

بررسی الزامات استنادپذیری ادله دیجیتال استخراجی از دستگاه های تلفن همراه

حسین سهلانی^{1*}

تاریخ دریافت: 1401/08/18

تاریخ پذیرش: 1401/10/28

چکیده

امروزه گوشی‌های تلفن همراه به یک پدیده‌ی جهانی تبدیل شده‌اند و جامعه مجازی با صدها میلیون کاربر را پدید آورده‌اند. امکانات و برنامه‌های مختلف سبب تمایل به استفاده از این تجهیزات بیش از گذشته گردیده و متقابلاً جرائم مربوط به این حوزه هم با افزایش چشمگیری روبرو بوده طوریکه تقریباً در تمام پرونده‌ها آثاری از این گوشی‌ها دیده می‌شود، لذا در راستای استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های تلفن همراه جهت کشف آثار جرائم الزاماتی مطرح می‌گردد که سبب استانداردسازی روال استخراج ادله و آینده‌نگری جهت دستیابی به این الزامات می‌گردد. ارائه راهبردهای آینده‌نگر در حوزه استنادپذیری، مستلزم شناخت هر چه بیشتر این علم و اولویت‌دهی آن‌ها می‌باشد که هدف این تحقیق ارائه چارچوبی است که بتواند در وهله اول این الزامات را مدون، شناسایی، تبیین و اولویت‌دهی کند و سپس راهکارهایی را برای آینده‌نگری این الزامات ارائه دهد. برای دستیابی به این الزامات با تعدادی از خبرگان مراکز علمی و اجرایی با تحصیلات حداقل کارشناسی و چندین سال فعالیت مرتبط با این حوزه مصاحبه صورت گرفت که پس از انجام مصاحبه‌ها، اشباع نظری حاصل شد. روش پژوهش این تحقیق، به صورت ترکیبی، کمی و کیفی بوده که داده‌های این پژوهش از مطالعات کارهای پیشین، تجربه کاری مؤلفین و همچنین از طریق مصاحبه عمیق با 12 نفر از خبرگان اصلی در مرحله کیفی و 20 نفر از خبرگان میانی در مرحله کمی حاصل گردید، به طوریکه با جمع‌آوری و کدگذاری اطلاعات در جهت شناسایی الزامات استنادپذیری ادله استخراجی به ارائه یک چارچوب مفهومی برای این الزامات پرداخته شد که مؤلفین توانستند یک چارچوب کاربردی در هشت‌جُذ اصلی شاخص‌های مربوط به حین استخراج ادله، بررسی بدافزارها، مجوزهای دسترسی به گوشی، برنامه‌های داخل گوشی، سخت‌افزار دستگاه همراه، چگونگی استخراج، محتوای ادله استخراج‌شده و آموزش افراد با 66 مؤلفه ارائه کنند که بر اساس یافته‌های پژوهش، مهم‌ترین الزام، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی با بار عاملی 88.60% شناسایی شد که در نهایت با توجه به وضعیت موجود سازمان‌های مسئول در حوزه استنادپذیری ادله دیجیتال برای دستیابی به الزامات اکتساب شده پیشنهادهایی در مقاله اعلام گردید.

واژگان کلیدی: ادله دیجیتال، موبایل فارتزیک، الزامات استنادپذیری، استنادپذیری ادله، ابزارهای فارتزیک.

¹ دانشگاه علوم انتظامی امین، (نویسنده مسئول)، sahlani_h@yahoo.com

۱- مقدمه و بیان مسئله

در دستگاه ذخیره می‌شود و برای ارائه در دادگاه مفید است، کشف و استخراج کنند.

در تحقیق پیش رو، مؤلفین بر روی الزامات استنادپذیری ادله دیجیتال استخراجی از گوشی‌های تلفن همراه و جستجوی مصنوعات تولیدشده و ذخیره‌شده در قسمت‌های مختلف گوشی، از طریق ابزارهای مربوطه تمرکز دارند. چنین یافته‌های مصنوعی می‌توانند عامل را با جرم رخ داده مرتبط کنند؛ بنابراین، بررسی دقیق و مستدل این برنامه‌ها می‌تواند اطلاعات مفیدی را در اختیار محققین و کارشناسان بررسی استنادپذیری ادله دیجیتالی استخراجی از گوشی قرار دهد. در ادامه این مقاله سعی شده با مطالبی در رابطه اهمیت بررسی استنادپذیری ادله استخراجی از گوشی‌های تلفن همراه و اقدامات محققین پیشین در این زمینه بیان شود سپس به بررسی چالش‌ها و الزامات مربوط به این موضوع از طریق مصاحبه با خبرگان و کارشناسان این امر پرداخته شود که نتیجه این بررسی‌ها منجر به ایجاد چارچوبی برای شناسایی الزامات استنادپذیری خواهد شد سپس در چارچوب ایجاد شده میزان اهمیت هر یک از مولفه‌ها بدست می‌آید و نهایتاً راهکارهایی برای دستیابی به الزامات مطرح شده بیان می‌شود.

بررسی الزامات استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های تلفن همراه یک فرصت ساختاریافته برای استاندارد سازی و بهینه سازی اقدامات مربوط به استخراج ادله مستدل ایجاد می‌کند که با توجه به رویکرد رو به جلو و نگاه به آینده در بررسی مؤلفه‌های تأثیرگذار در استنادپذیری می‌توان زمینه و بستر مناسبی را جهت سیاست گذاری و تصمیم‌گیری‌های بلندمدت در زمینه دستیابی به این الزامات و تسهیل سازی فرآیند استنادپذیری ادله دیجیتالی فراهم آورد لذا می‌توان عنوان کرد این مهمترین دلیل بر اهمیت بسیار زیاد این علم نوظهور می‌باشد. علاوه بر این، می‌توان با مشخص کردن میزان اهمیت

گوشی‌های هوشمند طی دو دهه گذشته پیشرفت‌های فزاینده‌ایی را پشت سر گذاشته‌اند و از آنجاکه یک دارایی باارزش محسوب شده و بیشتر برای تماس‌ها و پیام‌ها استفاده می‌شوند، به یک نیاز واقعی در زندگی انسان تبدیل شده‌اند. گوشی‌های هوشمند به کاربران این امکان را می‌دهند که با ارسال ایمیل و اتصال از طریق برنامه‌های مختلف رسلنه‌های اجتماعی، با دیگران ارتباط برقرار کرده و دسترسی راحت تری به اطلاعات و اخبار داشته باشند. در این سال‌ها استفاده از اپلیکیشن‌های رسانه‌های اجتماعی افزایش چشمگیری داشته طوریکه افراد در هر گروه سنی، مشاغل، دانشگاه‌ها، رسانه‌ها، سازمان‌های مجری قانون (LEA)¹ و حتی سازمان‌های تروریستی برای اهداف مختلف از آن‌ها استفاده می‌کنند. استفاده از رسلنه‌های اجتماعی به‌طور مداوم در حال افزایش است و این افزایش به دلیل برنامه‌های گوشی‌های هوشمند می‌باشد [1].

برنامه‌های شبکه‌های اجتماعی (SNA)² به کاربران اجازه می‌دهند یک نمایه ایجاد کنند، اطلاعات شخصی مانند تصاویر، ویدیوها و اطلاعات مکانی را بارگزاری کنند و آن اطلاعات را از طریق پیام‌های خصوصی یا پست‌های عمومی به اشتراک گذارند. این پدیده به مجرمان فرصتی داده تا از طریق اطلاعات شخصی کاربر، وی را تحت تأثیر قرار دهند و در نتیجه جرائم سایبری از طریق SNAها ایجاد کنند. این برنامه‌ها همچنین می‌توانند برای زورگیری سایبری³، تعقیب⁴، آزار جنسی⁵، کلاهبرداری سایبری⁶ و توهین⁷ مورد سوءاستفاده قرار گیرند [2]. از آنجا که بسیاری از اطلاعات مربوط به فعالیت‌های کاربر در حافظه داخلی گوشی ذخیره می‌شود، این گوشی‌های هوشمند به منبع مهمی از شواهد و مصنوعات برای بررسی اطلاعات جرم مرتبط با این SNAها تبدیل شده‌اند. این مصنوعات جمع‌آوری شده کاربران و محققان را قادر می‌سازد تا PII⁸ (اطلاعات قابل شناسایی شخصی) را که

⁵ Sexual harassment

⁶ Cyber scam

⁷ Insults

⁸ Personally identifiable information

¹ Law enforcement agencies

² Social networking apps

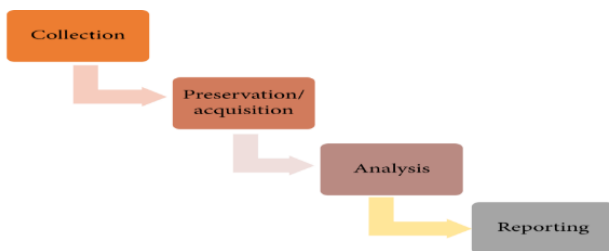
³ Cyber bullying

⁴ Stalking

2-2 - فرایند استخراج ادله دیجیتال استنادپذیر

از گوشی های تلفن همراه

مراحل استنادپذیری ادله دیجیتال برای جرائم و شواهد مختلف متفاوت می باشد ولی به صورت کلی می توان در 4 مرحله کلی بیان کرد: جمع آوری، استخراج، تجزیه و تحلیل و گزارش که در شکل 1 نیز نشان داده شده است (موسسه ملی استاندارد و فناوری (NIST) [5].



