تجزیه و تحلیل شبکه و دستگاه کالبدسنجی برنامه های کاربردی اجتماعی پیام رسانی اندروید

چکیده

این پژوهش قانونی با به دست آوردن و تجزیه و تحلیل داده- ذخیره دستگاه و ترافیک شبکه ای از 20 برنامه ی کاربردی محبوب پیام رسانی فوری برای آندروید بدست آمده. ما قادر به بازسازی قسمتی یا کل محتوای پیام از 16 مورد در 20 برنامه ی کاربردی آزمایش شده هستیم، که ضعف در اقدامات امنیتی و حفظ حریم خصوصی به کار گرفته شده توسط این برنامه نشان داده شده، اما ممکن است برای اهداف جمع آوری شواهد توسط دیجیتال پزشکی قانونی تفسیر می شود. این عمل نشان می دهد که ویژگی های این برنامه های کاربردی پیام های فوری است اجازه می دهد که داده مظنون به بازسازی و یا بازسازی جزئی باشد ، و اینکه آیا شبکه پزشکی قانونی و یا پزشکی قانونی دستگاه اجازه بازسازی فعالیت را می دهد. ما نشان می دهیم که در اغلب موارد ما قادر به بازسازی و یا داده های رهگیری مانند: کلمه عبور، تصاویر گرفته شده توسط برنامه های کاربردی، تصاویر، فیلم ها، صدا ارسال شده هستیم، پیام های ارسال شده بیشتر، طرح، تصویر پروفایل و غیره هستند.

لغات کلیدی : شبکه پزشکی قانونی ، پزشکی قانونی ، آندروید ، پیام رسانی فوری ، حفظ حریم خصوصی در برنامه های پیام رسان ، تست امنیت نرم افزار ، برنامه داده

روش شناسی

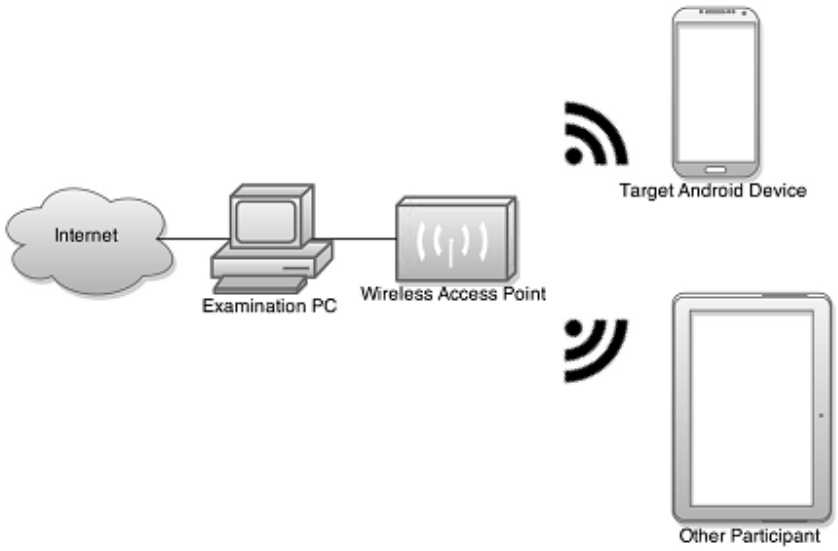
ما 20 برنامه ی پیام / پیام های اجتماعی از طریق مسنجر از فروشگاه Google Play بر اساس دو عامل: کلمه کلیدی و نتایج تعداد دریافت انتخاب کردیم. کلمات کلیدی استفاده شده در هنگام جستجو در فروشگاه گوگل : "چت"، "چت"، "قرار"، "قرار گذاشتن"، "پیام"، و "پیام دادن" بوده است. 20 برنامه ی کاربردی را انتخاب کنید. از بین این نتایج جستجو ما می خواستیم یک طیف گسترده ای از برنامه های کاربردی مبتنی بر یک طیف از محبوبیت را انتخاب کنیم .

