütünlüğünü doğrulamaktadır. MPE+ orijinal ikili veriler yerine kanıtların bir kopyasına göre davranan bir Python Komut Dosyası oluşturur, bu nedenle orijinal veriler değiştirilmeyecektir [21, 25].

5.5 Bölme Veri Kurtarma

Veri kurtarma, tüm adli araçların kalbidir. Tüm fiziksel edinim araçları tüm dahili belleğin alınmasına odaklanır. Bazıları (ör. APD, Hawakye ve ANDROFSY), dahili belleğin bir bölümünün fiziksel olarak edinilmesine izin verir.

5.6 Verileri Dışa Aktarma

Edinilen veriler daha sonra USB bağlantısı, Bluetooth, TCP soketi ve Kızılötesi gibi farklı yollarla kaydedilebilir. Dahası, doğrudan USB flaş belleği veya SD kartı kullanılarak kaydedilebilir. Tablo1, araçları ve verilerin nasıl dışa aktarılacağını göstermektedir.

5.7 Adli Bilişim Aşamaları Desteği

Ana mobil cihaz adli bilişim aşamaları şunlardır: Edinme, analiz etme ve raporlama. Oxygen, Cellebrite UFED, MSAB XRY / XACT, MOBILedit!, ViaExtract ve MPE+ gibi tüm mobil cihaz adli analiz aşamalarını destekleyen az sayıda ticari araç var. Ücretsiz araçlar arasında ANDROPHSY, mobil cihazın adli bilişim yaşam döngüsünü destekleyen tek araçtır.

5.8 Genel

Android sürümüne, cihaz modeline, çekirdek sürümüne, donanım profiline, kurulum sürümüne ve ürün yazılımı sürümüne özgü tüm Android akıllı telefonlarda olduğu gibi, her Android akıllı telefonda kullanılabilen genel bir kurtarma görüntüsü yöntemi yoktur. ANDROPHSY yöntemi, dd ve adb komutları gibi herhangi bir duruma uymak için düşük seviyeli Linux ve Android dahili adli bilişim işlevleri kullanarak modern bir yaklaşım izledi. DS, 4.4.2'ye kadar Android için fiziksel edinim işlemlerini desteklemektedir (sürüm 3 hariç). UFED ve ViaExtract, Android 2.2 ve 4 dahil olmak üzere tüm Android sürümleri için USB hata ayıklama yoluyla fiziksel olarak veri ayıklar. Oxygen, MSAB XRY ve MOBİLedit! gibi mobil adli bilişim araçları geniş bir Android akıllı telefon yelpazesini destekler fakat her Android akıllı telefonun kilidini açamayabilir.

6. Sonuç

Fiziksel adli bilişim araçlarındaki artış ve Android akıllı telefonlarının pratik kullanımıyla birlikte, bu makale, yeni araçları mevcut araçlar ile karşılaştırmak isteyen araştırmacılar için ölçütler belirlemiştir. Aynı zamanda, araştırmacıları veya uygulayıcıları, güvenilir ve uygun fiziksel adli araçlar seçerek, fiziksel imajları

yakalamak için daha etkili, interaktif ve uygun bir yol sağlar. Oxygen ve Cellebrite UFED gibi ticari adli araçlar, güvenilir, kullanımı kolay, birçok Android sürümünde kullanılabilir ve tüm adli bilişim süreçlerini destekler. Ancak, her Android akıllı telefonda, özellikle de hedef akıllı telefon kilitli olduğunda bunlar geçerli değildir. Dahası, kişisel kullanım için uygun değildir. Açık kaynak araçları ise genellikle kullanıcı dostu değil, sadece imaj edinim aşamasına odaklanır, ve Android akıllı telefonların sınırlı sürümünde kullanılabilir, ancak yine de güvenilirdir. Bir ilgi çekici açık kaynak kodlu adli bilişim aracı da ANDROPHSY, özellikleri ile ticari adli araçlar ile rekabet edebilir. Herhangi bir sürüm Android akıllı telefonun tüm belleğinin elde etmek için kullanılmak üzere tasarlanmıştır. Bu mobil cihaz adli yaşam döngüsü destekleyen ilk açık kaynak araçtır. Gelecekte, bu karşılaştırmalı analizde daha fazla fiziksel adli araç eklemeyi umuyoruz. Ayrıca, iOS ve Windows gibi farklı platformlarda fiziksel adli araçlar sağlamayı da. Gelecekteki araştırmalar için, iOS ve Android çalıştıran akıllı telefonlarda fiziksel adli araçları incelemek için pratik bir araştırma yapacağız.

