Android Akıllı Telefonların Firmware(bellenim) Güncelleme Protokollerine Dayalı Yeni Bir Edinim Yöntemi

(*New acquisition method based on firmware update protocols for Android smartphones*)

*

Seung Jei Yang*, Jung Ho Choi, Ki Bom Kim, Taejoo Chang

The Affiliated Institute of ETRI, P.O. Box 1, Yuseong, Daejeon, 305-600, Republic of Korea

***Çeviri:** Özgür Koca, ensei@tankado.com*

Özet

Android 6'nın piyasaya sürüldüğü şu zamanlarda pazardaki iOS payı artmış olsa da, akıllı telefon pazarında, Android hakim işletim sistemi olmaya devam ediyor. Piyasaya sürülen çeşitli Android akıllı telefonlar için veri toplama ve analizini gerçekleştiren adli çalışmalar yürütülmektedir. Bununla birlikte, yeni Android güvenlik teknolojilerinin uygulanması ile mevcut adli yöntemleri kullanarak veri edinmek daha zor hale gelmektedir. Bu sorunu çözmek için, Android akıllı telefonların firmware (bellenim) güncelleme protokollerini analiz etmeye dayalı yeni bir inceleme yöntemi önermekteyiz. Android akıllı telefonların fiziksel olarak edinilmesi ile önyükleme yükleyicisinde (bootloader) yer alan firmware güncelleme protokolü, tersine mühendislik yapılarak flash bellek okuma işlemi gerçekleştirilebilir (imaj alma). Deneysel sonuçlarımız, önerilen yöntemin ekran doğrulama kilidi aktif akıllı telefonlarla (USB hata ayıklama devre dışı bırakılmış [USB Debug] olsa dahi) bütünlük garantisi, edinim hızı ve fiziksel döküm açısından mevcut adli bilişim yöntemlerine göre daha üstün olduğunu göstermektedir.

Anahtar Kelimeler:

Android adli bilişim, Android fiziksel edinim, Firmware (bellenim) güncelleme protokolü, Flash bellek okuma komutu, Bootloader, Android Fastboot, JTAG, dowload mode

Sunuş

2014 yılının üçüncü çeyreğinde Android işletim sistemi, akıllı işletim sistemi pazar payının yaklaşık %84'ünü oluşturdu (Smartphone OS Pazar Payı 2014 yılının 3. çeyreği). Android akıllı telefon pazarının boyutu artık PC pazarınınkini aşıyor, sürekli olarak kişisel ve iş kullanımı için çeşitli teknolojiler ortaya çıkıyor (Bring your own device, 2014). Bu eğilim, silinen dosyaların iyileştirilmesine ve analiz edilmesine yardımcı olmak için flash belleğin fiziksel olarak edinilmesine yönelik araştırmaların özellikle gerekli olduğu Android forensics'in önemini de arttırmaktadır.

Mevcut Android fiziksel edinme yöntemleri aşağıdaki sorunlara sahiptir.

İlk olarak, çoğu adli araç, Android çekirdeği güvenlik açıklarını istifade ederek veya özel image (işletim sistemi) (Rooting (Android OS), 2014; Vidas ve diğerleri, 2011) kullanarak akıllı telefonlardan veri topluyor. Bununla birlikte, bu güvenlik açıkları sürekli olarak kapatılmakta ve çoğunlukla fiziksel bellek dökümü zafiyetlerinin giderildiği daha güvenlikli sürümler haline gelmekte. Ayrıca güvenlik teknolojilerinin son uygulamaları (Secure boot, 2014; Samsung KNOX, 2014) akıllı telefonlardan veri edinmeyi daha da zorlaştırıyor. İkinci olarak, özel kurtarma görüntüsünün (recovery image) değiştirilmesine dayanan döküm yöntemi (Son ve ark., 2013), kullanıcı verilerinin bütünlüğünü dikkate alan tek yaklaşımdır. Bununla birlikte, bu yöntem, özel kurtarma görüntüsünü cihaza yazamayı gerektirdiğinden, tüm flash bellek dökümünün bütünlüğünü garanti etmemektedir. Üçüncüsü, mevcut adli araçlar, akıllı telefonlardan veri edinmek için Android Hata Ayıklama Köprüsü (ADB) protokolünü kullanıyor. Bu nedenle, ekran deseni veya kullanıcı şifresi ile kilitlenmiş akıllı telefonlardan veri edinmek zordur (USB hata ayıklama devre dışı). Bu sorunları çözmek için, Android akıllı telefonların firmware güncelleme protokollerini analiz etmeye dayanan yeni bir fiziksel edinim yöntemi önermekteyiz.

Giriş

Yazılım (S/W) tabanlı ve donanımsal (H/W) tabanlı edinme yöntemleri, esas olarak Android akıllı telefonlardan veri edinmek için kullanılmaktadır. S/W tabanlı edinme yöntemleri, mantıksal edinim ve fiziksel edinime ayrılmıştır. Mantıksal edinim yöntemleri, bir akıllı telefonda depolanan kullanıcı verilerini ADB Yedekleme (Android Backup Extractor, 2014) veya İçerik Sağlayıcı (Hoog, 2011) aracılığıyla edinir. Bununla birlikte, bu yöntem yalnızca arama geçmişi ve resimler gibi kayıtlı dosyaları alır ve silinen dosyaları kurtaramaz. Fiziksel edinme yöntemleri, USB kablosunu taktıktan sonra genel verileri doğrudan akıllı telefonun flash belleğinden çıkarır. Flaş belleğinin fiziksel olarak dökümünü gerçekleştirmek için öncelikle bir yönetici ayrıcalığı edinmek için gereken root'lama işlemi gerçekleştirilmelidir. Root'lamaya dayalı edinim çalışmaları, bilimsel çalışmalarda ortaya konmuştur (Hoog, 2009; Lessard and Kessler, 2010). Bu çalışmalar, HTC akıllı telefonlarını geliştiren ve ADB kabuğu kullanan edinim yöntemleri de dahil olmak üzere Android adli bilişim konularını tartışır. Bununla birlikte bu yöntemler yalnızca USB hata ayıklama modu etkinleştirildiğinde veri edinmek için kullanılabilir. Ticari adli araçlar (Oksijen Forensic, 2014; AccessData MPEş, 2014; MSAB XRY, 2015) de bu yöntemi kullanmaktadır. Ancak, akıllı telefon açıldıktan sonra root'lama işlemi gerçekleştirildiğinden; Veri edinildiğinde bütünlük zarar görür. Buna ek olarak, Android işletim sistemi yeni bir sürümle güncellendiğinde, root'lamaya izin veren mevcut güvenlik açıklarına düzeltme eklenir; Bu nedenle, Android OS güncellendiğinde yeni bir root'lama tekniği bulunmalıdır. Cellebrite UFED 4PC (2015), kötüye kullanma yoluyla (exploit) temelde bir ADB fiziksel bellek dökümünü desteklerken bazı Samsung modelleri, özel bir önyükleme yükleyicisi aracılığıyla fiziksel bellek dökümünü desteklemektedir. Bununla birlikte, bu yöntemde, her modelin fiziksel bellek dökümü için ortak bir yükleyici yüklemek yerine farklı bir önyükleyici yüklemesi gerektiği bir sorunu vardır.

