فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی ـ ترویجی
سال دوازدهم، شمارهٔ چهل‌وپنجم، زمستان ۱۳۹۶

تاریخ دریافت: ۱۳۹۶/۰۹/۲۰
تاریخ پذیرش: ۱۳۹۶/۱۱/۰۴

ارائه الگوی فرایندی پی جویی جرائم در گوشی‌های هوشمند

وحید یادگاری[۱]، سجاد راسخ[۲]

چکیده

زمینه و هدف: در سال‌های اخیر شاهد تغییر مداوم فنّاوری از رایانه‌های رومیزی به دستگاه‌های تلفن همراه بوده‌ایم. محبوبیت گوشی‌های هوشمند به عنوان ابزاری پرکاربرد و چند منظوره که در سطوح مختلف جامعه نفوذ پیدا کرده، در حال افزایش است. گوشی‌های هوشمند به دلیل چند منظوره بودن برای انجام اموری همچون پرداخت قبوض، خرید برخط، مدیریت حساب مالی، جستجو در شبکه‌های اجتماعی و رایانامه به‌کار می‌روند ازاین‌رو به اطلاعات مهم و حساسی دسترسی دارند که می‌تواند فرصت مناسبی برای مجرمان سایبری فراهم کند. شبیه تمام فنّاوری‌های دیگر، نقص‌های امنیتی تلفن‌های همراه هوشمند، افراد و سازمان‌ها را در معرض خطرهای جدی قرار می‌دهد. دستگاه‌های غیر امن، برنامه‌های کاربردی دارای نشتی و آسیب‌پذیری، ایجاد آسیب‌پذیری به صورت سلاحی علیه امنیت و افزایش نرخ توسعهٔ بدافزارهای پیشرفته تلفن همراه، همگی تهدیدهایی جدی برای زیست‌بوم سامانهٔ هوشمند تلفن همراه محسوب می‌شوند. مجموعه این زیست‌بوم ناامن چگونگی تفکر در مورد پاسخ به جرائم گوشی‌های هوشمند را شکل می‌دهد و ارگان‌ها، سازمان‌های خصوصی و دولتی را ملزم به پشتیبانی از راهبرد پاسخ به جرائم گوشی‌های هوشمند می‌کند. هدف از این تحقیق ارائه یک الگوی مفهومی کاربردی برای ارائه پاسخی متفاوت از پاسخ به جرائم رایانهٔ شخصی و رایانهٔ همراه است.

روش‌شناسی: در این نوشتار از روش توصیفی با بهره‌گیری از منابع اسنادی، کتابخانه‌ای و رایانه‌ای استفاده شده است.

یافته‌ها و نتیجه‌گیری: از آن‌جایی‌که پاسخ به این‌گونه جرائم به دلایلی که بیان خواهد شد، متفاوت از پاسخ به جرائم رایانهٔ شخصی و رایانهٔ همراه است، در این تحقیق فرایند رسیدگی به جرائم گوشی‌های هوشمند و کارکردهای سایبری وابسته، انواع جرائم تلفن همراه، ابزارهای مورد نیاز برای رسیدگی به این جرائم بررسی، تبیین و یک الگوی مفهومی کاربردی ارائه شده است.

کلیدواژه‌ها: جرائم سایبری، شواهد الکترونیکی، فارنزیک، فضای سایبر، گوشی‌های هوشمند.

---

۱. نویسندهٔ مسئول: کارشناس ارشد مهندسی فنّاوری اطلاعات دانشگاه تربیت مدرس (رایانامه: V.Yadegary58@yahoo.com).
۲. کارشناس مهندسی فناوری نرم‌افزار رایانه.

مقدمه

تلفن‌های همراه به دلیل ماهیت متحرک‌بودن، دسترس‌پذیری بالا و امکانات متنوع ارتباطی، در طی سالیان گذشته بسیار مورد توجه قرار گرفته‌اند. با توجه به اینکه سیستم‌عامل اندروید توسط شرکت‌ها و توسعه‌دهندگان نرم‌افزاری مختلفی مورد استفاده قرار می‌گیرد، سهم بازار این سیستم‌عامل در دستگاه‌های همراه بسیار بیشتر از سیستم‌عامل‌های دیگر است. اندروید به صورت پیش‌فرض دارای برخی سازوکارهای امنیتی برای تأمین حداقل امنیت است؛ امّا این امنیت برای امن‌سازی اندروید کافی نیست و همواره مجرمان سایبری با شناسایی نقطه ضعف‌های امنیتی، اقدام به اعمال مجرمانه در گوشی‌های هوشمند می‌کنند. در پاسخ به فعالیت‌های مجرمان، نیاز است روش‌های کشف ادلهٔ دیجیتال در تلفن همراه مورد توجه باشد.

برای اینکار نیاز به جرم‌یابی و جمع‌آوری اطلاعات از دستگاه‌های اندرویدی است تا بتوان مشکلات و سوءاستفاده‌های امنیتی را تشخیص داده و آنها را تحلیل کرد. در این مقاله، پس از بیان مقدمه‌ای در مورد اندروید، مؤلفه‌های کلیدی امنیت اندروید و نحوهٔ جرم‌یابی اندروید به‌صورت عملی شرح داده می‌شود. سپس ابزارهای مورد استفاده برای جرم‌یابی اندروید معرفی شده و در نهایت چگونگی تحلیل اطلاعات به‌دست‌آمده از جرم‌یابی اندروید در قالب یک الگوی مفهومی کاربردی ارائه خواهد شد.