برنامه های کاربردی وسیعی از 000،500 بارگیری با بیش از 200 میلیون دانلود انتخاب شده است. ما همچنین می خواهم به یاد داشته باشیم که در این برنامه ها با ارتباط یک به یک متمرکز شده است. برای مثال، ما تنها خصوصیات اینستاگرام و ویژگی های نمایش مشخصات عمومی را مورد مطالعه قرار داده ایم. مثال دیگر این است که ما تنها پیام های مستقیم را در "Snapchat Stories " مورد مطالعه قرار داده ایم.

ما با اجرا کردن شبکه پزشکی قانونی و انجام بررسی ترافیک شبکه از دستگاه در حین ارسال پیام ها و با استفاده از ویژگی های مختلف این برنامه های کاربردی ، این آزمایش را در محیط آزمایشگاه کنترل شده به منظور کاهش تنوع شبکه با توجه به دستگاه های گوشی های هوشمند که اغلب در حال تغییر مرزهای شبکه عامل می باشند انجام شده است. ما همچنین انجام بررسی پزشکی قانونی از دستگاه آندروید خود را برای بازیابی اطلاعات از دستگاه مربوط به فعالیت ها با استفاده از هر یک از برنامه های کاربردی انجام داده ایم . جدول 5 یک لیست از برنامه های کاربردی تست شده که در آن ها مورد آزمایش قرار گرفتند می باشد، شماره نسخه خود را، و ویژگی های آن ها را نشان می دهد.

راه اندازی آزمایشی تجزیه و تحلیل شبکه

در پژوهش های ما با استفاده از یک گوشی HTC One M8 (مدل: # HTC6525LVW، با نسخه اندروید 4.4.2) و همچنین یک آی پد 2 (مدل: # MC954LL / A، با نسخه Ios 7.1.2). ما دو حساب برای هر نرم افزار با استفاده از آندروید و آی پد 2 یک هفته قبل از جمع آوری داده ها ایجاد کرده ایم. دستگاه آندروید هدف بررسی ما بوده است، و اپل به عنوان یک شریک ارتباطات با تبادل پیام با دستگاه مورد نظر استفاده شده است. ما یک کامپیوتر ویندوز 7 با WiFi و یک اتصال اترنت به اینترنت به راه اندازی یک نقطه دسترسی بی سیم استفاده می کنیم . این کامپیوتر به جذب ترافیک شبکه از طریق WiFi و از هر دو دستگاه های تلفن همراه استفاده می کند. این مجموعه در شکل 1 نشان داده شده است.



شکل 1 . راه اندازی شبکه آزمایشی

به منظور جلوگیری از ترافیک شبکه، ما یک نقطه دسترسی بی سیم که به هر دو دستگاه های تلفن همراه متصل شدند ایجاد کرده ایم . این با استفاده از ویندوز 7 مجازی ویژگی وای فای با پورت کوچک آداپتور دارد . این قابلیت به کاربران اجازه می دهد که ایجاد یک شبکه مجازی کنند که می تواند به عنوان یک نقطه دسترسی بی سیم برای دستگاه های متعدد عمل می کنند. برای این کار، کامپیوتر میزبان به اینترنت از طریق یک کابل اترنت متصل شده به طوری که کارت شبکه بی سیم در حال استفاده نیست. اتصال اترنت برای به اشتراک گذاشتن دسترسی به اینترنت خود با وای فای با پورت کوچک آداپتور تنظیم شده است. ما برای اجرا دستور NETSH WLAN تنظیم حالت $kev = 1234567890\ mode = allow\ ssid = test$ به منظور راه اندازی شبکه مجازی است .

پس از آن شبکه با استفاده از $netsh\ wlan\ start\ hostednetwork$ شروع به فعالیت می کند. بنابراین، ما در حال حاضر قادر به دیدن و اتصال به شبکه آزمایشی از دستگاه آندروید (HTC) و iPad هستیم. بعد، ما شروع به صدا و ترافیک شبکه در دستگاه های تلفن همراه با گرفتن اطلاعات فرستاده شده بیش از اتصال مجازی است. تعداد بسته کاهش یافته و میزان جذب ثبت نشده است.