Fiziksel dökümü aynı Galaxy serisinin bazı modellerinde desteklemediğinden, bu yöntem istikrarlı olarak kabul edilmez. Özel kurtarma

görüntüsünün değiştirilmesine dayanan bir edinim yöntemi, bilimsel çalışmalarda incelenmiştir (Vidas ve diğerleri, 2011; Son ve ark., 2013). Özel kurtarma görüntüsünün (recovery image) kullanılması kullanıcı verisinin bütünlüğünü garanti eder. Bununla birlikte, bu yöntem, özel kurtarma görüntüsünü yazmayı gerektirdiğinden, tüm flash bellek dökümünün bütünlüğünü garanti etmemektedir. Akıllı telefonlardan veri edinmek için ADB kabuğu protokolünü kullandığından, edinim yönteminde USB hata ayıklamasının etkinleştirilmiş olması gerekir. Bununla birlikte, USB hata ayıklama genellikle devre dışı olduğu için, desen kilidi veya kullanıcı şifresi ayarlandıysa bu yöntem geçerli değildir. Dahası, Secure Boot ve Samsung KNOX teknolojileri son zamanlarda Android'e uygulandığında, gelecekte bu satın alma yöntemini kullanırken zorlaşacak olan özel imajların yazılması konusunda kısıtlamalar gelecektir.

Flash cihazları (RIFF Box, 2014, ORT aracı, 2014; Z3X box, 2014) mobil cihazlardan veri çıkarmak için de kullanılır. Bununla birlikte, bu araçların ana işlevi S/W hasarına uğrayan kırılmış telefonları düzeltmektir. Dolayısıyla bu araçlar genel adli araçlar olarak düşünülmez.

H/W tabanlı edinme yöntemleri, JTAG tabanlı edinimi (Kim ve ark., 2008; Breeuwsma ve ark., 2007) ve Chip-off tabanlı edinimi (Jovanovic, 2012) içerir. JTAG tabanlı erişim yöntemi, akıllı telefonun PCB kartı üzerindeki JTAG hata ayıklama arayüzünü kullanarak verileri flaş bellekten okur ve kopyasını çıkartır. Chip-off tabanlı yöntem, flash bellek yongalarını akıllı kartların PCB kartından fiziksel olarak kaldırır ve flash belleğin ham verisini alır. JTAG tabanlı edinme yöntemi sorunludur çünkü tüm akıllı telefonlar JTAG soketine sahip değildir ve veri edinmek uzun sürer. Chip-off tabanlı bilgi toplama yöntemi, flash belleği ayırdığı için sınırlı durumlarda kullanılır.

Ön Çalışma

Flash bellek, esasen akıllı telefonlara veri depolamak için kullanılır. Flaş bellek fiziksel olarak küçük olduğundan ve çok miktarda veri depolayabildiğinden, akıllı telefonlar ve gömülü cihazlarda yaygın olarak kullanılmaktadır. Son zamanlarda, NAND flaşının ve bir denetleyiciyi ile aynı pakete entegre edildiği bir gömülü Multi-Media Card (eMMC), EXT4 dosya sistemini kullanarak depolanan verileri yönetmektedir. Ayrıca, BOOT, RECOVERY, SYSTEM ve USERDATA gibi bölümleri kurar ve çalıştırır. Tüm flash belleğin fiziksel dökümünden önce bir yönetici ayrıcalığı edinilmelidir. Böylece, yönetici ayrıcalığını elde etmek için BOOT bölümünde özel bir image üzerine yazılır ve bir uygulama (SuperUser.apk) veya bir binary dosya (*/system/su*) SİSTEM bölümüne yazılır. Buna ek olarak, yönetici ayrıcalığı, kurtarma modunda elde edilen root yetkisi ile veya Android işletim sistemindeki güvenlik açıklarından yararlanma yoluyla elde edilir. Genel olarak, Google'ın FASTBOOT (Android software development-fastboot, 2014) özel bir imajı flash'a yazma için kullanılır. Her bir üretici kendi firmware güncelleme programlarını (Samsung Kies, 2014; Samsung Odin, 2014; LG Yazılım ve araçları İndirme, 2014; Pantech SelfUpgrade, 2014; HTC Sync Yöneticisi, 2014; Sony PC Companion, 2014; Xiaomi Xiaomi Smartphone için MiFlash'i İndir) , 2015), Google tarafından sağlanan FASTBOOT aracılığıyla basitçe yazılmasını önlemek için bir protokol yayınlamadıkları için sadece orijinal üretici yazılımı flash'a yazabilir. Ürün yazılımı güncelleme işlemi, yalnızca akıllı telefonlar yazılım güncelleme veya indirme modu adı verilen özel bir mod girdiğinde çalışır. Bu modda yalnızca ön yükleyici ve USB işlevi çalışabilir ve yeni bir sistem firmware'i (ya da işletim sistemi) yazılabilir. Güncelleme işlemleri ve komutları, IDA Pro (HexRays, 2015) gibi bir araç kullanarak önyükleyici (boot loader) ve firmware güncelleme programının tersine mühendisliği ile analiz edilebilir.

Ürün yazılımı güncelleme protokollerine dayalı Android fiziksel edinimi

Adli bakış açısından, kullanıcı verilerini içeren flash bellek, veri edinimi sırasında ana hedeftir. Bu işlem, mantıksal bir edinim yöntemi yerine tüm flash belleği elde etmek için fiziksel bir edinim yöntemini gerektirir. Üretici yazılımı güncelleme işlemi sırasında, Android OS ya da yama S/W sorunlarını güncellemek için flash belleğine yazılır. Flaş belleğine doğrudan S / W aracılığıyla erişmenin tek yolu bir firmware güncelleme protokolüdür ve bundan dolayı firmware güncelleme işleminde kullanılan komutları analiz ederek yeni bir fiziksel bellek edinme yöntemi türetebiliriz.

Şimdiye kadar varolan adli edinim/imaj alma araçlarının sorunlarını çözmek için yazılım güncelleme protokollerini analiz eden bir araştırma yoktu. Bu çalışmada, LG, Pantech ve Samsung akıllı telefonları tarafından kullanılan üretici yazılımı güncelleme protokollerini analiz ettik. LG ve Pantech modellerinde, flash belleğe doğrudan erişim ve yazma komutlarının yanı sıra flash belleğin kopyasını çıkartmak için kullanılabilecek okuma komutlarının da yer aldığını gördük. Samsung modellerinde, flash belleğin dökümünü almak için daha önceden okuma komutlarının bulunduğunu doğruladık, ancak yeni versiyonlarda kaldırıldığını gördük. Bu analitik sonuçlara dayanarak, Android akıllı telefonlar için yeni bir fiziksel edinim yöntemi öneriyoruz.