مبانی نظری

اهمیت و ضرورت تحقیق

گوشی‌های هوشمند به دلیل چند منظوره بودن برای انجام اموری همچون پرداخت قبوض، خرید برخط، مدیریت حساب مالی، جستجو در شبکه‌های اجتماعی و رایانامه به‌کار می‌روند ازاین‌رو به اطلاعات مهم و حساسی دسترسی دارند که

می‌تواند فرصت مناسبی برای مجرمان سایبری فراهم کند. شبیه تمام فنّاوری‌های دیگر، نقص‌های امنیتی تلفن‌های هوشمند همراه، افراد و سازمان‌ها را در معرض خطرهای جدی قرار می‌دهد. دستگاه‌های غیرامن، برنامه‌های کاربردی دارای نشتی و آسیب‌پذیری، ایجاد آسیب‌پذیری به صورت سلاحی علیه امنیت و افزایش نرخ توسعهٔ بدافزارهای پیشرفته تلفن همراه، همگی تهدیدهایی جدی برای زیست‌بوم سامانهٔ هوشمند تلفن همراه محسوب می‌شوند. در پاسخ به این تهدیدها، علم تلفن همراه فارنزیک یا کشف ادلهٔ جرم در گوشی‌های هوشمند مطرح است و ضرورت دارد با مطالعه و فراگیری روش‌ها و ابزارهای کاربردی این حوزه، اقدام‌های مجرمان مستندسازی و به مرجع قضایی ارائه شود.

هدف‌های تحقیق

هدف اصلی: ارائه الگویی ترکیبی برای پی‌جویی جرائم در گوشی‌های هوشمند و کارکردهای سایبری وابسته.

هدف‌های فرعی

۱. شناخت زیست‌بوم و مؤلفه‌های سخت‌افزاری، میان‌افزاری و نرم‌افزاری گوشی‌های هوشمند؛

۲. بررسی روش‌ها و سطوح پی‌جویی جرائم در گوشی‌های هوشمند؛

۳. ارائه الگویی ترکیبی کاربردی برای پی‌جویی جرائم در گوشی‌های هوشمند.

تعاریف و اصطلاح‌ها

فضای سایبر[1]: در سند راهبردی دفاع سایبری جمهوری اسلامی ایران، فضای سایبری به صورت زیر تعریف شده است «مجموعه‌ای از سامانه‌ها و شبکه‌های رایانه‌ای شامل نیروی انسانی، زیرساخت‌ها، تجهیزات، سخت‌افزار، نرم‌افزار و سامانه‌های ارتباطی، نظارتی و مدیریتی است که به منظور تولید، ذخیره‌سازی، پردازش، تبادل و بهره‌برداری از اطلاعات ایجاد و سازماندهی شده‌اند» (سند راهبردی دفاع سایبری، ۱۳۹۱).

---

1 - Cyber Space

جرائم سایبری: جرائم سایبری در اصطلاح به جرائمی گفته می‌شود که در محیطی غیرفیزیکی، علیه فنّاوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی شده انجام می‌شود. امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فنّاوری اطلاعات و ارتباطات به‌شدت متحول شده و به جرائم سایبری تبدیل‌شده‌اند. جرائم سایبری نیز برای گسترش خود، رفته‌رفته جانشین عبارت‌هایی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فنّاوری اطلاعات نیز گفته می‌شود. (بهره‌مند و دیگران، ۱۳۹۳) به بعضی از مصادیق جرائم سایبری در جدول زیر اشاره شده است:

جدول شمارهٔ ۱

سرقت محصولات فکری (theft of intellectual property)	دزدی شناسه (Identity theft)
اخاذی اینترنتی (internet extortion)	رخنه (hack)
فریب‌کاری سرمایه‌گذاری (investment fraud)	بدافزاریاب وکرم رایانه‌ای (worm, virus)
دزدی نرم‌افزاری (software piracy)	حملهٔ ممانعت از خدمات (DoS)
اختلاس (embezzlement)	آزار سایبری (cyber stalking)
قاچاق کلمهٔ عبور (password trafficking)	قلدری سایبری (cyber bullying)
فریب‌کاری در ضمانت (serew services fraud)	قاچاق مواد مخدر (Drug trafficking)
چک جعلی تحویل‌دار (counterfeit eashier's check)	حذف بدهی (debt elimination)
فریب‌کاری با دست‌کاری در برنامه (program manipulation fraud)	دزدی حق نسخه‌برداری (copyright piracy)
فریب‌کاری باکارت اعتباری (credit card fraud)	نفوذ به سامانه (Penetration into the system)
وب‌ربایی (webjacking)	بدنامی سایبری (cyber defamation)

فریب‌کاری در حراج برخط (online auction fraud)	خسارت به شبکه خدمات شرکت (Damage to company service networks)
بمباران رایانامه و هرزنامه (email bombing and spamming)	پورنوگرافی (pornography)
فریب‌کاری مالی (financial fraud)	جرائم مخابراتی (telecommunication crime)

گوشی‌های هوشمند: گوشی‌های هوشمند با قابلیت‌های خاص و کاربردهایی نظیر رایانه‌های شخصی هستند؛ امّا لازم است ذکر شود که بدانید نمی‌توانند به قدرت رایانه‌ها کار کنند. گوشی‌های هوشمند به اینترنت وصل می‌شوند، دارای صفحه نمایش لمسی و دوربین هستند و برنامه‌های شخص ثالث و پخش‌کننده‌های موزیک را نیز اجرا می‌کنند (آبادی و دیگران: ۱۳۹۵).

جرم‌یابی دیجیتال (فارنزیک[1]): فرایند استفاده از دانش علمی برای گردآوری، تجزیه و تحلیل اطلاعات موجود بر روی سامانه‌های دیجیتال به منظور یافتن شواهد و مدارک احتمالی برای یک دادرسی را جرم‌یابی دیجیتال یا فارنزیک می‌گویند.

زیست‌بوم و ساختار گوشی‌های هوشمند

زیست‌بوم و ساختار گوشی‌های هوشمند را به شرح ذیل می‌توان بررسی و تشریح کرد (Homeland Security Report, 2017).