وایرشارک برای گرفتن وذخیره تصاویر ترافیک شبکه استفاده می شود. این فایل های ترایک شبکه را می توان از وب سایت در قسمت داده ها و ابزار دانلود کرد. بعد از بدست اوردن فایل های تصاویر ترافیکی، ما به بررسی آن ها با یک

محقق وایرشارک، شبکه کاو و نت ویتنس پرداختیم. نمودار کامل این در شکل 1 نشان داده شده است. ما برنامه ای را برای ساده سازی این فرایند توسعه دادیم که در بخش 6.1 نشان داده شده است

فعالیت های کاربر

هنگامی که شبکه راه اندازی شده و ترافیک برنامه آغاز شد، ما یک سری از اقدامات، پس از آن تلاش برای تجزیه و تحلیل پزشکی قانونی از دستگاه آندروید و ترافیک شبکه برای بازسازی انجام داده ایم. از آنجا که هر نرم افزار در بانک تست قابلیت متفاوت دارد (همانطور که در جدول 5 ذکر شده)، اقدامات ما بین هر برنامه متنوع انجام شده است چون ما می خواستیم بررسی تمام پیام رسان ها را پشتیبانی کنیم. اقدامات ما با استفاده از نرم افزار هایی که در جدول 5 ذکر شده است انجام می شود.

ما یک گزینه را به طور تصادفی از منبع نوع شواهد بر اساس قابلیت های هر برنامه انتخاب کردیم. پیام های ارسال شده و دریافت شده از این منبع انتخاب شدند چرا که آن ها با جنبه های ارتباطی، که باید محرمانه باشد مقابله می کنند، و یک منبع غنی از شواهد دیجیتال هستند. هنگامی که یک ردیابی برای شواهد فعالیت های واحد پیدا شده و نوع آن ثبت شد. ما پس از آن به ترافیک شبکه و نوع شواهد بعدی در لیست از قابلیت های نرم افزار در جدول 5 اقدام می کنیم تا زمانی که همه قابلیت های مورد آزمایش قرار گیرند.

راه اندازی آزمایشی ذخیره سازی داده ها

پس از اینکه تجزیه و تحلیل تمام شبکه تکمیل شد، ما شرح می دهیم در گوشی تجزیه و تحلیل داده های ذخیره سازی شده را. ما استفاده می کنیم از یک میکرو سیستم قفل شکن. XRY برای انجام یک کاربرد منطقی از دستگاه آندروید است. XRY با اجرای قانون، نظامی، و آزمایشگاه های پزشکی قانونی در بیش از 100 کشور برای کمک به تحقیقات پزشکی قانونی دیجیتال مورد اعتماد است. اعتبار و قانونی کردن نتایج ما با استفاده از تناوب رایگان: پشتیبان هلیم برای بازیابی فایل های نرم افزار است. و سپس فایل DB، با استفاده از اندیشه پشتیبان گیری استخراج و پایگاه داده SQLite برای مشاهده محتویات فایل ها می باشد .فایل DB هنگامی که یک ردیابی در فعالیت های واحد برای شواهد پیدا شد نوع آن را ثبت می کند. انواع شواهد ذخیره سازی ما در سیاهه های مربوط به چت و داده مشخصات

کاربر متن در فایل های پایگاه داده بخش بخش شده است. شواهد مستند برای هر نرم افزار در یک فایل DB که شامل چت و / یا اطلاعات کاربران است پیدا می شود.

دستگاه قبل از شروع آزمایش ما، لیست نصب کامل از برنامه های کاربردی پیام های فوری در جدول 5 در هر دو دستگاه تلفن همراه نشان داده شده است. جدول 1 لیستی از تمام نرم افزار و سخت افزار مورد استفاده در طول تحقیقات را نشان می دهد.

نتایج آزمایشی

چهار خروجی از بیست برنامه های کاربردی، یعنی Snapchat ، Tinder ، Wickr و BBM، رمزگذاری ترافیک شبکه خود را با استفاده از رمزگذاری HTTPS با استفاده از certificates و استفاده از SSL قادر به بازسازی هر گونه اطلاعات از این برنامه های کاربردی از طریق تجزیه و تحلیل ترافیک هستند، تجزیه و تحلیل داده های ذخیره سازی شده، ذخیره سازی و سرور تجزیه و تحلیل با توجه به رمزنگاری صورت گرفته است. نتایج کلی در جدول 2 نشان داده شده.