Firmware güncelleme protokolü

Bir Android akıllı telefon açıldığında veya yeniden başlatıldığında, ROM'un 0. Adresinden itibaren bir yüklü bir proses çalıştırılır ve CPU yapılandırması da dahil olmak üzere başlatma işlemleri gerçekleştirilir. Sonra, önyükleyici belleğe yüklenir ve H/W (donanımlar) başlatılır ve NAND ve USB gibi bileşenler kullanım için yapılandırılır. Bootloader uygulaması, Initial BootLoader (IBL), Primary BootLoader (PBL), Secondary BootLoader (SBL) gibi bir çok aşamadan geçerek Android modeline bağlı olarak SBL önyükleme yükleyicisinde veya ABOOT önyükleme yükleyicisinde bir firmware güncelleme protokolü çalıştırılır.

Bir tersine mühendislik aracını kullanarak, önyükleme yükleyicisini analiz etmek ve firmware güncellemeleri için kullanılan komutları tanımlamak mümkündür. Yazılımı güncellemek veya flash belleğe erişerek veri edinmek için akıllı telefon normal önyükleme modundan ziyade yazılım güncelleme modunda olmalıdır. Bu modda yalnızca önyükleyici ve USB modülü etkinleştirildiğinden, edinilen verilerin bütünlüğü, fiziksel edinme işleminden sonra bile birçok kez garanti edilir. Dolayısıyla, incelemesi yapılan kanıt telefonu, güç kapalıyken bellenim güncelleme modunda önyüklenir ve daha sonra fiziki edinme yapılırsa, flaş belleğin bir görüntüsünü almak için bütünlük korunabilir. Şekil. 1, Samsung, LG ve Pantech akıllı telefonlar yazılım güncelleme modunda önyüklendiğindeki ekran görüntülerini göstermektedir. Üretici yazılımı güncelleme moduna girerken kullanılan yazılım güncelleme modunu ve yöntemlerini belirten terimler, üreticiler arasında farklılık gösterir.

Şekil 1 - Firmware güncelleme modları (Samsung, LG, Pantech)

Tablo 1, bir akıllı telefon önyükleme yapıldığında firmware güncelleme moduna girme yöntemlerini göstermektedir. USB Jig, akıllı telefonlar için firmware güncelleme moduna giren basit bir devredir. Samsung ve LG akıllı telefonlar, microUSB konektörünün 4 ve 5 numaralı pinleri arasında 300 K ve 910 K Ohms'luk dirençlere (XDA geliştiricileri, 2012a, 2012b) göre yazılım güncelleme moduna girilebilir. Bu USB İzolasyon kabloları, Orijinal Donanım Üreticisi (OEM) kilidini açmak gibi mevcut sınırlamaların üstesinden gelmek için kullanılamaz.

LG firmware güncelleme protokollerinin analizi

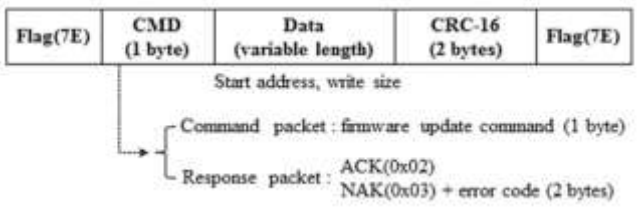
LG akıllı telefonlar için, LG tarafından sağlanan önyükleyici ve güncelleme programını (LG Software & Tools Download, 2014) ayrıştırarak firmware güncelleme süreçlerini ve komutlarını analiz ettik ve flaşın kopyasını almak için kullanılan okuma komutunu tespit ettik.

LG firmware güncelleme komutları

LG firmware güncelleme protokolü, bir komut paketi gönderme ve bir cevap paketi alma yapısında çalışır. Paketler, HDLC bayrağı (0x7E) ve ardından paket veri ve Döngüsel Yedekleme Kontrolü (CRC) -16'dan başlayan ve HDLC bayrağı (0x7E) ile biten Üst Düzey Veri Bağlantısı Kontrolü (HDLC) çerçeve yapısını kullanır. Şekil. 2 LG telefonlarının firmware güncelleme komutunu yapısını göstermektedir.

Model	Modun adı	Tuş bileşimi
Samsung Galaxy	ODIN	Aynı anda, Ses Azaltma, Ev ve Güç tuşuna basıp basılı tutun (ardından Ses Seviyesini Artır tuşuna basın) veya 300 Kohm USB Jig bağlayın
LG Optimus	DOWNLOAD	Sesi Açma tuşunu basılı tutun telefonu mikroUSB kablosuyla bilgisayara takın veya 910 K ohm USB Jig bağlayın
Pantech Vega	PDL Download	Ses Seviyesini Arttır, Ses Kapalı, Ev ve Güç tuşunu aynı anda basılı tutun
Google Nexus 4/5	DOWNLOAD	Sesi Açma tuşunu basılı tutun telefonu mikroUSB kablosuyla bilgisayara takın veya 910 K ohm USB Jig bağlayın.

Tablo 1 – Firmware güncelleme (download) moduna girme yöntemleri



Şekil 2 – LG Firmware güncelleme komut yapısı

LG firmware güncelleme moduna girdikten sonra, cihaz bilgilerini, GUID Partition Table (GPT) bölüm bilgilerini ve hafıza bilgilerini edinme komutları kullanılabilir. Tablo 2 LG firmware güncelleme komutlarını göstermektedir.

LG firmware güncelleme işlemleri aşağıdaki gibidir.

1. Cihaz bilgisini alın: 0x00.
2. İndirme moduna geç: 0x3A.
3. Sorgu özellikleri (Protokol ver., Vb.): 0x2F.
4. Partition bilgisini alın: 0x30.
5. Fabrika bilgilerini alın: 0xFA.
6. Sektör yazın (Birincil GPT): 0x39.
7. Bölümü yazmaya devam edin: 0x39.
8. İndirme tamamlandı: 0x38.
9. Sistemi yeniden başlatın: 0x0A.

LG flash bellek döküm komutu

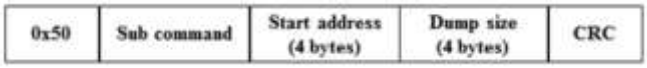
Önyükleme yükleyicisinde firmware güncelleme komutlarının tersine mühendisliği ile elde edilen sonuçlara dayanarak, Tablo 2'de gösterilenlere ek olarak flaş bellek için okuma komutlarını belirledik. Şekil 2 LG Optimus G modelinde (LG-E975) SBL3 önyükleme yükleyicisinin tersine mühendislikle elde edilen flash bellek için okuma komutunu (0x50) göstermektedir.

Firmware güncelleme moduna Tablo 1'de açıklanan işleme göre girildikten sonra, flash bellek ve GPT bölüm bilgisi boyutunu elde etmek için flash bellek bilgisi edinme (0x30) komutu gönderilir. Elde edilen bilgi, flash bellek boyutunu, bölüm sayısını, başlangıç adresini, bitiş adresini ve her bir bölümün adını içerir. Flash bellek (0x50) için okuma komutu başlangıç adresi ve döküm boyutu ile gönderilir ve daha sonra istenen boyut kadar flaş bellek verilerisi elde edilebilir.