شکل 1) فرآیند تجزیه و تحلیل فارتزیک بر مبنای NIST [5]

مراحل مربوط به استخراج و آنالیز اطلاعات مهم ترین و موثرترین مرحله در فرایند استنادپذیری می باشد که روش های استخراج محتویات گوشی ها عبارتند از: روش دستی³، منطقی⁴، فایل سیستم⁵، فیزیکی⁶، مبتنی بر تراشه⁷.

استخراج به روش دستی: روش استخراج دستی شامل مشاهده و ضبط محتوای داده ذخیره شده در یک گوشی هوشمند می باشد. این روش در دسترس ترین حالت ممکن بوده ولی فرایند زمان بری است و نمی تواند اطلاعات حذف شده را بازیابی کند اما می تواند رکوردی از صفحه های مختلف و رابط کاربری ارائه دهد [4].

استخراج به روش منطقی: اکتساب های منطقی گوشی تلفن همراه شامل استخراج تمام داده هایی است که دستگاه قادر به دسترسی به آن در سیستم ذخیره سازی خود دارد. این روش قابلیت استخراج و تجزیه و تحلیل داده ها در حالت قفل نیز داشته و بر اساس اصل به دست آوردن کپی بیت به بیت از فضاهای اختصاص یافته کار

هر یک مولفه های الزامات استنادپذیری ادله دیجیتال آماده سازی سازمان ها و جامعه را بر اساس اولویت دهی های از قبل مشخص شده معین کرد تا با تصمیم گیری های کوتاه مدت و اقدامات جهادی، درک زود هنگام خطرات و هشدارها؛ برنامه ریزی و سرمایه گذاری برای به دست آوردن منافع موجود و ... بتوان به بهترین نتیجه قابل تصور دست یافت.

ضرورت پاسخ به مطالبات مردم به ویژه در حوزه جرائم سایبری رو به رشد در گوشی های تلفن همراه و به طبع آن استنادپذیری ادله دیجیتالی استخراجی از گوشی های تلفن همراه در مراکز قضایی و انتظامی و شرکت های شاغل در این حوزه را اجتناب ناپذیر می کند. علاوه بر این برنامه ریزی، استاندارد سازی و بهینه سازی اقدامات مربوط به استنادپذیری ادله استخراجی ضرورت توجه به این امر را اجتناب ناپذیر می کند.

۲- مبانی نظری

استنادپذیری ادله دیجیتالی استخراجی از شواهد مفهوم نسبتاً جدیدی است که برخی عبارات و مفاهیم را در خود جای داده که در ادامه بیان می شود.

1-2 - فارتزیک و دیجیتال فارتزیک¹

فارتزیک در لغت به معنای پزشکی قانونی بوده اما مفهوم آن به جرم شناسی اشاره دارد و دیجیتال فارتزیک در اصطلاح به کلیه اقداماتی گفته می شود که بر روی تجهیزات الکترونیکی و دیجیتالی انجام تا از طریق آن شواهد مجرمانه استخراج گردد یا در مواردی به استنادپذیری ادله دیجیتال استخراجی معنی شده که در این مقاله هم با همین عنوان بیان شده است [3].

⁵ filesystem

⁶ physical

⁷ Chip off-based

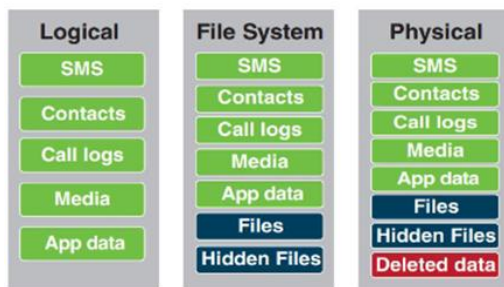
¹ Digital Forensic

² National Institute of Standards and Technology

³ manual

⁴ logical

در عین حال زمان‌برترین روش‌ها می‌باشند. در شکل (2) تفاوت و شباهت نتایج روش‌های مختلف نشان داده شده است [8].



شکل (2) تفاوت نتایج روش‌های استخراج [8]

۳- پیشینه تحقیق

بررسی تحقیقات انجام شده توسط محققان قبلی نشان می‌دهد که در حوزه به استنادپذیری ادله دیجیتال استخراجی مطالعات پراکنده‌ای انجام شده است؛ لذا در رابطه با موضوع این پژوهش، برای بالا بردن منابع تحقیقاتی، علاوه بر تحقیقات قبلی صورت گرفته در حوزه استنادپذیری ادله دیجیتال استخراجی در مجلات، پایگاه‌های علمی و سایر تحقیقات صورت گرفته در دانشگاه‌ها و مراکز علمی به مصاحبه با خبرگان و کارشناسانی که در این حوزه کارهای عملی انجام داده‌اند نیز پرداخته می‌شود. با این وجود در ادامه کارهای قبلی صورت با رویکرد بیان الزامات استنادپذیری در چندین دسته تقسیم بندی و بیان شده است.

1-3- چالش‌های موجود در استنادپذیری ادله

استخراجی

مؤلفین در مقاله [9] به آینده پژوهی استنادپذیری ادله دیجیتال جرائم سایبری مبتنی بر اینترنت اشیا پرداخته‌اند که در آن چارچوب اصلی کار خود را در چهارچوب اصلی استنادپذیری جرائم سایبری مرتبط با اینترنت اشیا، آینده پژوهی جرائم اینترنت اشیا، محدودیت‌ها و نواقص و ناامنی‌ها با 10 مؤلفه و 36 زیر مؤلفه ارائه کردند که بر اساس یافته‌های پژوهش، برای فائق آمدن بر چالش‌های اکتساب شده پیشنهادات ذیل را عنوان کردند؛ اتخاذ زود هنگام تدابیر لازم و تجهیز مراکز قضایی، انتظامی و آموزشی برای شناسایی چالش‌ها و اقدامات صورت گرفته در سایر مراکز علمی، بالا بردن بنیه علمی مراکز قضایی و انتظامی در حوزه کشف جرائم با رویکرد آینده پژوهی با برگزاری مانورهای

می‌کند و نمی‌تواند داده‌ها را از فضاهای شل بازیابی کنند لذا نمی‌توانند داده‌های حذف شده را به دست آورند [6].

استخراج به روش فایل سیستم: استخراج به روش فایل سیستم به بررسی عمیق ساختار فایل می‌پردازد و بیشتر زمانی مورد استفاده قرار می‌گیرد که کاربر قصد دارد با استفاده از API های مرتبط، به فایل خاصی در حافظه داخلی گوشی دسترسی پیدا کند. این روش استخراج معمولاً به‌عنوان ابزار اصلی استنادپذیری ادله استخراجی در بازیابی فایل‌های داده از حافظه داخلی مانند فایل‌های پایگاه‌داده، بررسی تاریخچه مرورگر وب، استفاده از برنامه و ... استفاده می‌شود [7].

استخراج به روش فیزیکی: اکتساب فیزیکی شامل کپی بیت به بیت از کل فضای ذخیره‌سازی فیزیکی است و برای بازیابی اطلاعات حذف شده موثر بوده و برای کنترل کامل نیاز به دسترسی روت داشته که دستیابی به دسترسی روت باعث تغییراتی در داده‌های دستگاه می‌شود و نیاز به سخت‌افزار و نرم‌افزار تخصصی برای این منظور می‌باشد [8]. در صورت روت بودن گوشی، دسترسی‌های لازم به ابزارهای استنادپذیری جهت استخراج بیشتر اطلاعات و بازیابی محتویات پاک‌شده و ... داده می‌شود.

استخراج بر پایه تراشه: این روش شامل برداشتن فیزیکی تراشه حافظه فلش از گوشی تلفن هوشمند و آماده‌سازی آن برای دستیابی به داده‌های خام موجود در تراشه با استفاده از تراشه خوان می‌باشد. این روش امکان ایجاد یک تصویر باینری از تراشه حافظه را برای بررسی کنندگان فراهم می‌آورد. ریسک استفاده از این روش بالا بوده و ممکن است دستگاه تلفن هوشمند دیگر قابل استفاده نباشد [5].