بازرسی بسته با این برنامه رمزگذاری ممکن نبود. با این حال، در طول تحقیقات ما نشان داده ایم که 16 مورد از 20 برنامه ی کاربردی مورد آزمایش ، ترافیک شبکه از تکه تکه کردن و / یا ذخیره سازی داده های رمزگذاری نشده بوده است. عدم رمزنگاری ممکن است با توجه به منابع در دسترس توسعه دهندگان و یا به دلیل شرکت این داده ها به عنوان غیر حریم خصوصی تهاجمی مورد استفاده قرار گیرند. ما فرض می کنیم که سازمان هایی که منابع برای رمز دار کردن ترافیک خود صرف کرده اند. حفره امنیتی / حریم خصوصی دارند.

شرایط خدمات و یا امنیتی / خصوصی سیاستی قبل از انجام مطالعه است. صفحات نرم افزار بر روی فروشگاه Google Play یا امنیتی / خصوصی و یا مرجع امنیتی / خصوصی به عنوان یک ویژگی کلیدی هستند. تنها استثنا Wickr است، که تاکید امنیتی / خصوصی دارد.

هدف ما ذکر این نکته است که مثبت های کاذب زمانی رخ می دهند که تبلیغات و جزییات تصویر پروفایل رمز گشایی شوند ، اما محتوای کاربر رمزگذاری شده است. این موارد به عنوان شواهد مستند نشده هستند. منفی کاذب

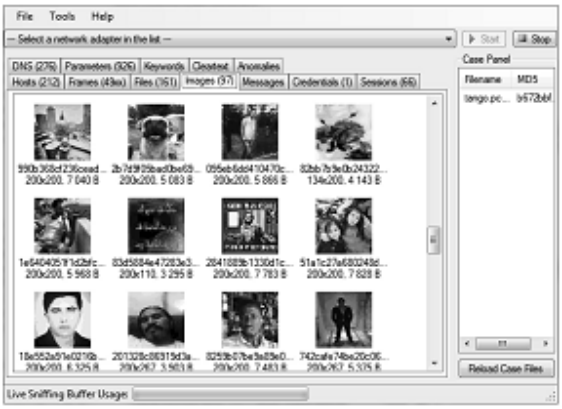
نیز رخ داده است که ما متوجه آثار فعالیت با استفاده از یک ابزار هستیم، اما در دیگری اینگونه نیست. بنابراین، برای بازسازی ترافیک، ما مطمئن هستیم که برای عبور از اعتبار نتایج ما با استفاده از Wireshark، NetworkMiner و NetWitness ایجاد شده است

جدول 1 دستگاه ها و ابزار مورد استفاده برای تست نرم افزار

دستگاه /ابزار	کاربرد	شرکت	نسخه نرم افزار / سیستم عامل
Laptop	ایجاد شبکه مجازی با استفاده از آزمون مینی پورت	Windows	Windows 7 SP2
One M8 (UNHcFREGdroid)	اتصال به شبکه آزمایشی	HTC	Android 4.4.2
IPad 2 (UNHcFREGapple)	اتصال خارجی به شبکه آزمایشی	Apple	iOS 7.1.2
NetworkMinerWireshark	مشاهده زنده ترافیک شبکه	NETRESEC	1.6.1
Wireshark	مشاهده زنده ترافیک شبکه	Wireshark	1.10.8
NetWitness Investigator	تجزیه و تحلیل ترافیک شبکه	EMC	9.7.5.9
XRY	ایجادکننده یانمایشگرتصویر منطقی	Micro Systemation	6.10.1
Helium Backup	ایجاد پشتیبان اندروید	ClockWorkMod	1.1.2.1
Android Backup Extractor	نمایش پشتیبان اندروید	dragomerlion	2014-06-30
SQLite Database Browser	نمایشSQLite/فایل DB	Erpe,tabuleiro,vapour	3.2.0