Komut	Açıklama
0x00	Cihaz bilgisini al (model, derleme tarihi)
0x3A	Download moduna git
0x2F	Protokol ve algoritma versiyonunu getir
0x30	MMC ve bölüm tablosu bilgisini getir
0xFA	Fabrika bilgilerini getir (IMEI, MAC adresi)
0x12	RAM belleği oku
0x39	Flash belleği yaz
0x0A	Sistemi resetle

Tablo 2 - LG firmware güncelleme komutları

Şekil 3 - . LG SBL3 ön yükleyicisinin tersine mühendislik yapılması



Şekil 4- LG okuma komutu formatı (0x50)

Şekil 4, flaş belleğin içini okuma komutunun (0x50) biçimini gösterir. Şekil 5, bir veri toplama örneğini göstermektedir. Tüm modellerin fiziksel olarak edinilmesi, Android işletim sisteminden ve çekirdek sürümünden bağımsız olarak okuma komutu kullanılarak gerçekleştirilebilir. Dahası, yazılım güncelleme modunda önyükleme yapıldığından, döküm görüntüsünün bütünlüğü daima korunur.

Pantech yazılım güncelleme protokolünün analizi

Pantech ve önyükleyici tarafından sağlanan firmware güncelleme programını (Pantech Self-Upgrade, 2014) tersine mühendislik yaparak yazılım güncelleme işlemini ve komutlarını analiz ettik ve flash bellek okuma komutunu tespit ettik.

PC -> Phone

```
Send 0x1c bytes to the device
 7E 50 01 01 00 00 00 00 00 00 80 02 00 00 02 00   ~P........€.....
 00 00 00 00 00 00 00 00 00 00 7C 1B 7E            ..........|.~
```

Phone -> PC

```
000003: Bulk or Interrupt Transfer (UP), 26.01.2015 15:07:07.077 +0.
Pipe Handle: 0x123046b8 (Endpoint Address: 0x83)
Get 0x3f454 bytes from the device
 50 01 01 00 00 00 00 00 00 80 02 00 00 02 00 00   P........€......
 04 E7 03 00 00 00 00 00 E0 1C 41 4E 44 52 4F 49   .?.....?ANDROID!
 44 21 A0 00 74 00 00 80 20 80 63 9C 29 00 00 00   ?.t..€ €c?... ?.
 20 82 00 00 00 00 00 00 10 81 00 01 20 80 00 08   ......?.. €.....
 00 00 00 00 00 00 38 06 FA E0 89 76 6D 61 6C 6C
 6F 63 3D 36 30 30 4D 20 63 6F 6E 73 6F 6C 65 3D   0M console=ttyHS
 74 74 79 48 53 4C 30 2C 31 31 35 32 30 30 2C 6E   L0,115200,n8 lpj
 38 20 6C 70 6A 3D 36 37 36 37 37 20 75 73 65 72   =67677 user_debu
 5F 64 65 62 75 67 3D 33 31 20 6D 73 6D 5F 72 74   g=31 msm_rtb.fil
 62 2E 66 69 6C 74 65 72 3D 30 78 30 20 65 68 63   ter=0x0 ehci-hcd
 69 2D 68 63 64 2E 70 61 72 6B 3D 33 20 63 6F 72   .park=3 coresigh
 65 73 69 67 68 74 2D 65 74 6D 2E 62 6F 6F 74 5F   t-etm.boot_enabl
 65 6E 61 62 6C 65 3D 30 20 61 6E 64 72 6F 69 64   e=0 androidboot.
 62 6F 6F 74 2E 68 61 72 64 77 61 72 65 3D 67 65   hardware=geehrc8
```

Şekil 7 – LG veri elde etme örneği (LG-F240S)

Pantech yazılım güncelleme komutları

Pantech modellerinde, yazılım güncelleme komutları ABOOT önyükleme yükleyicisinde uygulanır. Böylece, güncelleme işleminde kullanılan üretici yazılımı güncelleme komutları, ABOOT önyükleme yükleyicisi tersine mühendislikle analiz edilerek elde edilebilir. Tablo 3 Pantech akıllı telefonlarda kullanılan yazılım güncelleme komutlarını göstermektedir. Firmware güncelleme komutları, Tablo 1'de gösterildiği gibi firmware güncelleme moduna girdikten sonra yürütülür. Komut paketinin uzunluğu akıllı telefon modeline göre değişir. Vega Iron (IM-A870S) modeline kadar 32 baytlık bir komut paketi kullanılırken sonraki modellerde ise 128 baytlık bir paket kullanılmıştır. Pantech'in firmware güncelleme işlemleri aşağıdaki gibidir.

1. Cihaz bilgisini alın: AT * PHONEINFO.
2. İndirme moduna geçin: AT * PDL * START.
3. Firmware güncellemesini başlatın: 0x00.
4. Hazır disk bölümü yazılıyor: 0x02.
5. Sektör boyutuyla bölüm sil: 0x04.
6. Sektör boyutuyla bölüm yaz: 0x05.
7. 5 ve 6. süreçleri tekrarlayın.
8. Disk bölümünün tümü yazılır 0x03.
9. Sistemi yeniden başlat: 0x01.

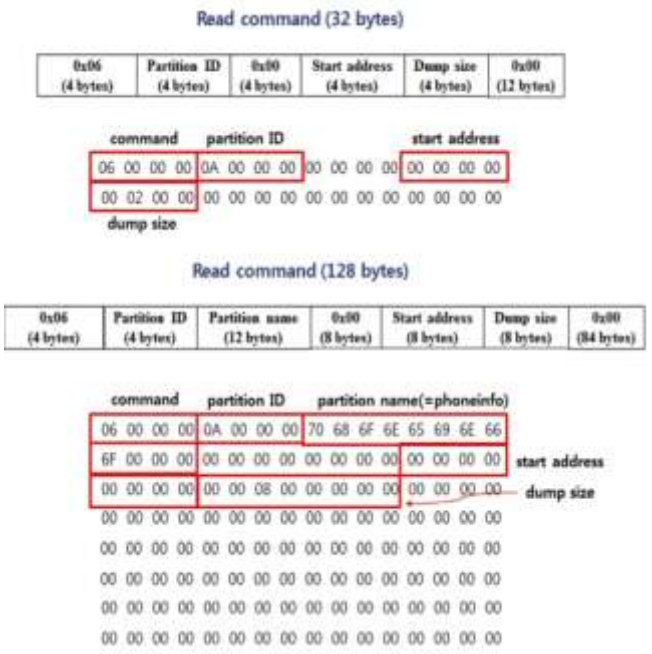
Pantech flash bellek dökümü komutu

Önyükleme yükleyicisinde firmware güncelleme komutlarının tersine mühendisliği ile elde edilen sonuçlara dayanarak 0x06 komutunun flash bellek için okuma komutu olduğu bulundu. Şekil 6, 32 bayt ve 128 baytlık paket uzunlukları ile okuma komutlarının yapılarını göstermektedir.