در مطالعات صورت گرفته، نویسندگان روش‌های مختلفی از جمع‌آوری داده‌های دخیل در فارتزیک تلفن همراه را ارائه کرده‌اند. با توجه به این مطالعات، مشخص شده است که اگر داده‌ها برای تجزیه و تحلیل سریع نیاز به بازیابی داشته باشند، تکنیک اکتساب دستی یا منطقی مناسب است. با این حال، در صورت نیاز به تجزیه و تحلیل دقیق و در مورد تلفن‌های آسیب‌دیده، تکنیک‌های فیزیکی یا مبتنی بر تراشه مناسب‌ترین و

- فارنزیك گوشی های موبایل با نسخه های سیستم عامل اندروید هشت و پایین تر (صرف نظر از نوع رمزنگاری واتساپ)
- فارنزیك گوشی های موبایل با نسخه های سیستم عامل اندروید 9 و بالاتر

جدول 1) نتایج عملکرد فارنزیك واتساپ توسط ابزارهای فارنزیکی [10]

مدل	اندروید	روش رمزنگاری	ufed logical	Ufed file system	Ufed physical	Axiom	Oxygen	DB extract
Galaxy s7	6	8	✓	✓	✓	✓	✓	✓
Htc one M9	6	8	✓	✓	✗	✓	✓	✓
Galaxy A5	7	12	✓	✓	✗	✓	✓	✓
Galaxy s4	7	8	✓	✓	✓	✓	✓	✓
Samsung A720	8	14	✓	✓	✓	✗	✓	✓
sm-G610	8	14	✗	✗	✗	✗	✗	✓
Galaxy note 8	8	14	✓	✓	✗	✓	✓	✓
Galaxy tab s2	8	12	✓	✓	✗	✓	✓	✗
Htc 10	8	12	✓	✓	✗	✓	✓	✓
Huaweinexus6p	8	14	✓	✓	✗	✓	✓	✗
RedmiNote8Pro	9	14	✗	✗	✗	✗	✗	✗
Redmi Note 10	10	14	✗	✗	✗	✗	✗	✗
Poco M3	10	14	✗	✗	✗	✗	✗	✗
Samsung s20	11	14	✗	✗	✗	✗	✗	✗

۲- نقش نوع رمزنگاری پایگاه داده در فارنزیك واتساپ

در بررسی های به عمل آمده مشخص گردید نسخه های رمزگذاری شده واتساپ تا نسخه crypt12، قابلیت استخراج کلید در گوشی های روت شده و غیر روت شده را داشته اما در مدل های crypt14 و با نسخه سیستم عامل اندروید 9 و بالاتر رمزگشایی پایگاه داده تقریباً مقدور نمی باشد.

۳- نقش روت بودن موبایل در نتیجه فارنزیك واتساپ

همان طور که از نتایج حاصل از آزمون ها به دست آمد، بیشترین اطلاعات استخراجی مربوط به گوشی های روت شده بود چراکه علاوه بر بازیابی و استخراج کلیه لاگ های واتساپ، استخراج کلید رمزگشایی و پایگاه داده واتساپ نیز در این مدل گوشی ها به نسبت گوشی های غیر روت محتمل تر می باشد.

۴- نقش فعال بودن پشتیبان گیری پایگاه داده واتساپ

پشتیبان گیری از پایگاه داده های واتساپ با توجه به پیشنهاد این برنامه می تواند در رمزگشایی و دستیابی به محتویات آنها نقش به سزایی داشته باشد.

اجرایی و ارزیابی اقدامات صورت گرفته، عقد قراردادهای بین المللی چند جانبه برای ارائه خدمات زیرساختی و جو بلدهی به استعلامات و درخواست ها، آماده سازی و فراهم آوردن زیرساخت های لازم همچون تغییر آدرس دهی از نسخه 4 به نسخه 6، الزام ارائه دهندگان خدمات اینترنت اشیا به رعایت استانداردها و لزوم آینده پژوهی برای کشف نظام مند فرصتها و چالش های حال و آینده در حوزه اینترنت اشیا. با توجه به اقدامات صورت گرفته در این مقاله [9] محققین مقله پیش رو مصاحبه های خود را با طرح سوالاتی در این زمینه شروع کردند و با تکمیل نظرات خبرگان و مطالعات بعدی بر غنای کار افزودند.

2-3 - چالش های موجود در استنادپذیری ادله

استخراجی از برنامه های گوشی های تلفن همراه

مظاهری در پایان نامه خود [10] برای بررسی چالش های حوزه استنادپذیری ادله استخراجی از برنامه واتساپ گوشی های تلفن همراه آزمایشات مختلفی را بر روی 34 دستگاه گوشی تلفن همراه با نسخه های سیستم عامل متفاوت در حالات روت و غیر روت شده و نیز استفاده از برنامه های مختلف واتساپ با نسخه های متفاوت و روش های رمزنگاری مختلف به عمل آورد که در این بین از ابزارهای استنادپذیری ادله دیجیتال مطرح در این حوزه مانند Axiom، oxygen، ufed cellebrite و ابزارهای بررسی استنادپذیری ادله استخراجی از برنامه واتساپ نظیر sqlite، whatsapp viewer، whatsapp key/DB extractor جهت بررسی و مقایسه استفاده کرده است که در جدول (1) قسمتی از نتایج حاصل از تحقیقات ایشان بیان شده است.

همان طور که در جدول (1) مشاهده می شود می توان نتایج اقدامات حاصله را در 4 دسته زیر تقسیم بندی کرد:

۱- نقش نسخه های اندروید در فارنزیك واتساپ

بر اساس نتایج حاصل از آزمون های صورت گرفته می توان استنادپذیری ادله استخراجی از برنامه پیام رسان واتساپ را بر اساس تأثیر نسخه اندروید به دو دسته تقسیم نمود:

۴- روش شناسی تحقیق

برای انجام این تحقیق هم از مطالعات کمی و هم از مطالعات کیفی به عنوان منبع داده استفاده شد. در این مرحله به بررسی ایده‌ها، رویکردها، نتایج و یافته‌های پژوهش‌های کیفی و کمی پیشین با هدف طراحی و توسعه چارچوب مفهومی الزامات استنادپذیری ادله دیجیتال استحضاری از گوشی‌های تلفن همراه پرداخته شده است و با برخورداری از نتایج یافته‌ها، می‌توان با اتخاذ تصمیمات درست و بهنگام، جهت حل مسائل و مشکلات استنادپذیری

ادله دیجیتال در مواجهه با تهدیدات آینده تصمیمات و رویکردهای مناسبی اتخاذ کرد لذا با توجه به اینکه هدف صرفاً بیان نظریه تئوری نمی‌باشد، نوع تحقیق کاربردی و روش آن توصیفی و از نوع پیمایشی می‌باشد و به صورت ترکیبی در دو بخش کیفی و کمی و در سه گام انجام می‌شود که در شکل (3) به صورت مرحله به مرحله نمایش داده شده است.

مرحله اول: ایجاد مدل اولیه تحقیق جهت شناسایی الزامات استنادپذیری دستگاه‌های همراه

گام اول: بررسی پیشینه و سوابق
گام دوم: بررسی مفاهیم و مبانی نظری
گام سوم: مصاحبه با خبرگان (شناسایی خبرگان امنیتی و دانشگاهی به روش هدفمند گلوله برفی (12 نفر)؛

مرحله دوم: تعیین مدل نهایی الزامات استنادپذیری دستگاه‌های همراه، به کارگیری و پیاده سازی آنها

گام اول: تدوین پرسشنامه مبتنی بر الزامات شناسایی شده در مرحله قبل؛
گام دوم: شناسایی خبرگان میانی امنیتی و دانشگاهی (20 نفر)؛
(جامعه آماری این گام تحقیق را حدود 25 نفر از خبرگان، مدیران و کارشناسان آشنا به موضوع تشکیل می‌دادند که با روش هدفمند گلوله برفی، اعضای نمونه انتخاب شدند)؛
گام سوم: توزیع پرسشنامه و جمع آوری آن (تکمیل پرسشنامه در جلسات مشترک با حضور خبرگان).
گام چهارم: تحلیل داده‌های پرسشنامه و بررسی اهمیت هر یک از چالش‌های استخراج شده؛

مرحله سوم: تعیین اهمیت الزامات عنوان شده

گام اول: شناسایی اهمیت الزامات تعیین شده در مرحله دوم و تحلیل آنها
گام دوم: ارائه راهکارهایی برای دستیابی به الزامات شناسایی شده.

شکل 3: فرایند تدوین الگوی مفهومی

و قابلیت اعتماد مصاحبه‌ها نیز توسط روش بازنگری متخصص بررسی و مورد تأیید قرار گرفت و یک چارچوب مفهومی اولیه از این یافته‌ها بدست آمد که در شکل (4) به نمایش گذاشته شده است.

در گام اول این تحقیق ابتدا به طور کیفی با روش مرور جامع به بررسی کلیه مقالات و مطالعات موجود و سوابق و اسناد و مدارک مرتبط و مصاحبه با خبرگان و افراد کلیدی در خصوص موضوع مولفه‌ها پرداخته شد و از روش مصاحبه نیمه ساختاریافته جهت گردآوری اطلاعات استفاده

۵- یافته های تحقیق و تجزیه و تحلیل آنها

1-5 - تشریح پرسشنامه

بر اساس مطالعات کیفی انجام شده و بررسی مقالات و مطالعات موجود و سوابق و اسناد و مدارک نسبتاً مرتبط و مصاحبه با خبرگان، پس از تکمیل و تحلیل فرمهای مصاحبه، ویژگی های متناسب با الزامات استنادپذیری ادله دیجیتال استخراجی از دستگاه های تلفن همراه شناسایی و گروه بندی گردیدند و سپس در هفت بُعد شاخص های مرتبط با بررسی بدافزارها، شاخص های مرتبط با آموزش افراد، شاخص های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت افزاری دستگاه همراه، شاخص های مربوط به چگونگی استخراج و شاخص های مربوط به استخراج ادله قرار گرفتند (الگوی مفهومی پیشنهادی اولیه، نشان داده شده در شکل 4).