جدول 2 نرم افزار های تست شده بدون آسیب پذیری

برنامه های کاربردی	قابلیت ها	فعالیت انجام	ترافیک شبکه رمزگذاری شده، ذخیره سازی داده ها و ذخیره سازی سرور	امنیتی تاکید
Tinder	گفتگو متنی	ارسال/دریافت پیام	بله	نه
Wickr	گفتگو متنی اشتراک گذاری تصویر	ارسال / دریافت پیام ارسال/دریافت تصویر	بله	بله
Snapchat	صوتی، تصویری و اشتراک گذاری تصویر	ارسال تصویر ارسال ویدئو دریافت ویدئو	بله	نه
BBM	گفتگو متنی اشتراک گذاری تصویر	ارسال / دریافت پیام ارسال / دریافت تصویر	بله	نه



شکل 2 . گرفتن تصاویر پروفایل از تانگو

گرفتن پیام های متنی

چهار موردی که ما در آن قادر به بازیابی پیام های متنی واقعی که بین دو دستگاه با استفاده از تجزیه و تحلیل ترافیک شبکه رد و بدل شده است هستیم. MessageMe ، MeetMe و ooVoo نشان می دهند هم پیام ئریافتی و

هم ارسالی را ، در حالی که ما تنها قادر به بازیابی متن از Okcupid از پیام های در حال ارسال هستیم (دریافت نکرده).

گرفتن محتوای چند رسانه ای

ما قادر به بازسازی انواع مختلف فایل های رسانه ای از ترافیک شبکه، از جمله تصاویر، فیلم ها، مکان ها، طرح ها و صدا هستیم.

ما بازسازی می کنیم تصاویر را هنگامی که تست می شوند در ، Instagram ، Oovoo، Tango ، Nimbuzz ، MessageMe ، textPlus ، TextMe ، Viber ، HEYWIRE ، Grindr و Facebook Messenger. برنامه های کاربردی نمایش مشخصات عمومی، Oovoo، Tango ، Nimbuzz ، MessageMe، textPlus، TextMe، Viber و HEYWIRE تصاویر را زمان دریافت رمزگذاری نمی کنند در حالی که Grindr موفق به رمز گذاری تصاویر در زمان ارسال می شود.

بعضی از برنامه شامل یکی از ویژگی های طرح ریزی هستند، که در آن می توان یک چیزی بر روی صفحه نمایش رسم و آن را به طرف مقابل ارسال کرد. ما قادر به بازسازی طرح از تمام برنامه های ذکر شده در جدول 5 با ویژگی های طراحی هستیم. علاوه بر این، ما قادر به بازسازی طرح توسط دستگاه از طریق Viber و MessageMe ، و ارسال طرح توسط دستگاه از طریق Kik هستیم.

بسیاری از برنامه های کاربردی به کاربران اجازه می دهند نقشه های گوگل محل سکونت خود را انتقال دهند؛ با این حال، بسیاری این منطقه را از طریق استراق سمع باز سازی نمی کنند. ما قادر به بازسازی تصاویر مکان از TextMe، Viber، و MessageMe هستیم که یک محل را ارسال یا دریافت کنیم. ما قادر به بازسازی تصاویر مکان از WhatsApp، Nimbuzz ، HEYWIRE، می باشیم.

همانطور که در جدول 5 اشاره شد، برنامه های پیام رسانی متعددی توانایی به اشتراک گذاشتن فایل های صوتی و تصویری بین کاربران را دارند. همه 10 برنامه ی کاربردی اجازه می دهد که اشتراک گذاری ویدیو انجام شود ، ما قادر به بازسازی کامل فیلم منتقل شده با Viber ، Tango ، Nimbuzz و MessageMe می باشیم . تمام برنامه های

کاربردی تست شده می توانند ارسال / دریافت و انتقال صدا کنند، ما تنها می توانیم فایل های صوتی که از طریق MessageMe فرستاده شده بازیابی کنیم.