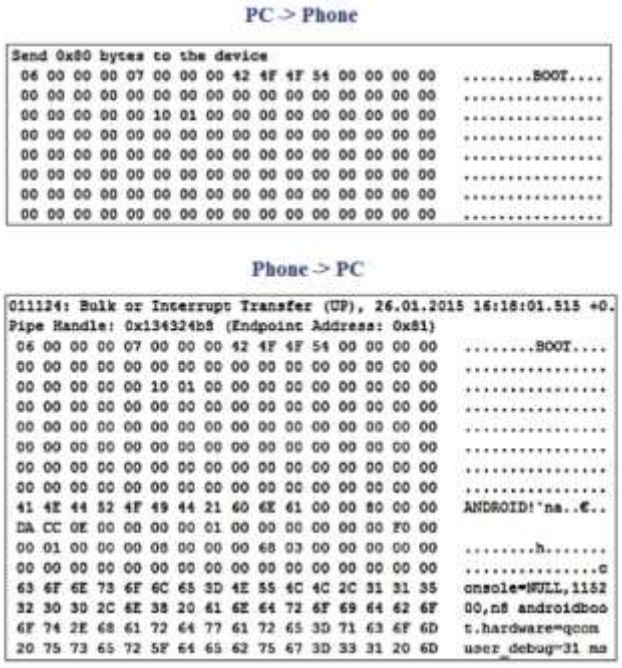
GPT bölümüyle ilgili bilgiler, flash belleğin fiziksel olarak edinilmesinden önce alınmalıdır. GPT bölümü (bölüm ID = 0x0A) flash bellek okuma komutunu (0x06) kullanarak elde edilir ve bölüm bilgileri analiz edilir. Analiz sonuçlarına dayanarak fiziksel edinim bir bölüm için veya tüm flash bellek için yürütülür. Tüm modellerin fiziksel olarak edinilmesi, Android OS ve çekirdek sürümüne bakılmaksızın gerçekleştirilebilir. Yazılım güncelleme modunda önyükleme yapıldığından, LG modellerinde olduğu gibi, döküm görüntüsünün bütünlüğü her zaman korunabilir. Şekil 7, Vega Iron2 (IMA910S) modelinden veri edinme örneğini göstermektedir.

Komut	Açıklama
0x00	Firmware güncelleme hazır komutu
0x01	Yeniden başlat komutu
0x02	Yazmaya hazır komutu
0x03	Yazma tamamlandı komutu
0x04	Disk bölümü silme komutu
0x05	Disk bölümü yazma komutu

Tablo 3 – Pantech firmware güncelleme komutları



Şekil 6 – Pantech firmware güncelleme komutları



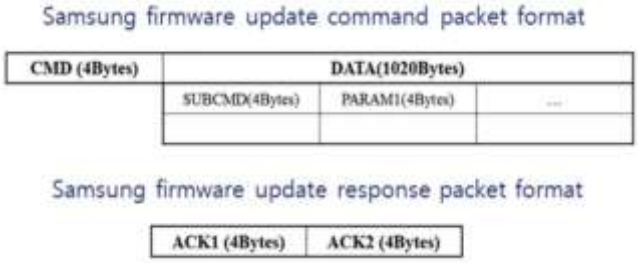
Şekil 7 – Pantech veri edinim örneği (IM-A910S)

Samsung bellenim güncelleme protokolünün analizi

Samsung akıllı telefonlar için, önyükleyici içindeki bellenim güncelleme protokolünü analiz ettik ve flaş belleği okuma için ilgili komutların bulunduğunu tespit ettik, ancak flaş belleğini okumak için gerçek kod kaldırılmıştır.

Samsung firmware güncelleme komutları

Samsung firmware güncelleme protokolünde bir PC bir komut paketi gönderir ve bir akıllı telefon bu komutu işler ve sonuçları bir cevap paketi ile geri gönderir. Komut paketi 1024 bayttan oluşur ve ilk 4 bayt değerlerine göre farklı bir işlev yürütür. Şekil 8, Samsung firmware güncelleme komutunun biçimini gösterir. Tablo 4, Samsung modellerinde kullanılan üretici yazılımı güncelleme komutlarını göstermektedir.



Şekil 8 – Samsung firmware güncelleme komut yapısı

Ana Komut	Alt Komut	Açıklama	
0x64	0x00	Firmware güncelleme protokolünü ön yükle	
0x65	0x00	Bölüm bilgi tablosu yazmaya hazır	
	0x01	Bölüm bilgi tablosu okumaya hazır	
	0x02	Bölüm bilgi tablosu okuma/yazma komutu	
0x66	0x00	Flash belleğe yazmaya hazır komutu	
	0x01	Flash belleği okumaya hazır komutu	*Kod kaldırılmış*
	0x02	Flaş bellek için yazma komutu	
	0x03	Flaş bellek okuma komutu	*Kod kaldırılmış*
0x67	0x01	Firmware güncelleme tamamlandı komut	

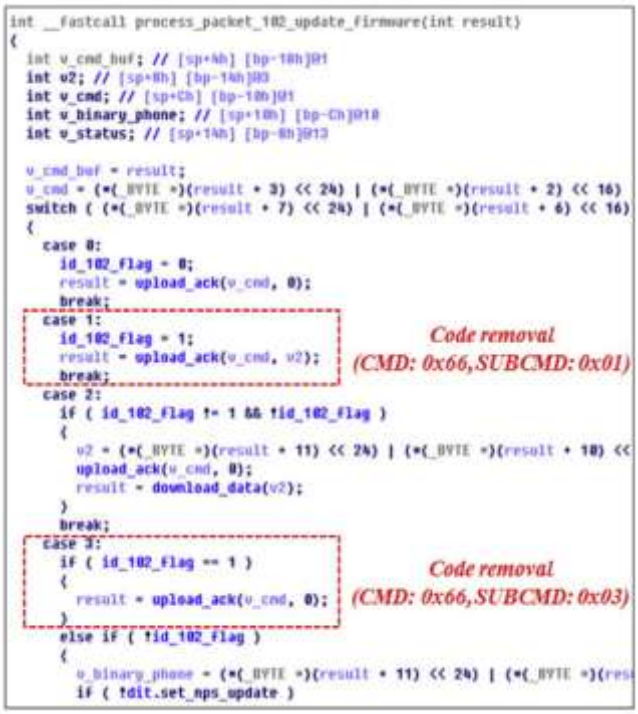
Tablo 4- Samsung firmware güncelleme komutları

Üretici yazılımı güncelleme işlemleri aşağıdaki gibidir. Donanım güncelleme protokolü, 0x64 komut paketi gönderilerek başlatılır. 0x65 komut paketini gönderdikten sonra, yeni firmware bölüm bilgisi tablosu ana belleğe yüklenir. Daha sonra, 0x66 komut paketi gönderilir ve yeni bölüm bilgisine dayanan üretici yazılımı flaş belleğe yazılır ve 0x67 komut paketi, firmware güncelleme işlemini tamamlamak üzere ayarlanır. 0x66 alt komutları (0x01 ve 0x03) flash

bellekteki verileri alabilir, ancak gerçek imaj alma kodu kaldırılmıştır. Oku komutu (CMD: 0x66, SUBCMD: 0x01, 0x03) gönderilirse, akıllı telefon yalnızca veri olmadan bir ACK mesajı gönderir. Sadece flash bellek okuma işlevi Galaxy S2 ve sonraki modellerde kaldırılmış olup olmadığını kontrol ettik. Şekil 9, IDA Pro aracını kullanarak Samsung önyükleme yükleyicisi içindeki okuma kodunun bulunduğu yeri göstermektedir. Döküm kodu kaldırıldığı için okuma komutunu kullanarak flaş belleği verilerini edinmek zordur. Bu nedenle, fiziksel olarak edinimi gerçekleştirmek için, okuma komutunun eklenmesi için ek araştırma gereklidir.