همان گونه که قبلاً نیز بیان گردید، در مرحله دوم الگوی اولیه تکمیل و به عنوان پرسشنامه در اختیار خبرگان میانی قرار گرفت. پرسشنامه مورد استفاده شامل دو قسمت بوده که قسمت اول مربوط به سئوالات جمعیت شناختی خبرگان و قسمت دوم مربوط به سئوالات تحقیق می باشد که در ادامه هر یک تشریح می گردد.



شکل 4. چارچوب مفهومی اولیه: دسته بندی مولفه های موثر در بررسی الزامات استنادپذیری ادله استخراجی از گوشی های تلفن همراه

در گام دوم تحقیق، با توجه به این که نظریه یا پژوهش های پیشین در رابطه با موضوع مورد بررسی بسیار ناقص بودند لذا محققین از روش کیفی با رویکرد نظرات خبرگان، متکی بر پژوهش های پیشین بهره جستند. هدف از این کار معتبر ساختن و گسترش دادن چارچوب مفهومی مرحله قبلی بود. در این مرحله چارچوب مفهومی برآمده از مرحله اول، با استفاده از روش تحقیق کیفی و کمی و از طریق مصاحبه با خبرگان ارشد غنی تر گشت و برخی از اشکالات آن توسعه داده شد و بر اساس چارچوب توسعه داده شده سئوالات پرسش نامه تهیه و تدوین گردید، چارچوب ثانویه و تکمیلی پژوهش، خروجی این مرحله می باشد که در شکل (5) قابل مشاهده می باشد.

در گام سوم به منظور اعتبار سنجی کمی چارچوب تکمیلی، نظر خبرگان میانی که بصورت هدفمند انتخاب گردیده بودند گرفته شد و پس از تدوین پرسشنامه بر اساس چارچوب ثانویه، نسبت به بررسی روایی ابزار تحقیق از روایی محتوایی و برای بررسی پایایی ابزار تحقیق از روش آلفای کرونباخ استفاده شد. سپس عملیات جمع آوری اطلاعات از طریق پرسشنامه 66 سوالی با طیف لیکرت 5 سطحی در 8 بعد شاخص های مرتبط با بررسی بدافزارها، شاخص های مرتبط با آموزش افراد، شاخص های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت افزاری دستگاه همراه، شاخص های مربوط به چگونگی استخراج و شاخص های مربوط به استخراج ادله با استفاده از مقیاس پایایی و روایی مورد بررسی قرار گرفت و نهایتاً داده های حاصل با استفاده از آمار توصیفی و استنباطی (با میانگین آماری و ارزیابی سطح بلوغ CMMI) مورد تجزیه و تحلیل قرار گرفت. مراحل تدوین چارچوب مفهومی تحقیق در شکل (3) آورده شده است.

2-5 - سوالات جمعیت شناختی

جامعه آماری این تحقیق افراد و کارشناسان شاغل در حوزه امنیت و استنادپذیری ادله دیجیتال در مجموعه های مختلف انتظامی و قضایی و شرکت های امنیتی، محققین دانشگاهی و ... می باشند که سعی شده افراد از شاغلین مرتبط که تجربه کار عملی و آگاهی نسبت به موضوع دارند، انتخاب شوند. تعداد جامعه آماری مذکور 32 نفر بود که از بین این 32 نفر 12 نفر به عنوان خیره اصلی در گام اول مورد مصاحبه قرار گرفتند و 20 نفر به عنوان خبره میانی برای تکمیل پرسشنامه در نظر گرفته شدند. خبرگان به روش هدفمند در طول فرآیند تحقیق انتخاب شدند. نمونه گیری هدفمند یکی از روش های شایع نمونه گیری است که گروه های شرکت های کننده بر اساس معیارهای از قبل مشخص شده مربوط به سؤال ویژه پژوهش انتخاب می شوند.

جدول 2: اطلاعات جمعیت شناختی پرسش شوندگان

میزان تحصیلات نمونه آماری			
تحصیلات	فراوانی	درصد	
دکتری	4	12.5	
کارشناسی ارشد	18	56.25	
کارشناسی	10	31.25	
جمع	32	100	

سابقه فعالیت نمونه آماری			
سابقه فعالیت	فراوانی	درصد	
زیر 5 سال	7	21.87	
6 تا 10	15	46.87	
11 تا 15	8	25	
16 تا 20	2	6.2	
بالای 20	0	0	
جمع	32	100	

رده مسئولیتی نمونه آماری

میزان آشنایی با موضوع نمونه آماری			
رده مسئولیتی	فراوانی	درصد	
عضو هیئت علمی	3	9.37	
مدیریتی	3	9.37	
کارشناسی	26	81.25	
جمع	32	100	

رشته تحصیلی نمونه آماری			
رشته	فراوانی	درصد	
فنی و سایر	17	53.125	
مدیریت و IT	5	15.625	
کامپیوتر	10	31.25	
جمع	32	100	

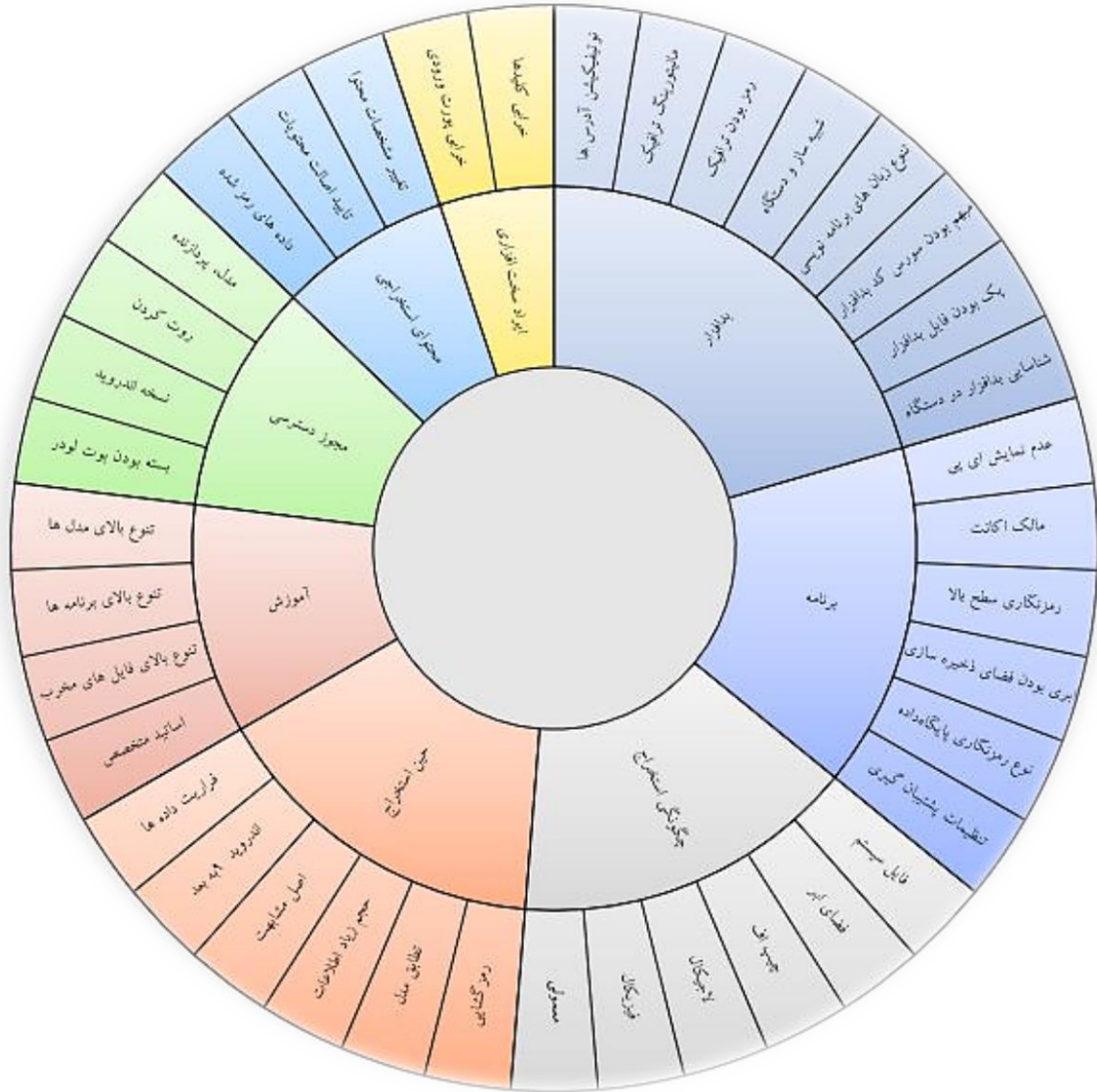
در جدول (2)، اطلاعات جمعیت شناختی کل خبرگان، مشتمل بر میزان تحصیلات، رشته تحصیلی، میزان آشنایی با موضوع تحقیق، سابقه یا سنوات خدمتی و رده مسئولیتی بیان گردیده است عنوان هر جدول بیانگر یکی از ویژگی های پرسش شوندگان بوده و مورد با بیشترین آمار به صورت خاص مشخص شده است.