فراتر از محتوای چند رسانه ای ارسال شده در پیام، ما قادر به بازسازی تمام تصاویر تانگو ، و همچنین تصاویر پروفایل دیگر کاربران تانگو هستیم. جالب این که، این تصاویر پروفایل نه تنها مربوط به مخاطبان در گوشی ما است بلکه شامل تصاویر پروفایل کاربران دیگری است که ما قادر به شناسایی ان ها نمی باشیم . که در شکل 2 نشان داده شده.

یو ار ال استفاده شده برای محتوای طرف سرور

در طول تست ترافیک شبکه ، ما فایل های PCAP با استفاده از Wireshark برای بازیابی لینک به سرور برنامه کاربردی استفاده می کنیم. مشخص شده است که این لینک ها هنوز فعال هستند و منجر به ارسال / دریافت رسانه ها در طول می شوند. این بدان معنی است که این برنامه ها بر روی سرور ذخیره سازی و بدون استفاده از احراز هویت کاربر فعالیت می کنند. این به حر جستجوگر اجازه می دهد به لینک های دانلود دسترسی داشته باشد. همه این لینک ها پس از آزمایش ما هنوز فعال بوده اند. جدول 3 برخی از آدرس ها را در ترافیک شبکه Viber ، نمایش مشخصات عمومی، Oovoo ، Tango ، MessageMe ، Grindr، Heywire ، textPlus و Facebook Messenger ، پیدا شده است که در آن نقطه محتوای کاربران ذخیره شده و در سرورهای متعلق به آن برنامه های کاربردی نشان داده شده است.

جدول 3 فایل های رمزگذاری نشده کاربر بر روی سرور نرم افزار

Application	URL for server-side media
Viber	https://s3.amazonaws.com/share2014-04-21/0d1b42b9f6be43c8b83f0ea4b141f8fae4fb5d775093a17c0e06861c6e2e9300.mp4
Instagram	http://photos-e.ak.instagram.com/hphotos-ak-xaf1/10553994_908375655855764_354550189_n.jpg
ooVoo	http://g-ugc.oovoo.com/nemo-ugc/40051d186b955a77_b.jpg
Tango	http://cget.tango.me/contentserver/download/U8gkjgAAvvzybrAuOcfZPw/9b4IqEqk
MessageMe	http://watercooler.msgme.im/u/107917517644387942 4/m/p3joe2.mp4
Grindr	http://cdns.grindr.com/grindr/chat/aa0e6063299350a9b80278feb56a8606acae1267
HeyWire	http://mms.heywire.com/cs/GetImage.aspx?c=p-&p=0%2fmms1%2f20140725%2fp-ec2f5715-afeb-4db4-a5c0-8aaf8ac80689.jpeg
TextPlus	https://d17ogcqyct0vcy.cloudfront.net/377/549/1Kw7ihM5Rl1OkDoXWa.jpg
Facebook Messenger	http://scontent-lga.xx.fbcdn.net/hphotos-xpf1/v/t34.0-12/11156748_10152706456535706_749142264_n.jpg?oh=efbf52c9c9f74525ced5d3d17642ae69&oe=553AE540

جدول 5 قابلیت های نرم افزار، اعمال و آثار

برنامه های کاربردی	قابلیت ها	فعالیت قابل انجام	آثار ترافیک شبکه	آثار ذخیره سازی داده ها	آثار سرور
WhatsApp (2.11)	گفتگوی متنی، صوتی، تصویری، محل، و به اشتراک گذاری V-card	ارسال / دریافت پیام ارسال / دریافت صدا ارسال / دریافت تصویر ارسال ویدیو ارسال V-card ارسال / دریافت موقعیت GPS	موقعیت V-card (ارسال)		
Viber (4.3.0.712)	گفتگوی متنی تماس صوتی ، تصویری، طرح، و به اشتراک گذاری مکان	ارسال / دریافت پیام ارسال / دریافت طرح ارسال / دریافت تصویر ارسال / دریافت صدا دریافت تماس صوتی ارسال / دریافت موقعیت GPS	تصاویر (دریافت شده) طرح (دریافت شده) ویدئو (دریافت شده) موقعیت(ارسال/دریافت)		تصاویر، ویدئو، طرح
Instagram (6.3.1)	گفتگوی متنی ویدئو و به اشتراک گذاری تصویر	ارسال / دریافت تصویر	تصویر(ارسال/ دریافت)		تصاویر
Okcupid (3.4.6)	گفتگوی متنی	ارسال / دریافت پیام ارسال / دریافت تصویر	متن (ارسال)		