۱. فنّاوری‌های گوشی همراه هوشمند شامل سخت‌افزار، سیستم‌عامل و سخت‌افزارهای افزودنی مثل سیم کارت و... ؛

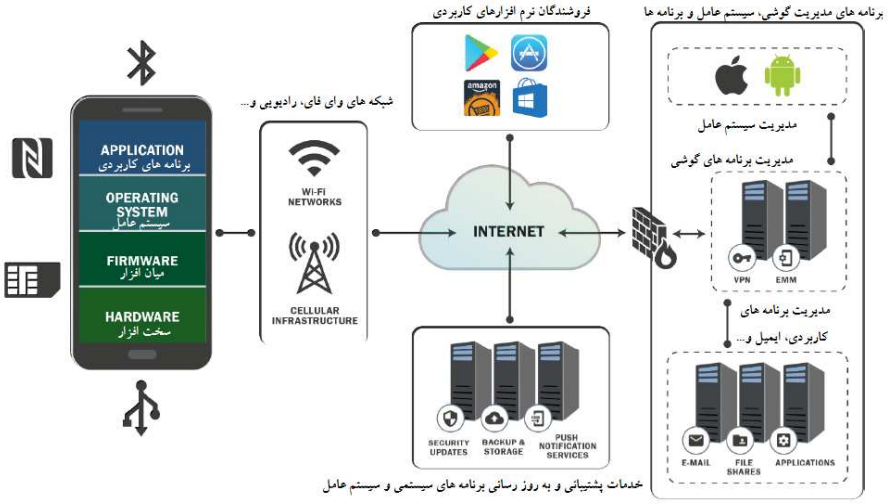
۲. برنامه‌های کاربردی و عمومی؛

۳. شبکه‌های ارتباطی مثل ارتباط با وای‌فای، بلوتوث، ارتباط رادیویی و خدمات دیگر که توسط اپراتورهای تلفن همراه ارائه می‌شود؛

1-Forensic

۴. فروشندگان خدمات کاربردی و سامانه‌ای شامل برنامه‌های پشتیبانی و به‌روزرسانی برنامه‌های رایانه‌ای، سیستم‌عامل و برنامه‌های کاربردی می‌شود. این خدمات به طور معمول توسط شرکت‌های سازندهٔ گوشی، سیستم‌عامل و برنامه‌های کاربردی ارائه می‌شود؛

۵. خدمات و زیر ساخت‌های اساسی شامل برنامه‌های مدیریت گوشی هوشمند[۱]، سیستم‌عامل گوشی هوشمند و مدیریت برنامه‌های کاربردی[۲] است.

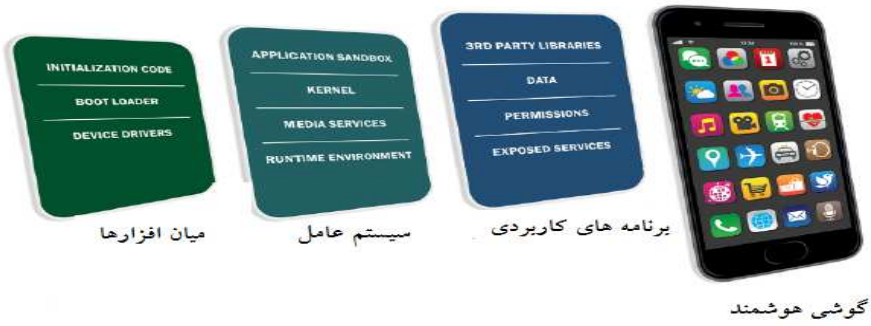


شکل ۱- ساختار گوشی‌های هوشمند(Homeland Security Report, 2017)

۱) **شناخت نرم‌افزاری گوشی هوشمند:** گوشی‌های هوشمند نیز همانند رایانه‌ها دارای نرم‌افزارهای رایانه‌ای[۳]، میان‌افزارها[۴] و برنامه‌های کاربردی[۵] هستند. نرم‌افزارهای سامانه‌ای در گوشی هوشمند با نام نرم‌افزار تلفن همراه شناخته می‌شود و از انواع آن می‌توان به سیستم‌عامل‌هایی مثل اندروید و آی او اس و... اشاره کرد. میان‌افزارها نیز

1- Mobile Device Management (MDM)
4- Mobile Application Management (MAM)
3-System software(Mobile OS)
4-Firm Ware
5-Application

به برنامه‌هایی که هماهنگی بین سخت‌افزار و نرم‌افزار را بر عهده دارند مثل نرم‌افزارهایی که سخت‌افزار را به سیستم معرفی و راه‌اندازی می‌نمایند و با نام درایور[1] شناخته می‌شوند و... اطلاق می‌شود و به نرم‌افزارهای کاربردی مثل گوگل مپ، فتوشاپ و... نیز برنامهٔ کاربردی یا اپلیکیشن گویند.



شکل ۲- لایه‌های نرم‌افزاری گوشی‌های هوشمند(Homeland Security Report, 2017)

۲) **شناخت سخت‌افزاری گوشی هوشمند:** گوشی هوشمند شامل قسمت‌های مختلف سخت‌افزاری مثل باطری، مانیتور لمسی و یا معمولی، پردازنده، حافظهٔ داخلی و بیرونی و فنّاوری‌های ارتباطی و... است که در شکل ۳ کلیات آن توضیح داده شده است.

شکل ۳-فنّاوری‌های گوشی(Homeland Security Report, 2017)

1- Driver

در مراحل بعدی، مهم‌ترین اجزا و فنّاوری‌های گوشی که در موضوع امنیت نیز نقش اساسی دارند تشریح می‌شود.

۳) **شناخت رسانه‌های ذخیره‌ساز گوشی همراه :** یکی از قسمت‌های مهم به لحاظ امنیتی در گوشی‌های هوشمند، قسمت‌هایی است که می‌تواند ذخیره کنندهٔ اطلاعات باشد. در ادامه انواع حافظه در گوشی شرح داده می‌شود.