3-5 - سوالات استنباطی تحقیق

لازم به یادآوری است که سوالات تحقیق 66 مورد در نظر گرفته شده که از طریق آن ها نظرات نخبگان میانی درباره شاخص های هر سؤال جمع آوری گردیده است. ابعاد و مولفه های مربوط به هر کدام از سوالات در جدول (3) آمده

است (برای وضوح بیشتر نمودار از هر مولفه اصلی تنها برخی از زیر مولفه ها نشان داده شده است).

است و با توجه به چارچوب مفهومی اولیه، چارچوب نهایی ذیل استخراج گردید که در شکل (5) به نمایش گذارده شده



شکل 5: چارچوب نهایی الزامات استنادپذیری ادله استخراجی دستگاه های تلفن همراه

4-5- پایایی و روایی ابزار تحقیق

در این پژوهش، روایی منطقی پرسشنامه از دو جنبه روایی ظاهری و محتوایی به جهت روشن و بدون ابهام بودن گویه ها و همچنین کفایت کمیت و کیفیت آن ها با کمک تعدادی از خبرگان و صاحب نظران استنادپذیری ادله دیجیتال مورد بررسی قرار گرفت و در جهت رسیدن به یک پرسشنامه استاندارد، تغییرات لازم در آن ها اعمال شد. در این راستا، به

منظور اعتبار ظاهری پرسشنامه مواردی از قبیل طرح سوالات کوتاه و جامع، مرتبط با موضوع تحقیق، عدم ابهام در سوالات، عدم وجود سوالات منفی، حذف سوالات القاء کننده رعایت گردید. همچنین جهت اعتبار محتوایی پرسشنامه مواردی مانند اطمینان از برداشت یکسان از سوالات، اطمینان از منطبق بودن برداشت مشارکت کنندگان و محقق کنترل گردید. نهایتا با ثبت نتایج پرسشنامه ها در نرم افزار SPSS و انجام محاسبات آمار استنباطی میزان پایایی و اعتبار

5-5 - تحلیل داده‌های استخراجی پرسش نامه‌ها

در تهیه سوالات و شاخص‌های پرسش نامه از نقطه نظرات خبرگان در حوزه استنادپذیری ادله دیجیتال استفاده شد که به روش نمونه‌گیری گلوله برفی از میان افراد خبره انتخاب شدند. نحوه تکمیل پرسشنامه به این ترتیب بود که در ابتدا موضوع جهت مطالعه اولیه در اختیار خبرگان قرار می‌گرفت، سپس خبرگان با توضیحات حضوری محقق و بر اساس مطالعه قبلی به مصاحبه پاسخ می‌دادند. پس از تکمیل مصاحبه با هر یک از خبرگان، فرد یا افراد دیگری را جهت مصاحبه انتخاب می‌گردید. انتخاب و مصاحبه با افراد تا جایی ادامه یافت که اشباع اطلاعاتی صورت گرفت و مفاهیم جدیدی برای تکمیل پرسشنامه‌ها مشاهده نشد، مصاحبه‌ها به صورت حضوری و مجازی با کارشناسان و خبرگان استنادپذیری ادله دیجیتال طی جلسات مختلف انجام گردید. سپس به منظور اعتبارسنجی داده‌های جمع‌آوری شده در فاز بعدی از پرسشنامه استفاده شد و نظرات هر یک از خبرگان در رابطه با اهمیت هر یک از الزامات اخذ گردید که در جدول (4) نتایج حاصل از پرسش نامه‌ها نشان داده شده است.

پرسشنامه این تحقیق با محاسبه آلفای کرونباخ، مورد سنجش قرار گرفته است. مقدار ضریب آلفای کرونباخ کل 76.0% به دست آمد که نشان دهنده وجود پایایی بالایی برای پرسشنامه می‌باشد (جدول 3).

جدول 3. پایایی جزئی پرسشنامه

متغیر	مقدار آلفای کرونباخ
شاخص‌های مربوط به آموزش افراد	85%
شاخص‌های مربوط به محتوای استخراج ادله	70%
شاخص‌های مربوط به چگونگی استخراج	72%
ایراد سخت‌افزاری دستگاه همراه	86%
چالش‌های مبتنی بر برنامه	79%
شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی	74%
شاخص‌های مرتبط با بررسی بدافزارها	71%
شاخص‌های مربوط به حین استخراج ادله	70%
میانگین آلفای کرونباخ	76%

جدول 4. تحلیل آماری سوالات تحقیق و میزان اهمیت هر یک از مولفه‌ها و رتبه اخذ شده آن‌ها در هر گروه

رتبه	میزان اهمیت (%)	توصیف	مولفه‌ها	شاخص‌ها
3	78	تغییر ویژگی‌های فایل در اثر انتقال در بستر شبکه‌های اجتماعی؛ زمان ایجاد، زمان دسترسی و ...	تغییر مشخصات محتوا	محتوای استخراج شده
5	70	عملکرد ضعیف ابزارهای تشخیص اصالت علی‌الخصوص در فایل‌های چند رسانه‌ای	تایید اصالت محتویات	
1	88	رمزنگاری پارتیشن data از اندروید 7 به بعد که رمزگشایی در پردازنده‌های جدید را بسیار مشکل می‌نماید	داده‌های رمز شده	
		داده‌ها و فایل‌های رمزنگاری شده در میان محتویات بدست آمده از گوشی تلفن همراه		
		عدم دستیابی به اطلاعات در ریکاوری گوشی‌های رمز شده حتی با اخذ دامپ فیزیکی و روت بودن گوشی		
		عدم آنالیز اتوماتیک محتوای شبکه‌های اجتماعی به دلیل رمزنگاری		

4	75	تغییر محتوا به سبب فشرده سازی و یا عبور از بستر اینترنت به عنوان مثال تفاوت ویژگی های صوتی گوینده در هنگام تطبیق با نمونه اصلی صدای مورد بررسی	تغییر محتوا	شاخص های حین استخراج ادله
2	82	از بین رفتن اطلاعات مکانی و برخی ویژگی های دیگر به سبب حفظ حریم خصوصی	از بین رفتن محتوا	
9	60	نقش سیستم عامل و تاثیر نسخه های مختلف معدود بودن ابزارهای جمع آوری داده های فرار در اندروید و ios	فراریت داده ها	
1	82	عدم اخذ دامپ فیزیکی یا روت بودن گوشی برابر است با عدم امکان دستیابی به اطلاعات	عدم امکان اخذ دامپ فیزیکی در اندرویدهای 9 به بعد	
11	52	برخلاف هارد دیسک، دامپ فیزیکی در گوشی از mmcblk ها اخذ می شود نه از همه خانه های حافظه	اصل مشابهت (کپی بیت به بیت)	
12	50	در گوشی های جدید با حافظه بالا نیاز به سیستم آنالیز با کانفیگ بالا جهت بهبود عملکرد می باشد	حجم زیاد اطلاعات	
6	69	عقب بودن حداقل یکساله ابزارها در پشتیبانی از گوشی های جدید - وجود مدل گوشی همراه در میان پایگاه داده مدل های معرفی شده به ابزار فارنزیک امکان بررسی بهتر عملیات فارنزیک را میسر می کند.	تطابق مدل گوشی با مدل های موجود در ابزار آنالیز	
2	80	غیرفعال بودن USB debugging در حالت پیش فرض امکان فارنزیک بسیاری از مدل ها را ناکام می گذارد	رمزگشایی و ریکاوری حافظه داخلی	
10	55	عدم تطابق قوانین با برخی روشهای فارنزیک (مدارک دیجیتالی وقتی از نظر قانونی معتبر هستند که به نحوی جمع آوری، تجزیه و تحلیل، رسیدگی و ذخیره شده باشند که توسط قانون قابل قبول باشند و شواهد منطقی برای اثبات آن وجود داشته باشد).	تطابق قانونی	
4	76	وابستگی روش های فارنزیک به برند و مدل پردازنده	نقش سخت افزار	
5	72	عدم اطمینان به عملکرد استاندارد ابزار مثلاً خراب کردن بوت لودر گوشی در اثر تلاش برای اخذ دامپ فیزیکی و منطقی	اعتماد به ابزار	
3	78	با توجه به انحصار برخی از تجهیزات و وجود تحریم، در خرید و نگهداری این تجهیزات مشکلاتی وجود دارد	دسترسی به منابع سخت افزاری و نرم افزاری	
7	66	استفاده از ابزارهای مخفی کننده محتوا (Vault) که در اکثر موارد داده ها را رمز هم می کنند	مخفی بودن اطلاعات	