ooVoo (2.2.1)	گفتگوی متنی تماس صوتی تماس تصویری	ارسال / دریافت پیام ارسال / دریافت تصویر	متن (ارسال/ دریافت) تصاویر(ارسال/ دریافت)	ورود به گفتگو	تصاویر
Tango (3.8.95706)	گفتگوی متنی تماس صوتی تماس تصویری به اشتراک گذاری تصویر	ارسال / دریافت پیام ارسال / دریافت تصویر	تصاویر(ارسال/ دریافت)		ویدئو
Kik (7.3.0)	گفتگوی متنی فیلم، تصویر و به اشتراک گذاری طرح	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت طرح	طرح (ارسال)	ورود به گفتگو	
Nimbuzz(3.1.1)	گفتگوی متنی تماس صوتی ، تصویری ، و اشتراک محل	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت GPS محل سکونت ارسال / دریافت ویدئو	موقعیت (ارسال) تصاویر(ارسال/ دریافت) ویدئو (فرستاده)	متن ساده کلمه عبور گفتگو	
MeetMe (8.6.1)	گفتگوی متنی اشتراک گذاری تصویر	ارسال / دریافت پیام ارسال / دریافت تصویر	متن (ارسال/ دریافت)	ورود به گفتگو	
MessageMe (1.7.3)	گفتگوی متنی تماس صوتی ، تصویری،	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت طرح	موقعیت (ارسال/دریافت) متن (ارسال / دریافت)		ویدئو

	طرح، و به اشتراک گذاری مکان	ارسال / دریافت GPSموقعیت ارسال / دریافت ویدئو ارسال / دریافت موسیقی	تصاویر (ارسال / دریافت) طرح (دریافت شده) موسیقی (ارسال)		
TextMe (2.5.2)	گفتگوی متنی تماس صوتی تماس تصویری ویدئو و به اشتراک گذاری تصویر	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال فایل در Dropbox دریافت ویدئو	موقعیت(ارسال/دریافت) تصاویر (دریافت شده)	متن ساده کلمه عبور ورود به گفتگو	
Grindr (2.1.1)	گفتگوی متنی تصویر و اشتراک گذاری موقعیت	ارسال / دریافت پیام ارسال / دریافت تصویر	تصاویر (ارسال)		تصاویر
HeyWire (4.5.10)	گفتگوی متنی تماس صوتی، تصویر، و به اشتراک گذاری موقعیت	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت موقعیت	موقعیت(ارسال) تصاویر (دریافت)	ورود به گفتگو	تصاویر
Hike (3.1.0)	گفتگوی متنی تماس صوتی محل، و به اشتراک	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت موقعیت	موقعیت(ارسال)	ورود به گفتگو	

	گذاری V-card				
textPlus (5.9.8)	گفتگوی متنی تماس صوتی اشتراک گذاری صدا و تصویر	ارسال / دریافت پیام ارسال / دریافت تصویر	تصویر(ارسال/دریافت)	برنامه استفاده شده تصاویر، ورود به گفتگو	
Facebook Messenger (25.0.0.17.14)	گفتگوی متنی تماس صوتی ، تصویری ، موقعیت ، و برچسب	ارسال / دریافت پیام ارسال / دریافت تصویر ارسال / دریافت ویدئو ارسال / دریافت صدا ارسال/دریافت GPS موقعیت ارسال / دریافت برچسب	تصاویر(ارسال/ دریافت) ریز عکس ها به ویدئو (دریافت)		تصاویر، ویدئو ریز عکس ها

تحقیقاتی از این قبیل برای تشویق توسعه دهنده ها و کاربران برای توجه بیشتر در مورد امینت و حریم خصوصی مهم است. طیفی از برنامه های تست شده توسط ما قادر به رمزگشایی داده های آن ها به یک روش یا روش دیگر نبودند.