آی سی فلش و حافظهٔ داخلی

محل اول ذخیرهٔ اطلاعات اصلی کاربران تلفن‌های همراه و تبلت‌ها و تجهیزات مشابه، به‌صورت یک یا دو تراشه است که از کارخانه بر روی برد لحیم شده‌اند. این دو تراشه به‌صورت ذیل طبقه‌بندی‌شده‌اند:

۱. آی سی فلش[1] که شامل سیستم‌عامل گوشی و یا تبلت است؛

۲. حافظهٔ داخلی که به‌عنوان یک حافظهٔ کمکی است.

آی سی فلش و هارد کمکی نیز یک تراشهٔ کوچک حاوی سیستم‌عامل (جاوا، سیمبین، اندروید، iOS و...) تلفن همراه است. در واقع وقتی یک گوشی از لحاظ نرم‌افزاری دچار مشکل می‌شود یعنی اطلاعات درون این آی سی، دچار مشکل شده است. اطلاعاتی که در این تراشه ذخیره می‌شود شامل موارد ذیل است که در گوشی‌ها و تبلت‌ها و ... متفاوت است:

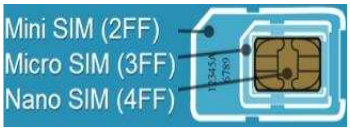
- شماره‌های گرفته‌شده؛
- شماره‌های دریافت شده؛
- دفترچهٔ تلفن؛
- پیامک‌ها؛
- پست‌های الکترونیکی و رایانامه‌ها؛
- فعالیت‌های اینترنتی؛
- نرم‌افزارها؛

1-ROM Memory

- اطلاعات صاحب تلفن همراه؛
- و ... (فریدون‌نژاد، ۱۳۹۴: ۱۲).

حافظهٔ سیم‌کارت

حافظهٔ دیگری که برای ذخیرهٔ اطلاعات در تلفن‌های همراه و برخی از تبلت‌ها استفاده می‌شود، تراشهٔ کوچکی به نام سیم‌کارت است.



سیم‌کارت[1] یک تراشهٔ الکترونیکی است که با حافظهٔ دائمی اندکی از طرف مخابرات به مشترک ارائه می‌شود. مخابرات از طریق سیم‌کارت مشترک را شناسایی و امکان برقراری تماس را به وجود می‌آورد و همچنین از طریق سیم‌کارت، خدمات نیز ارائه می‌کند. هر سیم‌کارت دارای یک شمارهٔ ۱۱ رقمی است که مخابرات امکان برقراری تماس و شناسایی کاربر را از طریق این شماره انجام می‌دهد. سیم‌کارت، اطلاعات شناسایی شخصی، شماره تلفن همراه، دفترچهٔ تلفن، پیام‌های متنی و دیگر دیتاها را نگه می‌دارد. سیم‌کارت‌ها از لحاظ حجم حافظه دارای اندازه‌های متفاوت ۱۶، ۳۲، ۶۴ و ۵۱۲ کیلوبایتی هستند و موارد توزیع و استفادهٔ آنها بستگی به گستردگی شبکه تلفن همراه آن منطقه دارد. حافظه‌های ۱۲۸ و ۵۱۲ مگابایتی هم در بازار وجود دارد. سیم‌کارت شامل اطلاعات به خصوصی از شبکه است که برای تصدیق، شناسایی و خدمات‌گیری مشترکان در شبکه مورد استفاده قرار می‌گیرد این اطلاعات عبارت‌اند از:

- شماره شناسایی بین‌المللی: عدد ۱۹ یا ۲۰ رقمی است که بر روی بدنهٔ سیم‌کارت حک شده است؛
- شناسه ناحیه مکانی: اطلاعات مربوط به جایگاه مشترک در شبکه است؛

1Subscriber Identity Module

- حافظه دفترچه تلفن: توسط این قابلیت می‌توان در سیم‌کارت‌ها لیست مخاطبان در دفترچه تلفن را ضبط و اضافه کرد؛
- حافظه پیام کوتاه: با کمک این قابلیت حداکثر می‌توان ۲۰ پیغام نوشتاری در داخل سیم‌کارت ذخیره کرد.

کارت حافظه (ممورى کارت)

حافظهٔ دیگری که برای ذخیرهٔ اطلاعات در تلفن‌های همراه، تبلت‌ها و دستگاه‌های این‌چنینی استفاده می‌شود، تراشه‌ای به نام کارت حافظه است. این تراشه دارای اندازه‌های مختلفی است که در اکثر تلفن‌های همراه، تبلت‌ها و دوربین‌های دیجیتال و دستگاه‌های دیجیتال مشابه مورد استفاده قرار می‌گیرد. مقدار حافظهٔ این تراشه‌ها متفاوت است. (۲، ۴، ۸، ۱۶، ۳۲، ۶۴ و ... گیگابایت) امروزه اکثر دستگاه‌های تلفن همراه، تبلت‌ها و ... دارای حافظهٔ جانبی (ممورى کارت) هستند (فریدون‌نژاد، ۱۳۹۴: ۱۳).

چارچوب و فازهای بررسی جرم در گوشی‌های هوشمند

استانداردهای بررسی جرم در رایانه دو نوع است:

نخستین استاندارد McKemmish است که مربوط به سال ۱۹۹۹ میلادی است و در این استاندارد ابتدا شناسایی[1] سپس حفاظت[2] و بعد از آن تجزیه و تحلیل[3] و در آخر گزارش‌گیری[4] انجام می‌گیرید.

دومین استاندارد NIST است که مربوط به سال ۲۰۰۶ بوده و ترتیب انجام عملیات به این صورت است که ابتدا جمع‌آوری[5] سپس بررسی[6] و بعد از آن تجزیه و تحلیل و در آخر گزارش‌گیری است.