Android'in fiziksel edinim süreci

LG ve Pantech akıllı telefonların firmware güncelleme protokollerini analiz ettikten sonra, flash bellek için okuma komutunun korunduğunu ve bu komutu kullanarak fiziksel edinimin gerçekleştirilebileceğini bulduk. Samsung modellerinde yazılım güncelleme komutlarında flaş bellek okuma komutu vardı, ancak gerçek imaj alma kodu kaldırılmıştı. Bu analize dayanarak Android akıllı telefonlar için yeni bir fiziksel edinim prosedürü geliştirdik. Öncelikle, önyükleme yükleyicisinde yazılım güncelleme protokolünü tersine mühendislik yaparak flash bellek okuma komutunun olup olmadığını kontrol ettik. Bir okuma komutu varsa, LG ve Pantech modellerinde fiziksel edinimi gerçekleştirilebilir. Değilse, okuma komutunun eklenmesi için yama yazılım yapmak gerekir.



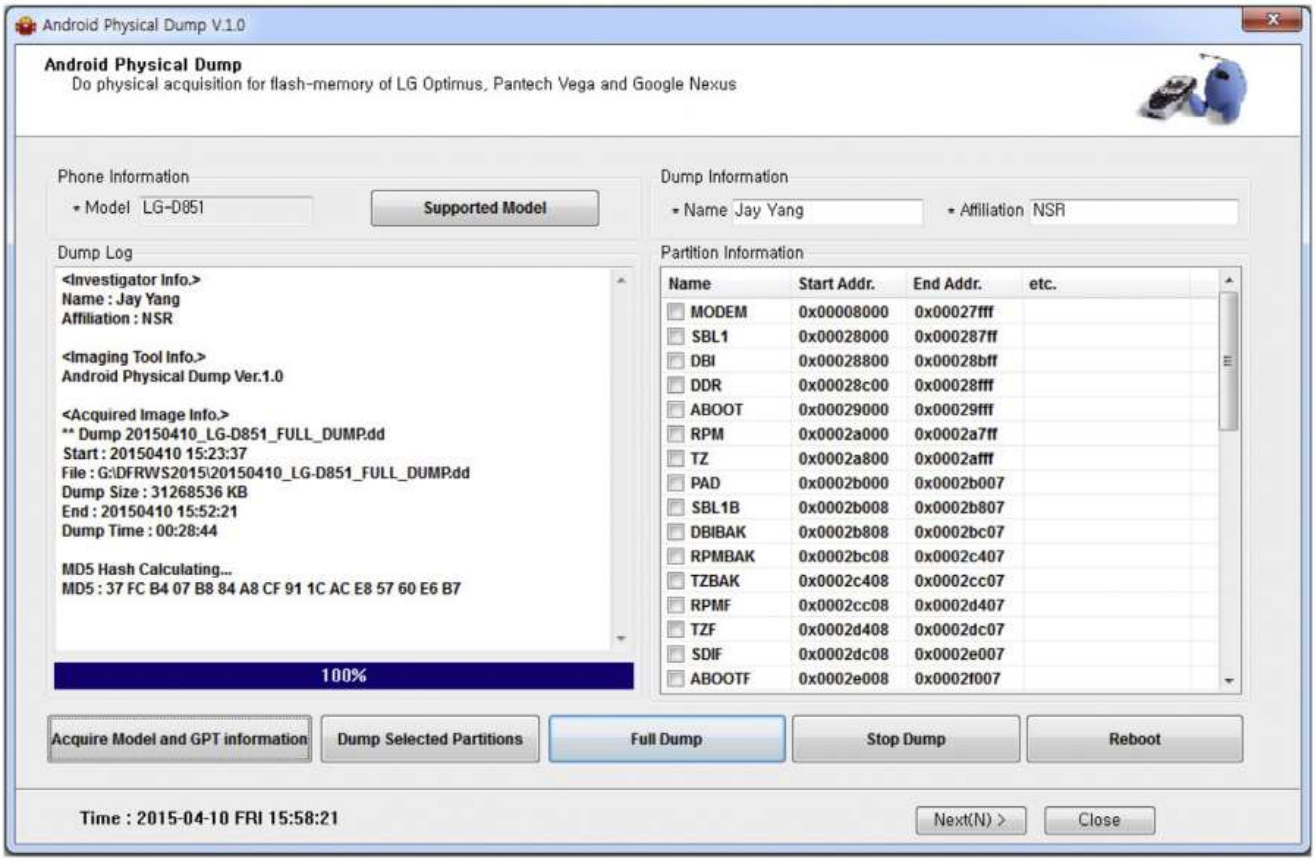
Şekil 8 – Bootloader (önyükleyici) içinde okuma komutunun tersine mühendisliği

Android'in Fiziksel Edinimi

Makalede önerilen edinim yöntemini kullanarak, C++ 'da Android Physical Dump (APD) adlı bir edinim aracı geliştirdik. Şekil 10 APD aracını göstermektedir. Bir USB kablosuyla bağlandıktan sonra fiziksel olarak edinme butonları tıklanır.

Desteklenen modeller

APD aracı şu anda en yeni Android modellerinin 80'inden fazlasını destekliyor. Şu anda, APD, LG Optimus, Pantech Vega ve Google Nexus modellerinden fiziksel çöplükler yapabilir. Desteklenen modellerin temsili örnekleri şunlardır: LG G3, G2, G, Pantech R3, Iron2, Nexus 4/5 ve G Watch.



Şekil 10 – Android Physical Dump (APD)

Firmware güncelleme modunda başlatma

İlk fiziksel döküm adımında, cihaz yazılım güncellemesinde modunda önyüklenir. Akıllı telefonlar, AT komutu veya indirme modu komutu aracılığıyla firmware güncelleme moduna girebilir. Bununla birlikte, fiziksel bellek döküm alma işlemi, normal bir önyükleme sonrasında gerçekleştirilirse, edinilen verilerin hash değeri değişebilir. Bu nedenle, telefon ele geçtikten sonra kapatılması ve ürün yazılımı güncelleme moduyla önyüklemesi yapılmalıdır.

Telefona bağlanın ve model bilgisini edinin

Bir USB kablosu kullanarak akıllı telefona bağlayın. USB sürücüsü önceden kurulmuş olmalıdır. USB sürücüsü üreticinin web sayfasından indirilebilir. Bir USB kablosu bağladıktan sonra, Model ve GPT bilgilerini al düğmesini seçin. Kullanıcı yalnızca üreticiyi seçerse, akıllı telefon model adı otomatik olarak görüntülenir. Model bilgilerini aldıktan sonra, GPT bölüm bilgisi komutu gönderilerek bölüm bilgisi elde edilir. Şek. 10'da, pencere her bölüm için bölüm adını, başlangıç adresini ve bitiş adresini sunar.