مطالعات آینده

هنوز هم این زمینه نیاز به کار دارد. این برنامه ها به صورت مدام تغییر می کنند، ویژگی های امنیت و به روز رسانی به آن اضافه شده است.

یک نمونه از این بروزرسانی جدید در نرم افزار فیس بوک مسنجر است. برنامه های کاربردی، چه در فیس بوک مسنجر یا نه، می نواند داده های متفاوت بسته به تنظیمات کاربر داشته باشد، نسخه سیستم عامل، و تولید کننده ذخیره می شود. بنابراین، تست مداوم نیاز به در نسخه های جدید از این برنامه ها انجام شود / OSS به عنوان آن ها منتشر می

شوند تا تعیین کند چه چیزی تغییر کرده است و چه مقدار از دانش قبلی از این برنامه های کاربردی هنوز صادق است.

برسی هر نسخه از نرم افزار برای مصنوعات دیجیتال پزشکی قانونی در شیوه ی این پژوهش به مدت طولانی انجام شده است. به همین دلیل است که در آینده انیاز به تست یک فرایند نیست. گروه تحقیقاتی ما، در یک پروژه به تجزیه و تحلیل فعالیت های برنامه های نصب شده بر روی یک دستگاه برای تعیین رمزگذاری شبکه ترافیک و خدمات برنامه های کاربردی در برقراری ارتباط با (بخش "Datapp" را ببینید)

20 برنامه ی کاربردی انتخاب شده تنها برنامه های پیام رسانی در بازار آندروید نیستند، و به وضوح مقدار زیادی از دامنه برای آزمایش مشابه در دیگر برنامه های پیام رسان انجام شوده وجود دارد. همانطور که قبلا اشاره شد، بسیاری از برنامه های رسانه های اجتماعی مانند فیس بوک، سیستم های خود را، که نیاز به تجزیه و تحلیل ترافیک شبکه دارند. علاوه بر این، برنامه های می تواند ذخیره و ارسال داده های امن بر روی یک سیستم عامل را ممکن کنند ، بنابراین نیاز نیست آزمایش در سراسر سیستم عامل های مختلف انجام شود.

برنامه داده

تلاش بسیار کمی برای بازسازی شواهد دیجیتال مورد بحث مورد نیاز است؛ ابزار ما روند خودکار دارند. نتایج ما را می توان با ابزار رایگان ، توسط هر کسی با یک لپ تاپ و دو دستگاه های دیجیتال کوچک به دست آورد. پس از آن تحقیقات ما کامل می شود، ما ابزار خود را به نام " برنامه داده" میشناسیم و به طور خودکار بیشتر این روند برای هر کسی و برای انجام امنیت نرم افزار و تست حریم خصوصی توسعه یافته است. برنامه دادهاهرم پروژه های منبع باز مانند NetworkMiner است. ابزار به طور خودکار ایجاد یک شبکه بی سیم می کنند. این ابزار بیشتر برای عوام ایجاد شده بود، به طوری که در آینده آن ها می توانند برنامه های کاربردی خود را تست کنند. برنامه داده برای دانلود از وب سایت (www.unhcfreg.com) تحت داده ها و ابزارهای در دسترس است.

نتیجه

در این مقاله، ما 20 برنامه ی کاربردی آندروید از طریق تجزیه و تحلیل ترافیک شبکه و تجزیه و تحلیل ذخیره سازی سرور / دستگاه بررسی شده است. Thiswas به منظور بررسی شواهد دیجیتال است که می تواند از ارزش به بازرسان پزشکی قانونی و همچنین برای ارزیابی امنیت نرم افزار در ارسال / دریافت اطلاعات و حریم خصوصی نرم افزار در ذخیره سازی داده ها انجام می شود. کار ما نتایج مختلف را نشان داده است .

ما قادر به بازیابی اطلاعات دیگر مربوط به کاربر از Snapchat، Tinder ، Wickr یا BBM هستیم. در 16 برنامه های باقی مانده، ما قادریم که حداقل برخی از شواهد داده های رمزگذاری نشده ، ارسال شده و / یا بازیابی شده توسط دستگاه مان را بازسازی کنیم.