8	63	توجه به وجود فضای دوم؛ در برخی برندها امکان تشخیص فضای دوم مشکل می باشد.	فضای دوم برخی مدل گوشی ها	
4	78	معمولی ترین روش استخراج است که با استفاده از اسکرین شات از صفحه صورت می گیرد علی الخصوص در بررسی اپ های ایرانی بسیار مشهود است	به صورت معمولی و دستی	شاخص های مربوط به چگونگی استخراج
1	85	بهترین حالت استخراج اطلاعات از گوشی های تلفن همراه می باشد که در اغلب روت بودن گوشی نیز می باشد	به روش فیزیکی	
2	82	در این روش تنها اطلاعات موجود و قابل دسترس استخراج می گردند که امکان تایید اصالت با چالش روبرو است.	به روش منطقی	
5	75	در مواردی کاربرد دارد که نیاز به جداسازی هارد داخلی گوشی مطرح باشد و احتمال آسیب سخت افزاری به موبایل بالا می باشد.	Chip-off and JTAG	
3	80	در صورت عدم دست یابی به رمز ورود فضای ابری فارتزیک و استخراج اطلاعات آن با چالش روبرو می گردد همچنین احتمال حذف داده ها از راه دور به دلیل لزوم بررسی آنلاین فضای ابر بالا می باشد.	فضای ابر	
6	72	در این روش علاوه بر دست یابی به اطلاعات مدل منطقی، به برخی فایل های سیستمی نیز می توان دست یافت	استخراج فایل سیستم	
10	61	زمانبر بودن بررسی در برخی از روشها	پیچیدگی زمانی	
9	63	ابزارهای فارتزیک بلید از استلنداردهای لازم برخوردار و مورد قبول محاکم قضایی باشند	ابزارهای استاندارد	
11	55	گزارش نویسی باید استاندارد و مورد قبول دادگاه باشند	گزارش نویسی	
7	69	ناقص بودن اطلاعات در بررسی آفلاین بخصوص در اینستاگرام و تلگرام احتمال حذف اطلاعات از راه دور در بررسی آنلاین گوشی	آفلاین و یا آنلاین بودن بررسی	
8	65	عدم پشتیبانی فروشنده به دلایل تجاری و سیاسی (تحریم)	پشتیبانی و خدمات پس از فروش	
2	65	ایراد در این بخش موجب عدم نمایش پیام های تایید بر روی صفحه در حین استخراج محتویات و اخلاص در امر فارتزیک و استخراج می گردد	شکستگی و خرابی LCD	ایراد سخت افزاری دستگاه همراه
4	50	هزینه بالای تعمیر تجهیزات در کنار دسترسی به داده ها باید مدنظر قرار گیرد.	هزینه بالا	
3	60	در عملیات فارتزیک گوشی همراه گاها نیاز است گوشی به حالت ریکاوری مد و یا دانلودینگ مد برود که لازمه آن استفاده از کلیدهای ولوم، پاور و هوم است	خرابی کلیدها (برای رفتن به ریکاوری مد و یا دانلودینگ مد)	

1	70	در برخی موارد پورت ورودی معیوب بوده و حالت انتقال دیتا آن فعال نبوده و تنها عملیات شارژ انجام می شود	خرابی پورت ورودی برای اتصال به سیستم	چالش های مبتنی بر برنامه
9	72	غیر فعال کردن تنظیمات پشتیبان گیری در شبکه های اجتماعی توسط کاربر و یا محدود بودن آن به چند روز موجب عدم تشکیل پایگاه داده بکاپ در بازه های زمانی تنظیمی می شود	تنظیمات مربوط به پشتیبان گیری برنامه ها توسط کاربر	
1	92	نوع رمزنگاری پایگاه داده برنامه های نصبی موجود بر اساس نسخه برنامه می باشد به عنوان مثال پایگاه داده msgstore.db واتساپ در نسخه های قبلی مبتنی بر crypt12 بود که در نسخه های جدیدتر crypt14 شده است که رمزگشایی آن مشکل تر شده است.	نوع رمزنگاری پایگاه داده برنامه های نصبی موجود	
7	80	برنامه هایی مانند واتساپ، تلگرام و ... اطلاعات خود را در فضای ابر ذخیره می کنند.	ابری بودن فضای ذخیره سازی	
2	90	حتی بعد از دسترسی به پایگاه داده برنامه های مختلف با توجه به رمزنگاری سطح بالای آن ها عملا استفاده از آن ها غیر ممکن است.	رمزنگاری سطح بالا	
8	76	در برخی برنامه ها مانند اینستاگرام هنگام ریکاوری رمز عبور نیاز به گوشی و سیمکارت مالک اکانت می باشد	گوشی و سیمکارت مالک اکانت	
10	70	عدم نمایش ip در session های برخی از برنامه ها مانند واتساپ	عدم نمایش ip	
5	85	داشتن رمز ورود بر روی برنامه موجب چالش در بررسی به روش دستی یا معمولی می شود	رمز ورود اپلیکیشن	
4	86	در برنامه ها با رمز دو مرحله ای بررسی با چالش های بیشتری روبرو است.	وجود رمز دو مرحله ای	
12	65	برخی برنامه های قابلیت پنهان نمودن پیام های مخاطبین را داشته که در روش دستی می تواند موجب پنهان ماندن ادله گردد	پنهان بودن پیام	
3	88	با توجه به اینکه برخی برنامه ها امکان دسترسی از طرق مختلف را دارند امکان حذف اکانت وجود دارد.	کنترل از راه دور	
11	68	عدم نگهداری سابقه session های منقضی شده در برنامه های مختلف مانند تلگرام و واتساپ	عدم نگه داری لاگ	
6	82	خارجی بودن ip مربوط به sessionها به دلیل استفاده از vpn	ip نامعتبر	

13	60	برخی از برنامه ها مدتی را جهت انصراف از حذف همیشگی اکانت در نظر می گیرند به عنوان مثال مدت هفت روزه برای حذف همیشگی اکانت تلگرام	حذف اکانت	
1	95	وابستگی بالا به مدل، نوع پردازنده و ... برای عبور از رمز ورود و اقدامات بعدی وجود تمهیدات امنیتی مانند Knox, secureboot, oem, frp و ...	عبور از رمز گوشی، مدل، پردازنده، security level	شاخص های مبتنی بر مجوزهای دسترسی به گوشی
2	93	حذف اطلاعات حین تلاش برای روت کردن گوشی به دلیل وجود frp	روت کردن	
4	85	چالش در اندروید های 7 به بعد به دلیل رمزنگاری پارتیشن data	عبور از رمز ورود، نسخه اندروید	
5	80	علاوه بر نسخه سیستم عامل ارتقا سیستم عامل نیز در دسترسی به تلفن همراه می تواند تاثیر گذار باشد.	Firmware update protocol	
3	90	حذف اطلاعات گوشی در اثر تلاش برای بازکردن بوت لودر	بسته بودن بوت لودر	
1	90	سخت و زمانبر بودن تشخیص بدافزار های bind شده	شناسایی بدافزار در دستگاه	شاخص های مرتبط با بررسی بدافزارها
9	75	Pack بودن فایل های بدافزار در آنالیز استاتیکی آنها	Pack بودن فایل بدافزار	
7	80	مبهم بودن سورس کد بدافزار در آنالیز استاتیکی	مبهم بودن سورس کد بدافزار	
8	78	تنوع زبان های برنامه نویسی بدافزارها	تنوع زبان های برنامه نویسی بدافزارها	
10	74	رفتار متفاوت بدافزار حین اجرا در شبیه ساز و گوشی	شبیه ساز و دستگاه	
2	88	رمز بودن ترافیک شبکه در بررسی داینامیک بدافزارها	رمز بودن ترافیک	
3	87	نامشخص بودن زمان ارسال ترافیک و لذا زمانبر شدن فرایند مانیتورینگ ترافیک	زمانبر بودن مانیتورینگ ترافیک	
4	85	استفاده از نوتیفیکیشن به جای تعبیه آدرس ها در سورس کد	نوتیفیکیشن آدرس ها	
6	83	استفاده از DNS سرورهای رایگان خارجی که شناسایی مقصد ترافیک شبکه را غیرممکن می نماید	DNS سرورهای رایگان	
5	84	استفاده از سرویسهای خارجی Push Notification	سرویسهای خارجی	

1	70	ضعف آموزش کارشناسان فارنزیکی به دلیل تنوع بالای خواسته های فارنزیکی موبایل - اهمیت میزان تسلط کارشناسان ادله در خصوص مهارت در خصوص انتقال صحیح تجهیزات به مرکز بررسی فنی	تنوع بالای مدل ها	شاخص های مرتبط با آموزش افراد
4	55	آموزش و بررسی نکات کلیدی برنامه هم مشکل می باشد و هم زمانبر	تنوع بالای برنامه ها	
3	60	نیاز به مهارت و نفرت متخصص و متعدد می تولد جوابگوی تعداد بالای مخرب ها باشد	تنوع بالای فایل های مخرب	
2	65	اساتید متخصص و بومی باید تربیت شوند	اساتید متخصص	
5	50	با توجه به انحصار طلبی و درآمدزایی بالا برخی از تکنیک ها و ترفندها آموزش داده نمی شوند	روحیه اشتراک دانش	
6	45	با توجه به دانش کم هم بسیاری از کارشناسان کسب درآمد می کنند لذا روحیه آموزش پذیری کمی دارند	درآمدزایی با دانش کم	

جدول 5: رتبه بندی مولفه های اصلی الزامات استنادپذیری ادله استخراج شده از گوشی تلفن همراه

رتبه	میانگین	بعد
8	57.5	شاخص های مربوط به آموزش افراد
3	78.6	شاخص مربوط به محتوای استخراج شده
5	71.36	شاخص های مربوط به چگونگی استخراج
7	61.25	ایراد سخت افزاری دستگاه همراه
4	78	چالش های مبتنی بر برنامه
1	88.6	شاخص مجوزهای دسترسی به گوشی
2	82.4	شاخص های مرتبط با بررسی بدافزارها
6	66.91	شاخص های مربوط به حین استخراج ادله