Fiziksel edinim

APD aracı, bir bölüm dökümünü ve tüm flash bellek dökümünü gerçekleştirmek için uygulanmıştır. Seçilen Bölümleri edinme düğmesi tıklandıktan sonra, ilgili bölümün fiziksel bir dökümü gerçekleştirilir. Döküm işlemi bittikten sonra, döküm görüntüsünün döküm süresi ve MD5 hash değeri Döküm Günlük penceresinde görüntülenir.

Full Dump butonu tüm flash belleği almak için seçilir. Fiziksel edinme işlemi, edinilen GPT bölüm bilgisindeki flash belleğin başlangıç ve bitiş adreslerini kullanarak yürütülür. Edinim işlemi tamamlandıktan sonra, araştırmacı bilgileri, edinim aracı bilgileri ve döküm bilgisi Şekil 10'da gösterildiği gibi görüntülenir. Döküm bilgileri, hesaplanan MD5 hash değerini ve döküm

görüntüsünün başlangıç zamanı ve bitiş süresini gösterir. Hash değerinin hesaplanması, döküm imajının bütünlüğünü kontrol etmek için önemlidir.

APD aracını kullanarak elde edilen dosya ham veri formatıdır ve akıllı telefon adli araçları (Cellebrite UFED Fiziksel Analiz Cihazı 2015, Rehberlik EnCase, 2014, R-Linux, 2014) aracılığıyla analiz edilebilir.

Denemeler

Android adli bilişim alanında en önemli faktörler, desen kilidi ve kullanıcı şifresi nedeniyle adli imajının bütünlüğünü, hızlı kanıt toplama ve alınan flash imajının bütünlüğünü garanti altına almaktadır. Bu üç faktöre dayanarak, bu çalışmada önerilen APD aracını en yeni Android akıllı telefonlarını kullanarak mevcut edinim yöntemleriyle karşılaştırdık. Karşılaştırılan araçlar arasında, özel kurtarma görüntüsünü temel alan iyi bilinen Cellebrite UFED 4PC, döküm yöntemi ve root'la istismarı yoluyla ADB fiziksel dökümü ve JTAG tabanlı edinim vardı. Tablo 5, elde edilen deneysel sonuçları göstermektedir. G3 (F400S, D851), Optimus G (F180S, E975), R3 (IM-A850S), Iron2 (IM-A910S) ve Nexus 4/5 (E960, D821) gibi farklı modeller kullanılmıştır. Flaş belleğini APD aracı ile dışarı alma işlemini tamamladıktan sonra, alınan imajın kalitesini belirlemek için elde edilen imaj Cellebrite UFED Fiziksel Analiz Cihazı (2015) kullanarak karşılaştırılmıştır.

Elde edilmiş görüntünün bütünlüğünü koruma

Bir önceki çalışmada (Son ve ark., 2013), kullanıcı verileri bütünlüğü bir JTAG tabanlı edinim yöntemi ile kontrol edildi. Bu yöntem, kullanıcı verilerinin bütünlüğünü sağlar, çünkü yalnızca özel imajı flash belleğe yazılmıştır. Bununla birlikte, flash belleğin kurtarma bölümü değiştirildiğinden, tüm flash belleğin bütünlüğü hasar görür. Edinim işlemi sırasında kullanılan Cellebrite UFED 4PC ile bütünlük de hasar görüyor çünkü edinim işlemi normal açılıştan sonra gerçekleştirilmektedir.

Buna karşılık, önerilen erişim yöntemi, tüm flash belleğin bütünlüğünü korumaktadır. Yazılım güncelleme modunda önyüklenir ve fiziksel bilgi edinme, flash bellek okuma komutunu kullanarak gerçekleştirilir. Böylece, tüm flash belleğin bütünlüğünün muhafaza edilip edilmediğini teyit etmek için JTAG tabanlı edinim yöntemini karşılaştırrılabilir. Sonuçların doğruluğunu sağlamak için, deney işlemi bir önceki çalışmada olduğu gibi yerine getirilmiştir (Son ve ark., 2013). Beş kez flash bellek edinimi gerçekleştirildikten sonra edinilen görüntülerin karma değerleri karşılaştırılmıştır.

Edinme hızı

Akıllı telefonların kullanımındaki hızlı artış nedeniyle, analiz edilmesi gereken akıllı telefonların sayısı da hızla artıyor. İncelenmesi gereken telefonlarının sayısı büyük olduğundan, alanda 8 saati aşan bir edinme zamanı gerektiren JTAG tabanlı erişim yöntemini kullanmak kolay değildir. Bu nedenle, hızlı S/W tabanlı edinim yöntemleri sıklıkla kullanılır. Tüm flash bellek için edinme süresini karşılaştıran sonuçlar Tablo 5'te gösterilmiştir. Sonuçlar, 8 modelin edinme sürelerinin ortalama değerlerini temsil etmektedir. Önerilen yöntem, verileri bir bilgisayara göndermek için akıllı telefonun maksimum boyutunu ayarlayabildiğinden, diğer yöntemlerle edinme süresinden yaklaşık dört kat daha hızlıdır. 32 GB flaş bellek elde etmek için ortalama olarak 30 dakika gerekiyordu.

	Açıklanan yöntem	Cellebrite UFED 4P	Özel kurtarma modu	Root'larak ADB ile döküm alma	JTAG yöntemi
Bütünlük garantisi	0	0	X	X	0
Imaj alma hızı (32GB)	30 dk.	120 dk.	120 dk.	180 dk.	480 dk. [a]
Ekran kilitli akıllı telefonun imajı alma	0	0	X	X	0

[a] ***JTAG tabanlı edinme yönteminde cihazı sökme ve adaptörü bağlantı süresi hariç tutulmuştur***

Tablo 5 – Deney sonuçları

Ekranı kilitli akıllı telefonlardan fiziksel olarak edinme (USB hata ayıklama devre dışı)

Çoğu S/W tabanlı adli araç, fiziksel edinim için ADB protokolünü kullanır. ADB protokolünü kullanmak için akıllı telefonda USB hata ayıklamasının etkinleştirilmesi gerekir. Bununla birlikte, tüm Android akıllı telefonlar güvenlik nedenlerinden ötürü varsayılan olarak USB hata ayıklaması devre dışı bırakılmış olarak teslim edilir. Böylece, mevcut kazanım yöntemlerini uygulamak için USB hata ayıklamasının etkinleştirilmesi gerekir. Bu nedenle, bir desen veya kullanıcı şifresi tarafından kilitlenmiş (USB hata ayıklamalı devre dışı bırakılmış) bir akıllı telefondaki mevcut yöntemlerden birini kullanarak fiziksel edinimi gerçekleştirmek imkansızdır. Bu eksiklik, Android'in fiziksel edinimi alanında çözülmesi gereken önemli bir konudur. Bununla birlikte, önerilen yöntem bu sorunun üstesinden gelmektedir. Ekranı kilitli bir akıllı telefon olsa bile, telefon kapalıyken ve firmware güncelleme modunda yeniden başlatıldıktan sonra fiziksel olarak edinme gerçekleştirmek mümkündür.