1- Identification
2 - Preservation
3 - Analysis
4 - Reporting
5- Collection
6 - Examination

از تلفیق این دو استاندارد در سال ۲۰۱۴ میلادی استانداردی با همان نام NIST برای گوشی‌های هوشمند طراحی شد که به ترتیب ۱.حفاظت؛ ۲.جمع آوری؛ ۳.تجزیه و تحلیل و بررسی و ۴.گزارش گیری انجام می گیرد (آبادی و دیگران: ۱۳۹۵).

چارچوب بررسی جرم در رایانه‌ها

NIST (۲۰۰۶) framework
1. Collection
2. Examination
3. Analysis
4. Reporting

McKemmish (۱۹۹۹) framework
1. Identification
2. Preservation
3. Analysis
4. Reporting

NIST (۲۰۱۴) framework
1. Preservation
2. Collection
3. Analysis/Examination
4. Reporting

چارچوب بررسی جرم در گوشی‌های هوشمند: در این قسمت تمامی مراحل مربوط به چارچوب بررسی جرم در گوشی‌های هوشمند مورد بررسی قرار می گیرد.

مرحلهٔ حفاظت: فرایندی ایمن برای حفاظت از دارایی‌ها، بدون اینکه اصلاح و یا تغییر در محتویات داده‌های موجود بر رسانه‌ها صورت بگیرد (دریابار: ۱۳۹۵).

تأمین امنیت و بررسی صحنهٔ جرم

۱. جداسازی باتری برای جلوگیری از اتصال الکتریکی (غوطه‌وری در یک مایع)؛

۲. قطعات سالم حافظه را از گوشی تلفن همراه آسیب‌دیده خارج و محتویات آنها را به طور مستقل بازیابی کرد.

مستندسازی از صحنهٔ جرم

۱. رکوردی از تمام داده‌های قابل مشاهده ایجاد شود (منظور بایگانی کردن مدارک)؛

۲. عکاسی از صحنهٔ جرم و محتویات صفحهٔ نمایش.

جداسازی (ایزولاسیون)

جداسازی یا قطع از شبکه‌های متصل شده برای جلوگیری از موارد زیر به کار می‌رود:

۱. جلوگیری از رمزهای مَستر ریست؛

۲. جلوگیری از داده‌های ورودی (تماس‌ها و یا پیامک‌های متنی) که وضعیت فعلی داده‌های گوشی را تغییر می‌دهند؛

۳. جلوگیری از تشخیص موقعیت جغرافیایی کارشناس جرم‌یابی؛

۴. جلوگیری از ریسک بازنویسی اطلاعات جدید بر روی اطلاعات قبلی.

راه کارها

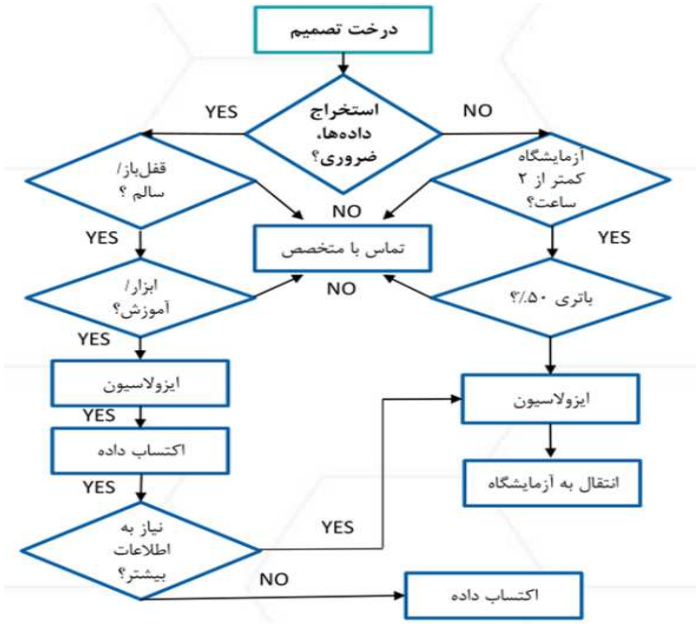
۱. فعال کردن حالت هواپیما، مانع استفاده از GPS نمی‌شود؛

۲. خاموش کردن دستگاه گوشی تلفن همراه، فعال‌سازی رمزهای احراز هویت و از دست دادن حافظهٔ موقت[1]؛

۳. کاورهای ضدامواج رادیویی؛[2]

۴. دستگاه‌های پارازیت.[3]

در شکل زیر مراحل تصمیم‌گیری در صحنهٔ جرم را نشان می‌دهد



1 - RAM
2 - RIC
3- Jamming

مرحلهٔ شناسایی و جمع‌آوری اطلاعات

این فاز با شناسایی گوشی هوشمند مورد نظر آغاز می‌شود

- اجزاء و نوع گوشی، سیستم‌عامل و ویژگی‌های دیگر مسیر ایجاد یک کپی قانونی (ایمیج‌گیری) و مستندسازی از محتویات دستگاه مورد نظر را تعیین می‌کند؛
- اطلاعاتی که به طور کلی استخراج می‌شوند، نشان می‌دهند که باید از کدام ابزارها و روش‌ها در بررسی جرم استفاده کرد؛
- سپس فرایند ایمیج‌گیری (رونوشت‌برداری) از اطلاعات داخل گوشی تلفن همراه انجام می‌شود؛
- فرایند ایمیج‌گیری در صحنه از آن‌جایی‌که در این نوع ایمیج‌گیری محدودیت زمانی وجود دارد؛ بنابراین، فقط در موارد خاصی که زمان بیشتری در دسترس باشد قابل انجام است؛
- فرایند ایمیج‌گیری خارج از محل واقعه، در محلی که بتوان در آن با تجهیزات مناسب کار کرد مانند آزمایشگاه فارنزیک و در عین حال پیش‌نیازهای فرعی را هم برآورده کرد این پیش‌نیازها مانند حفاظت از خود سامانه و اطلاعات داخل آن است که در بخش قبلی به آن پرداخته شد؛
- برای جمع‌آوری و ایمیج‌گیری از اطلاعات داخل گوشی باید با ابزارهای مختلف این کار تجربه کنید تا بدانید که کدام ابزار ایمیج‌گیری برای کدام گوشی تلفن همراه به طور مؤثرتری کار می‌کند (دریابار: ۱۳۹۵).