Referanslar

[1] T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," in 2015 World Congress on Internet Security (WorldCIS), Dublin, 2015

[2] L. Cai, J. Sha, and W. Qian, "Study on forensic analysis of physical memory," in Proc. of 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013), 2013.

[3] H. Yang, , J. Zhuge, H. Liu, and W. Liu,"A tool for volatile memory acquisition from Android devices," in Advances in Digital Forensics XII, New Delhi, Springer International Publishing, 2016, pp. 365-378.

[4] J. Sylve, A. Case, L. Marziale, and G.G. Richard, "Acquisition and analysis of volatile memory from android devices," Digital Investigation, vol. 8, no. 3, pp. 175-184, 2012.

[5] I. Kollár, "Forensic RAM dump image analyser," MCS thesis, Charles Univ., Prague, Czech Republic, 2010.

[6] M. Guido, J. Buttner, and J. Grover, "Rapid differential forensic imaging of mobile devices," Digital Investigation, vol. 18, pp. S46-S54, 2016.

[7] L. Spector, "USB 3.0 speed: real and imagined," PCWorld, 2014. [Online]. Available: http://www.pcworld.com/article/2360306/usb-3-0-speedreal-and-imagined.html. Accessed: Oct. 17, 2016.

[8] C. A. Jayasinghe, "Android smart phone contact analyzer", MSIS dessirtation, 2015.

[9] A. Distefano, G. Me, and F. Pace. "Android anti-forensics through a local paradigm," Digital Investigation: The International Journal of Digital Forensics & Incident, vol. 7, pp. S83-S94, 2010.

[10] X. Lee, C. Yang, S. Chen, and J. Wu, "Design and implementation of forensic system in Android smart phone," in Convergence and Hybrid Information Technology - 5th International Conference, Daejeon, 2009.

[11] A. Simao, F. Sicoli, L. Melo, F. Deus, and R. Sousa Junior, "Acquisition of digital evidence in android smartphones," in Proc. of 9th Australian Digital Forensics Conference, p. 116-124, 2011.

[12] W. Jansen, and R. P. Ayers, "SP 800-101. Guidelines on cell phone forensics," 2007.

[13] C. Ntantogian, D. Apostolopoulos, G. Marinakis, and C. Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," Computers & Security, vol. 42, pp. 66-76, 2014.

[14] P. Wächter, "Practical infeasibility of Android smartphone live forensics,"Master thesis, Friedrich-Alexander Univ. Erlangen-Nürnberg, Erlangen and Nurnberg, Bavaria, 2015.

[15] S. J. Yang, J. H. Choi, K. B. Kim, and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones," Digital Investigation, vol. 14, pp. S68-S76, 2015.

[16] I. U. Akarawita, A. B. Perera, and A. Atukorale, "ANDROPHSY-forensic framework for Android," in Proc. of 2015 Internatoinal Conferace on Advances in ICT for Emerging Regions (ICTer), pp. 250-258, 2015.

[17] R. Fasra, and A.R. Meeran, " Performing digital autopsy on an Android device: an "open aource" approach," International Journal of Computer Technology and Applications, vol. 9, no. 15, pp. 7111-7117, 2016.

[18] "Cellebrite UFED,". [Online]. Available: http://www.cellebrite.com/Mobile-Forensics. Accessed: Oct. 17, 2016.

[19] "Oxygen Forensic® analyst,". [Online]. Available: http://www.oxygen-forensics.com/en/. Accessed: Oct. 17, 2016.

[20] majo, "The pioneers of mobile forensics," MSAB, 2016. [Online]. Available: https://www.msab.com/. Accessed: Oct. 17, 2016.

[21] P. Corporation, "Device seizure," [Online]. Available: https://www.paraben.com/device-seizure.html. Accessed: Oct. 17, 2016.

[22] I. I. Yates, "Practical investigations of digital forensics tools for mobile devices," in Proc. of 2010 Information Security Curriculum Development Conference, pp. 156-162, 2010.

[23] C. Labs, "MOBILedit!," 2016. [Online]. Available: http://www.mobiledit.com/forensic. Accessed: Oct. 17, 2016.

[24] S. Goetsch, "Team," in Computer Security, NowSecure, 2016. [Online]. Available: https://www.nowsecure.com/solutions/mobile-app-securitytesting/. Accessed: Oct. 17, 2016.

[25] AccessData, "Mobile phone examiner plus," AccessData, 2016. [Online]. Available: http://accessdata.com/solutions/digital-forensics/mpe. Accessed: Oct. 17, 2016.