Sonuç

Android akıllı telefonların firmware güncelleme protokollerini analiz ederek tüm flash belleği elde etmek için yeni bir yöntem geliştirdik. Üreticiler tarafından sağlanan firmware güncelleme programlarını çözdük ve firmware güncelleme protokollerini önyükleme yükleyicisinde analiz ettik. Üretici yazılımı güncelleme protokollerinin analitik sonuçlarına dayanarak, bazı flash bellek güncelleme protokollerinde flaş bellek okuma komutlarının korunduğunu ve dolayısıyla fiziksel edinimin gerçekleştirilebileceğini bulduk. Flash bellek okuma komutları kaldırıldığında cihazda yer almadığı durumlarda, okuma komutunun eklenmesi için ek araştırma gereklidir. Bu yeni edinme yöntemine dayanarak, 80'in üzerinde en yeni Android modellinin flash belleğinin fiziksel olarak dışarı aktarılmasını destekleyen bir edinme programı geliştirdik. Önerilen aracı mevcut yöntemlerle karşılaştırarak, yöntemimizin tüm flash belleğin bütünlüğünü koruduğunu ve yüksek hızlı elde ettiğini kanıtladık. Bunu yaparken de bir desen veya kullanıcı parolası ile ekran kilitlemesine bağlı kısıtlamaya bakılmaksızın fiziksel edinme yapılabilir.

Önerilen edinme yöntemi, yeni Android akıllı telefonlar her başlatıldığında firmware güncelleme protokolünü analiz etmeniz gerektiği konusunda bir sınırlama getirir. Bununla birlikte, üretici yazılımı güncelleme protokolü tüm Android akıllı telefonların önyükleme yükleyicisinde uygulanır ve diğer taraftan her üretici tüm modellerine aynı üretici yazılımı güncelleme protokolünü uygular. Bu şekilde edinme yöntemi analiz edilerek üreticilerin tüm modelleri için fiziksel edinme gerçekleştirilmesine izin veren yazılım güncelleme protokolü bulunabilir. Bu nedenle, bu alanda sürekli araştırma yapılması gerekmektedir.

Kaynaklar

AccessData MPEþ
http://accessdata.com/solutions/digitalforensics/mpe; 2014.
Android Backup Extractor.
http://sourceforge.net/projects/adbextractor/; 2014.
Android Debug Bridge (ADB).
http://developer.android.com/tools/help/adb.html.
Android software development e fastboot.
http://en.wikipedia.org/wiki/
Android_software_development#Fastboot; 2014.
Breeuwsma M, Jongh M, Klaver C, Knijff R, Roeloffs M.
Forensic data recovery from flash memory. Small Scale
Digital Forensics J 2007;1(1):
Bring your own device.
http://en.wikipedia.org/wiki/Bring_your_ own_device; 2014.
Cellebrite UFED 4PC. http://www.cellebrite.com/Mobile-
Foensics/Products/ufed-4pc;
Cellebrite UFED Physical Analyzer.
http://www.cellebrite.com/MobileForensics/Applications/ufe
d-physical-analyzer; 2015.
Grover J. Android forensics: automated data collection and
reporting from a mobile device. Digit Investig
2013;10:S12e20.
Guidance EnCase. http://www.guidancesoftware.com/; 2014.
Hannay P. Kindle forensics: acquisition & analysis. Proc
Conf Digital Forensics, Secur Law 2011;6(2):143e50.
Hex-Rays. https://www.hex-rays.com/index.shtml/; 2015.
High-Level Data Link Control (HDLC).
http://en.wikipedia.org/wi ki/HighLevel_Data_Link_Control.
Hoog A. Android forensics. Mobile forensics world 2009.
Hoog A. Android forensics: investigation, analysis and
mobile security for
Google Android. Syngress; 2011.
HTC Sync Manager. http://www.htc.com/us/software/htc-sync-
manager/; 2014.
Iqbal A, Alobaidli H, Baggili I, Marrington A. Amazon
kindle fire HD forensics. In: Digital forensics and cyber
crime; 2013. p. 39e50.
Jovanovic Z. Android forensics techniques. International
Academy of
Design and Technology; 2012.
Kim K, Hong D, Ryu J. Forensic data acquisition from cell
phones using JTAG
interface. Information Security Research Division; 2008.
p. 410e4.
Lessard J, Kessler G. Android forensics: simplifying cell
phone examinations. Small Scale Digital Device Forensics J
2010;4(1):1e12.
LG Software & tools Download.
http://www.mylgphones.com/lgsoftware-tools download; 2014.

MSAB XRY. https://www.msab.com/products/xry; 2015.
MultiMediaCard.
http://en.wikipedia.org/wiki/MultiMediaCard #eMMC; 2014.
Mutawa N, Baggili I, Marrington A. Forensic analysis of
social networking
applications on mobile devices. Digit Investig
2012;9:S24e33.
ORT tool. http://www.orttool.com; 2014.
Oxygen Forensics. http://www.oxygen-forensic.com/; 2014.
Pantech Self-Upgrade.
http://www.pantechservice.co.kr/down/self/main.sky; 2014.
R-Linux. http://www.r-
tt.com/free_linux_recovery/index.shtml/; 2014.
RIFF box. http://www.riffbox.org; 2014.
Rooting (Android OS).
http://en.wikipedia.org/wiki/Rooting_ (Android_OS); 2014.
Samsung Kies. http://www.samsung.com/us/kies/; 2014.
Samsung KNOX. http://www.samsungknox.com/; 2014.
Samsung Odin. http://odindownload.com/; 2014.
Secure Boot.
https://source.android.com/devices/tech/security/secureboo
t/index.html; 2014.
Smartphone OS Market Share Q3 2014.
http://www.idc.com/prodserv/smartphone-os-market-
share.jsp; 2014.
Son N, Lee Y, Kim D, James J, Lee S, Lee K. A study of
user data integrity during acquisition of Android devices.
Digit Investig 2013;10:S3e11.
Sony PC Companion.
http://support.sonymobile.com/gb/tools/pccompanion/; 2014.
Sylve J, Case A, Marziale L, Richard G. Acquisition and
analysis of volatile
memory from android devices. Digit Investig 2012;8:175e84.
Vidas T, Zhang C, Christin N. Toward a general collection
methodology for Android devices. Digit Investig
2011;8:S14e24.
XDA developers. How to make your own usb jig. 2012.
http://forum.xdadevelopers.com/galaxy-s2/help/guide-how-
to-make-use-jig-resetbinary-t1604707.
XDA developers. LG 910K USB flash cable scheme. 2012.
http://forum.xdadevelopers.com/showthread.php?t¼2069564.
Xiaomi Download MiFlash for Xiaomi Smartphone.
http://www.jayceooi.
com/download-miflash-for-xiaomi-smartphone/; 2015.
Z3X box. http://z3x-team.com; 2014