مکان‌های مهم ذخیرهٔ داده‌ها

۱. حافظهٔ داخلی (حافظهٔ رم، حافظهٔ گوشی)؛
۲. حافظهٔ خارجی (حافظهٔ SD)؛
۳. پایگاه‌های داده (SQLiteo)؛
۴. ترافیک شبکه.

روش‌های استخراج اطلاعات

استخراج اطلاعات به سه سطح تقسیم می‌شود که هرچه این سطوح به سمت بالا می‌رود روش‌های موجود در آن فنی‌تر، تهاجمی‌تر، زمان‌برتر و و گران‌قیمت‌تر می‌شود (آبادی و دیگران: ۱۳۹۵).

الف) استخراج به صورت دستی

در این روش برای مشاهده و ثبت محتوای داده‌های ذخیره شده بر روی دستگاه نیاز به دستکاری دستی دکمه‌ها، صفحه کلید و یا صفحه نمایش لمسی را دارند. به طور مثال با استفاده از یک دوربین دیجیتال خارجی، می‌توان اطلاعات کشف شده را ثبت و ضبط کرد.

البته در این روش امکان دارد که اطلاعات موجود بر روی دستگاه در نتیجهٔ یک ارزیابی سهوی تغییر یابند و یا بر روی اطلاعات قبلی، اطلاعات دیگری بازنویسی شود (NikenDwiWahyuCahyani, etl,2016).

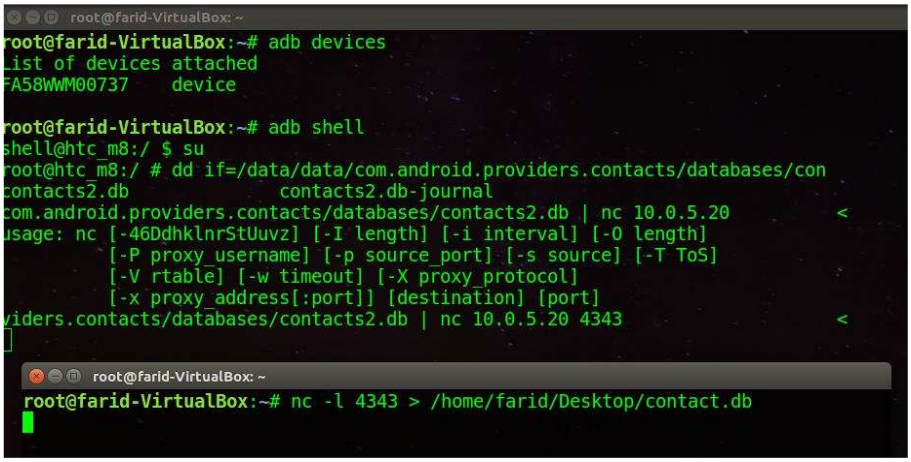
ب) استخراج منطقی[1]

- اتصال بینیک گوشی تلفن همراه و یک دستگاه آزمایشگاهی فارنزیک، با یک اتصال سیمی به عنوان مثال USB و یا RS-232 یا به‌صورت بی‌سیم (وای فای) حاصل می‌شود.
- گرفتن نسخهٔ پشتیبان و یا کپی bit-by-bit از اطلاعات ذخیره شده منطقی (Logical) مانند پایگاه داده، برنامه‌ها، پوشه‌ها و فولدرها، پیام‌ها، اطلاعات تماس و غیره؛

1- Logical

- فولدرهای رایج و مهم
  - (/data/data/<app package name>/:)
  - lib : فایل‌های کتابخانه‌ای برنامه
  - Files : فایل‌های ساخته شده توسط برنامه
  - cache : فایل‌های موقتی
  - Databases(SQLite) : فایل‌های پایگاه داده برنامه
- برای مثال آدرس /data/data شامل پایگاه داده برنامه‌هاست و با دستور زیر می‌توان از SQLite برنامه مورد نظر استخراج منطقی حاصل کرد.

#dd if=/data/data/SUBDIR/DATABASENAME.db of=/PATH



(NikenDwiWahyuCahyani, etl,2016)

ج) استخراج فیزیکی[1]

گرفتن نسخهٔ پشتیبان و یا کپی bit-by-bit از کل محل ذخیره‌سازی به‌صورت فیزیکی از روی حافظه‌ها مانند حافظهٔ SD و RAM

۱. برقراری ارتباط شبکه‌ای بین گوشی اندروید و رایانهٔ فارنزیک (SSH یا NC)؛

۲. استخراج حافظه SD و یا RAM با استفاده از دستور DD؛

1 - Physical

۳. استخراج فیزیکی از RAM.

- / -dev/(f)mem - /dev/kmem

On the forensic workstation:

#nc -l "PORT" /"ADDRESS/FILE_NAME.dd"
On the Android Device:

#dd if=/dev/mem | nc "FORENSIC WORKSTATION IP ADDRESS" "PORT" (Heather mahalik, 2017).

مرحلهٔ بررسی و تجزیه و تحلیل

در این مرحله تمامی اطلاعات به‌دست آمده باید مورد بررسی قرار گیرد و همچنین روش‌های علمی برای آشکارسازی مدارک و شواهد دیجیتال مورد استفاده قرار گیرد هدف‌هایی که در این مرحله پیگیری می‌شود به شرح ذیل است.