پس از بررسی، الزامات استنادپذیری ادله دیجیتال استخراجی از گوشی های تلفن همراه در قالب هشت بُعد، شاخص های مرتبط با بررسی بدافزارها، شاخص های مرتبط با آموزش افراد، شاخص های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت افزاری دستگاه همراه، شاخص های مربوط به چگونگی استخراج، شاخص های مربوط به ادله استخراج شده و شاخص های مربوط به حین استخراج ادله گروه بندی و طبقه بندی گردید که اهمیت هر یک از گروه ها با توجه به نظرات خبرگان میانی در جدول (5) به نمایش گذارده شده و علاوه بر آن تعداد 10 مولفه مهم تر که باید در اولویتهای برنامه ریزی قرار گیرند مشخص گردید (با توجه به نظرات خبرگان میانی، به شرح جدول 6):

جدول 6: مهم ترین چالش های استنادپذیری ادله دیجیتالی استخراجی از گوشی های تلفن همراه

رتبه	مولفه جزئی	میزان اهمیت (%)	مولفه اصلی
1	عبور از رمز گوشی، مدل، پردازنده، security level	95	شاخص های مبتنی بر مجوزهای دسترسی به گوشی
2	روت کردن	93	شاخص های مبتنی بر مجوزهای دسترسی به گوشی
3	نوع رمزنگاری پایگاه داده برنامه های نصبی موجود	92	چالش های مبتنی بر برنامه

4	رمزنگاری سطح بالا	90	چالش های مبتنی بر برنامه
5	بسته بودن بوت لودر	90	شاخص های مبتنی بر مجوزهای دسترسی به گوشی
6	شناسایی بدافزار در دستگاه	90	شاخص های مرتبط با بررسی بدافزارها
7	داده های رمز شده	88	محتوای استخراج شده
8	کنترل از راه دور	88	چالش های مبتنی بر برنامه
9	رمز بودن ترافیک	88	شاخص های مرتبط با بررسی بدافزارها
10	زمانبر بودن مانیتورینگ ترافیک	87	شاخص های مرتبط با بررسی بدافزارها

همان طور که در جدول (5) مشاهده می شود میانگین بار عاملی شاخص های مبتنی بر مجوزهای دسترسی به گوشی مهم ترین الزام بوده که برای آینده نگری استنادپذیری گوشی های تلفن همراه حتما باید مد نظر قرار گیرد. در رابطه با شاخص مربوط به آموزش افراد که در رتبه هشتم قرار گرفته با توجه به تجربه بیش از 10 ساله سازمان های شاغل در این حوزه و وجود افراد با تحصیلات آکادمیکی بالا کسب رتبه هشتم و چالشی نبودن این شاخص در بین سایر شاخص ها دور از ذهن نمی باشد.

با توجه به موارد عنوان شده در جدول (6) عبور از رمز گوشی، مدل، پردازنده، security level که از مولفه های جزئی شاخص های مبتنی بر مجوزهای دسترسی به گوشی می باشد به عنوان مهم ترین الزام استنادپذیری ادله دیجیتالی استخراجی از گوشی های تلفن همراه از نظر خبرگان میانی انتخاب شده است که با توجه به پیشینه تحقیق نیز می توان اهمیت این مولفه را تایید کرد و رفته رفته با به روز سازی تکنولوژی رمزنگاری در گوشی های تلفن همراه باز کردن آن ها بیش از پیش سخت تر و بعضا غیر ممکن شده است.

6-5 - تحلیل بلوغ بر مبنای CMMI

در این تحقیق مصاحبه در دو مرحله انجام گردید که در مرحله اول به منظور کشف مقوله های کلیدی و با طرح سوالات باز انجام شد و در مرحله دوم یک پرسشنامه نیمه ساختاریافته تهیه شد و به صورت حضوری و مجازی، توسط

خبرگان تکمیل گردید. پرسشنامه آزمون خبرگی الگوی مفهومی پیشنهادی جهت اخذ تأییدیه خبرگان و تعیین میزان اهمیت هر یک از ابعاد و مولفه های شناسایی شده و همچنین بررسی مطابقت و تناسب هر یک از مؤلفه ها با ابعاد تعیین شده، تهیه شد. پس از جمع بندی و تحلیل پاسخ های داده شده به پرسشنامه مذکور برابر جدول (4)، اهمیت ابعاد و مؤلفه های چارچوب مفهومی پیشنهادی به دست آمد که با استناد به مطالعات کتابخانه ای، مصاحبه ها و مطالعات میدانی و همچنین تجزیه و تحلیل انجام شده، ده الزام و مانع مهم استنادپذیری ادله استخراجی از موبایل به شرح جدول (5) به دست آمد.

با توجه به مولفه های استخراجی و مشخص شدن اهمیت هر یک از آن ها این سؤال مطرح می شود وضعیت فعلی به چه صورت می باشد که چگونه می توان بر اساس مقادیری قابل اندازه گیری نشان داد که یک سازمان به چه میزان در دستیابی به اهداف کلیدی خود قرار دارد مدل هایی مانند CMMI می توانند سطح بلوغ یک سازمان را بر مبنای معیارهای کسب شده به نمایش گذارند که در جدول (7) بر مبنای مدل سطوح بلوغ در CMMI جایگاه کنونی یکی از سازمان های مسئول در حوزه استخراج ادله دیجیتال در هشت بعد اصلی مطرح شده بر اساس نظرات تقریبی (به جهت تبدیل نظرات کیفی به کمی با طیف لیکرت 5 سطحی) 20 نفر از کارشناسان شاغل در آن سازمان آورده شده است.

بررسی قرار می گیرد، بعضاً حتی اطلاعات بازیابی شده از گوشی به صورت تغییر یافته و یا رمز شده بوده و نمی توان از آن ها استفاده کرد که برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره تقریبی 42 در سطح سوم بوده یعنی استانداردهای لازم حدوداً تعریف شده و تقریباً استفاده می شود ولی با توجه به موارد بیان شده جای کار دارد.

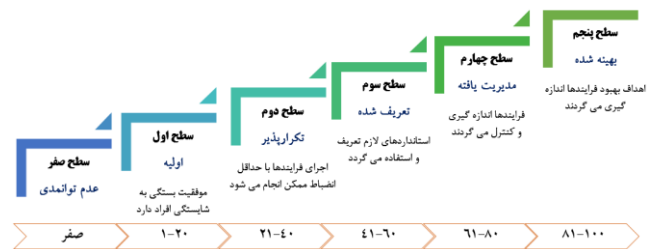
شاخص های مربوط به چگونگی استخراج: شاخص چگونگی استخراج اشاره به روش های موجود برای بررسی گوشی های تلفن همراه دارد که در این بین روش منطقی، بهترین حالت استخراج اطلاعات از گوشی های تلفن همراه می باشد که در اغلب موارد نیاز به روت بودن گوشی نیز می باشد علاوه بر این باید دقت داشت که ابزارهای فارتزیکي مورد استفاده در استخراج اطلاعات گوشی ها باید از استانداردهای لازم برخوردار و مورد قبول محاکم قضایی باشند که برابر تحلیل نظرات خبرگان در این شاخص بر اساس ارزیابی سطح بلوغ CMMI با نمره تقریبی 47 در سطح سوم بوده یعنی استانداردهای لازم حدوداً تعریف شده و تقریباً استفاده می شود.

الزامات مربوط به ایراد سخت افزاری دستگاه همراه: بعد چالش های سخت افزاری اشاره به ایراداتی دارد که در عملیات استنادپذیری ادله استخراجی از گوشی همراه نیاز است بعضاً نیاز است گوشی به حالت ریکاوری مد و یا دانلودینگ مد برود که لازمه آن استفاده از کلیدهای ولوم، پاور و هوم است که بعضاً در گوشی ها این موارد آسیب دیده است یا ایراداتی دیده می شود که هزینه تعمیر آن ها بالا بوده و باید مدنظر قرار گیرد لذا برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره تقریبی 68 در سطح چهارم بوده یعنی فرایندها اندازه گیری و کنترل می گردند لازم به ذکر است که برخی مواقع ایرادات اساسی بوده و برای آن ها نیاز به تجهیزات و تجربه بالا می باشد و ریسک انجام آن توسط کارشناسان بالا بوده لذا چنین مواردی توسط افراد متخصص بیرون از شرکت صورت می گیرد.

چالش های مبتنی بر برنامه: چالش های مربوط به برنامه اشاره به مشکلاتی دارد که کارشناس استنادپذیری برای دسترسی به شواهد موجود در برنامه ها با آن ها روبرو است بعضاً حتی بعد از دسترسی به شواهدی مانند پایگاه داده برنامه، با توجه به رمزنگاری سطح بالای آن عملاً نمی تواند از آن ها استفاده کند. برابر تحلیل

جدول 7. ارزیابی بلوغ استنادپذیری ادله دیجیتالی استخراجی از گوشی های تلفن همراه

میانگین نمره	بعد
67	شاخص های مربوط به آموزش افراد
42	شاخص های مربوط به محتوای استخراج شده
47	شاخص های مربوط به چگونگی استخراج
68	ایراد سخت افزاری دستگاه همراه
52	چالش های مبتنی بر برنامه
35	شاخص های مبتنی بر مجوزهای دسترسی به گوشی
45	شاخص های مرتبط با بررسی بادهزارها
48	شاخص های مربوط به حین استخراج ادله



شکل 6. سطوح بلوغ در CMMI

طبق ارزیابی صورت گرفته و سطوح بلوغ در CMMI، میزان موفقیت در استخراج و استنادپذیری ادله دیجیتالی گوشی های تلفن همراه را می توان به این صورت تعریف کرد:

شاخص های مربوط به آموزش افراد: بعد آموزش اشاره به یاددهی و یادگیری نیروهای تخصصی در جهت مرتفع سازی مشکلات و چالش های استنادپذیری دارد. برابر تحلیل نظریات کارشناسان شاغل در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره 67 در سطح چهارم بوده یعنی به حد قابل قبولی رسیده و فرایندها اندازه گیری و کنترل می گردند.