- جمع‌آوری اطلاعات در مورد افراد درگیر (چه کسی؟)؛
- تعیین ماهیت دقیق از حوادث رخ داده (چه چیز؟)؛
- ساخت یک جدول زمانی از وقایع (چه زمانی؟)؛
- کشف اطلاعاتی که انگیزه برای حمله را توضیح می‌دهد (چرا؟)؛
- کشف ابزارها یا موارد سوءاستفاده (از چه طریقی؟).

مدارک و شواهدی که می‌توان از یک گوشی هوشمند استخراج کرد شامل

- دفترچه تلفن / اطلاعات تماس؛
- لیست تمام تماس‌های خروجی و ورودی؛
- پیام‌های متنی؛
- پست الکترونیکی؛
- اطلاعات محل سکونت (Leom MD etl,2017).

تجزیه و تحلیل برنامه‌های کاربردی و فایل ها

در تجزیه و تحلیل برنامه‌ها و فایل‌ها ابتدا باید شناسایی روابط بین فایل‌ها صورت گیرد به عنوان مثال: ارتباط‌های فایل‌های پست الکترونیک با پیوست‌های رایانامه، بعد از به‌دست آوردن روابط بین فایل‌ها تحلیل چارچوب زمانی فایل‌ها را مورد بررسی قرار می‌دهیم به‌عنوان مثال تعیین می‌کنیم که وقایع مختلف در چه فواصل زمانی صورت گرفته و ترتیب اتفاق‌های صورت گرفته بر روی گوشی را بر روی Time Line مشخص می‌کند (Berman KJ etl,2015).

تجزیه و تحلیل روش‌های پنهان کردن اطلاعاتی

یکی از کارهای مهمی که بعد از جمع‌آوری اطلاعات از روی سامانه‌ها انجام می‌شود بحث روش برخورد با فایل‌های رمزدار و پنهان است و خود شامل پروسه‌ای پیچیده و زمان‌بر است و ابزار و ترفندهای خاصی را طلب می‌کند این نوع فایل‌ها به سه دسته تقسیم می‌شوند (Grispos G etl,2015).

- فایل‌های محافظت‌شده با کلمهٔ عبور؛
- فایل‌های رمزگذاری شده و فشرده؛
- اطلاعات پنهان نگاری.

ابزارهای بررسی و تجزیه و تحلیل

این ابزارها که به طور معمول دارای قیمت‌های بالایی هستند و تهیه کردن آنها پروسه‌های خاصی دارد به‌دلیل اینکه کاربری آنها فقط برای سازمان‌های اطلاعاتی است؛ بنابراین، به راحتی در اختیار قرار نمی‌گیرند و به طور معمول با واسطه انجام می‌شود؛ در اینجا ما این ابزارها را به دو دسته تقسیم می‌کنیم:

- تجاری

Paraben Mobile Field Kit (MFK)
OxygenForensic Analyst
EnCase® Forensic v 7+

- متن باز

Hex Editors

Autopsy
The Sleuth Kit (TSK)
Scalpel
iCat
Formost (WWW.Digitalintelligence.com,2017).

مرحلهٔ گزارش‌نویسی

قرار بر این است که شواهد و مدارک دیجیتالی و همچنین، ابزارها، روش‌ها و روش‌های استفاده شده به همراه بررسی و تجزیه تحلیل جرم در یک دادگاه قانونی یا محافل دیگر رسمی به چالش کشیده شوند؛ بنابراین، مستندسازی مناسب برای آماده‌سازی افراد برای شرح وقایع و بازرسی‌ها از آغاز تا پایان ضروری است. آماده‌سازی خلاصه‌ای دقیق از تمام اقدام‌های انجام شده و نتایج حاصل از تحقیقاتی که متکی بر اسناد و مدارکی محکم و قابل اطمینان از یادداشت‌ها، عکس‌ها و محتویاتی است که به‌وسیلهٔ ابزارهای گوناگون تولید می‌شوند (ابراهیمی، دریابار و تدین: ۱۳۹۵).

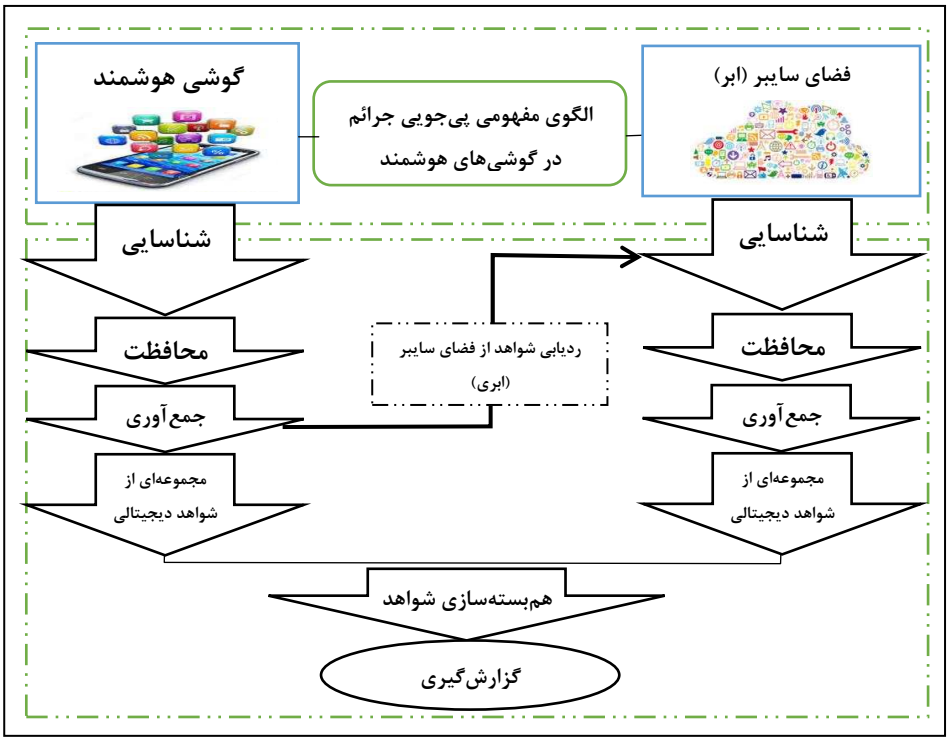
به طور کلی یک گزارش شامل اطلاعات زیر است:

- خلاصه‌ای از درخواست قضایی (مجوز قضایی)؛
- مشخصات آزمایشگاه، سازمان و کارشناسان تحلیلگر فارنزیک؛
- شناسهٔ پرونده یا شمارهٔ سند؛
- مشخصات بازرس پرونده؛
- مشخصات نماینده یا هویت ارسال کننده؛
- تاریخ دریافت شواهد، تاریخ گزارش؛
- لیست شرحِ آیتم‌های ارائه شده برای بررسی و تحلیل، از قبیل شمارهٔ سریال، سری ساخت و الگو؛
- تجهیزات و تنظیمات مورد استفاده در بررسی و تحلیل؛
- شرح مختصری از اقدام‌های انجام شده در طول بررسی، مانند جستجوی رشته‌ای، جستجوی تصاویر گرافیکی، بازیابی فایل‌های پاک شده و غیره (IJACSA, 2016).

نتیجه گیری و پیشنهادها

در این مقاله سعی شده تا با بررسی ساختار گوشی‌های هوشمند مانند سخت‌افزار و نرم‌افزارهای آن و مراحل کشف ادله دیجیتال در گوشی‌های هوشمند و همچنین آشنایی با ابزارها و ترفندهای پی‌جویی جرائم به یک الگوی مفهومی و استاندارد دسترسی پیدا کنیم که با یک نگاه کلی به این الگوی مفهومی بتوان به روند کار و نحوهٔ پی‌جویی جرائم در گوشی‌های هوشمند پی برد. در این الگو علاوه بر جمع‌آوری داده‌های گوشی، اطلاعات فضای مجازی آن مثل فعالیت در شبکه‌های اجتماعی، رایانامه و در اساس هر نوعی دادهٔ ذخیره شده در رایانش ابری نیز جمع‌آوری و توسط یک نمونه هم‌بسته‌سازی می‌شود تا تصویر متحد و یک‌پارچه‌ای از مجموع داده‌های فارنزیکی نمایش داده شود.

الگویی که در این مقاله برای پی‌جویی جرائم در گوشی‌های هوشمند و کارکردهای سایبری وابسته به آن ارائه می‌شود به شکل زیر است:



منابع لاتین

Berman KJ, Glisson WB, Glisson LM (2015) Investigating the Impact of Global Positioning System Evidence. In: Hawaii International Conference on System Sciences, Hawaii, Jan 5–8,2015 (IEEE), 5234–5243

Grispos G, Glisson WB, Storer T (2015) Recovering residual forensic data from smartphone interactions with cloud storage providers.In: KO R, CHOO K-KR (eds) Cloud Security cosystem.

Grispos G, Glisson WB, Storer T (2015) Recovering residual forensicdata from smartphone interactions with cloud storage providersIn: KO R, CHOO K-KR (eds) Cloud Security Ecosystem.Syngress, an Imprint of Elsevier, Waltham

Heather Mahalik Report (2016), From WWW.Sans.org.

Homeland Security Report,2017, From WWW.Sans.org

IJACSA, International Journal of Advanced Computer Science and Applications,Vol. 7, No. 1, 2016

Leom MD, DOrazio CJ, Deegan G, Choo K-KR (2017) Forensic Collection and Analysis of Thumbnails in Android. In: Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communication, Helsinki, Finland,Aug 20–22, (IEEE) 1059–1066

Niken DwiWahyu Cahyani1,2 &NurulHidayahAb Rahman1,3 &William Bradley Glisson4 &Kim-Kwang Raymond (2016),The Role of Mobile Forensics in Terrorism InvestigationsInvolving the Use of Cloud Storage Service and Communication Apps, Mobile NetwAppl DOI 10.1007/s11036-016-0791-8

Syngress, an Imprint of Elsevier, Waltham, Berman KJ, Glisson WB, Glisson LM (2015) Investigating theImpact of Global Positioning System Evidence. In: Hawaii International Conference on System Sciences, Hawaii, Jan 5–8, 2015 (IEEE), 5234–5243

WWW.Digitalintelligence.com.

منابع فارسی

آبادی، مهدی؛ فریبا غفاری، مهسا لمیعیان؛ فاطمه شبانی؛ علی شیخی، محسن سائسی (۱۳۹۵) «جرم‌یابی اندروید: راه‌کارها، چالش‌ها و ابزارها»، *همایش ملی امنیت سامانه‌های هوشمند همراه*.

ابراهیمی، شیوا؛ فرید دریابار و محمدحسام تدین (۱۳۹۵)، «رسیدگی به حوادث سامانهٔ هوشمند تلفن همراه و جرم‌شناسی گوشی‌های هوشمند اندروید»، *همایش ملی امنیت سامانه‌های هوشمند همراه*.

بهره‌مند، حمید (۱۳۹۵)، «چالش‌های مقررات تعدد جرم در جرائم سایبری»، *همایش ملی رویارویی باجرائم سایبری چالش‌ها و راه‌کارها*، اسفندماه، تهران.

دریابار، فرید (۱۳۹۵)، *جرم‌شناسی در گوشی‌های هوشمند*، بی‌جا.

سند راهبردی دفاع سایبری سال ۱۳۹۱.

فریدون نژاد، رضا (۱۳۹۴)، *آنچه از تلفن همراه باید بدانید*، تهران: پارس.