شاخص های مربوط به محتوای استخراج شده: بعد محتوای استخراج شده به اطلاعاتی دلالت دارد که در اختیار کارشناس برای

۶- نتیجه‌گیری و پیشنهادها

1-6 - جمع بندی

مشخص شدن الزامات استنادپذیری ادله دیجیتال استخراجی از گوشی‌های تلفن همراه، آینده را به کمک امروز آورده و مبنای تصمیم‌گیری‌ها، سیاست‌گذاری‌ها و برنامه‌ریزی‌ها در ساختار مدیریتی، آموزشی، پژوهشی و فناوری خواهد بود. لذا با وجود مراکز امنیتی انتظامی و قضایی در حوزه‌های استنادپذیری ادله دیجیتال در سطح کشور، می‌توان توسعه تکنولوژیکی در مجموعه برنامه ریزان و کارکنان این نهادها را انتظار داشت.

لذا یافته‌های مرتبط با شاخص‌ها و الگوی‌های متجانس با رویکرد استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های تلفن همراه، با توجه به مطالعات صورت گرفته و نظرات نخبگان، پیشنهادات محققین مقاله در دو چارچوب مفهومی اولیه و چارچوب حاصل از نظرات نخبگان در اشکال 4 و 5 و در هشت بعد کلی بیان گردید که از بین این هشت بعد، همان‌طور که در جدول (5) مشاهده می‌شود میانگین بار عاملی شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی با 88.6 درصد مهم‌ترین الزام بوده و شاخص مربوط به آموزش افراد که با 57.5 درصد در رتبه هشتم قرار گرفته است، با توجه به الزامات مطرح شده در چارچوب ارائه شده باید راهکارهایی برای این موارد دیده شود.

راهکارهای دستیابی به الزامات با توجه به نظرات اکتسابی از پرسش‌نامه‌ها و نظرات خبرگان راهکارهای دستیابی به الزامات مطرح شده در قالب هشت‌بعد، شاخص‌های مرتبط با بررسی بدافزارها، شاخص‌های مرتبط با آموزش افراد، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی، چالش‌های مبتنی بر برنامه، ایراد ساخت‌افزاری دستگاه همراه، شاخص‌های مربوط به چگونگی استخراج، شاخص‌های مربوط به ادله استخراج‌شده و شاخص‌های مربوط به حین استخراج ادله در نظر گرفته شده است که در قسمت پیشنهادها به راهکارها و نحوه دستیابی به الزامات به صوت مشروح پرداخته شده است.

در رابطه با بررسی وضعیت موجود استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های تلفن همراه، پیاده‌سازی و سنجش بلوغ متناسب با یکی از سازمان‌های مرتبط (به نمایندگی از کل) با موضوع استنادپذیری مد نظر قرار گرفت که سطح متناسب با نمره کسب شده در سنجش بلوغ CMMI در جدول (7) بیان گردیده

نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره تقریبی 52 در سطح سوم بوده یعنی استانداردهای لازم حدوداً تعریف شده و تقریباً استفاده می‌شود ولی با توجه به موارد بیان شده علی‌الخصوص در رابطه با دستیابی به اطلاعات رمز شده جای کار دارد.

شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی: دسترسی به اطلاعات گوشی تلفن همراه نیازمند عبور از رمز گوشی و داشتن سایر دسترسی‌هاست لذا در صورت نداشتن چنین دسترسی باید یا چنین دسترسی‌هایی را ایجاد کرد و یا از آن‌ها عبور کرد که انجام چنین اقدامی وابستگی بالایی به مدل، نوع پردازنده و ... گوشی برای عبور از رمز ورود و اقدامات بعدی دارد که برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره 35 در سطح دوم بوده اجرای فرایندها با حداقل انضباط ممکن انجام می‌گردد.

شاخص‌های مرتبط با بررسی بدافزارها: شناسایی و بررسی بدافزارها با توجه به پیشرفت‌های صورت گرفته در حوزه هک و نفوذ، کار سخت و زمانبر بوده و بعضاً این بدافزارها در سایر نرم‌افزارها گنجانده می‌شوند که در این صورت تشخیص بدافزارها مشکل‌تر نیز می‌شود و در مواقعی نیز بعد از شناسایی با توجه به رمز بودن ترافیک شبکه امکان بررسی بدافزارها با مشکلات خاص خود روبرو می‌باشد، با این وجود برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره 45 در سطح دوم بوده اجرای فرایندها با حداقل انضباط ممکن انجام می‌گردد.

شاخص‌های مربوط به حین استخراج ادله: ممکن است در حین استخراج داده‌ها با چالش‌های مربوط به حفظ اصالت داده‌ها و یا با اعمال روش‌های مختلف برای دستیابی به اطلاعات، گوشی به تنظیمات کارخانه برگردد و اطلاعات همگی از بین روند یا این تفاسیر، برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره 48 در سطح دوم بوده اجرای فرایندها با حداقل انضباط ممکن انجام می‌گردد.

است. نتیجه به دست آمده حاکی از آن است که ادارات و معاونت های دخیل در استنادپذیری ادله دیجیتال با استفاده از ظرفیت های موجود در چارچوب ها و استناداردهای بین المللی حرکت می نمایند و با توجه به نوظهور بودن این فناوری، در سطح بلوغ میانه ای قرار دارند و می توانند خود را با آینده نگری و پی گیری هدفمند به سطح بلوغ مناسب تری برسانند.

2-6- پیشنهادها و کارهای آینده

دانش استنادپذیری ادله دیجیتال پیوسته در حال تکامل بوده و طبیعتاً الزامات آن هم به طور متقابل، همواره با تغییر فناوری علی الخصوص در گوشی های تلفن همراه، تغییرات اساسی یافته است. در دوران گذشته، آموزش، بیشتر مدنظر بوده است، درحالیکه با تغییر در حیطه نیازها، نقش تجهیزات پر رنگتر گردیده است. الزامات استنادپذیری ادله دیجیتال استخراجی از گوشی های تلفن همراه، با توجه به نتایج به دست آمده از تجزیه و تحلیل داده های جمع آوری شده، مورد تأیید خبرگان قرار گرفت و با استناد به مطالب جمع آوری شده در تحقیق پیش رو، پیشنهادهایی در رابطه با ارتقاء و بهبود وضعیت هر یک از الزامات تعیین شده در استنادپذیری ادله دیجیتال استخراجی از گوشی های تلفن همراه، ارائه گردید.

دستیابی به الزامات آموزشی:

در حوزه آموزشی، دوره های آکادمیک مربوط به تعمیرات گوشی های تلفن همراه، استنادپذیری ادله دیجیتالی استخراجی از انواع گوشی های تلفن همراه، آموزش بررسی برنامه های مربوط به استنادپذیری ادله دیجیتال و ... به صورت جامع و مستمر بررسی و وضعیت فعلی ارزیابی و بر اساس دوره های بین المللی برای رسیدن به حالات استاندارد، آموزش ها و الزامات مربوطه به روز گردد طوری که کارشناسان استنادپذیری ادله دیجیتال به تمام فنون مورد نیاز تسلط کافی داشته باشند و تا تحقق کامل سطح چهارم و حتی دسترسی به سطح نهایی مدل CMMI ادامه یابد. با نگاه جزئی تر می توان موارد زیر را در نظر گرفت.

- توسعه دانش در زمینه تجهیزات و امکانات سخت افزاری و نرم افزاری موردنیاز واحدهای استنادپذیری ادله دیجیتال تا تولید دانش و ادبیات بومی در کشور در تمام زمینه ها؛

- ارتقاء دانش با طرح ریزی کوتاه مدت و میان مدت و ارزیابی دوره ای برای بررسی میزان تاثیرپذیری دوره های صورت گرفته و نیل به اهداف پیش رو.

- ایجاد انگیزه جهت موفقیت و تلاش مضاعف در دوره های آموزشی، تعامل بیشتر با مراکز دانشگاهی و بخش های خصوصی و دانش بنیان، اعزام کارکنان جهت حضور در دوره های آموزشی داخلی و در صورت اعزام به خارج از کشور، اجرای آموزش حین خدمت تخصصی جهت ارتقاء مهارت و تخصص کارکنان و ... نیز می تواند مؤثر می باشد.

- توجه به نیروهای چابک، متخصص، متعهد و تلاشگر در مجموعه لازم و ضروری است که برای دستیابی به چنین نیروهایی علاوه بر آموزش آن ها به تغییر بینش کارکنان و ایجاد تعلق خاطر و دلبستگی آنان به سازمان و ارتقاء حس مسئولیت و مالکیت آن ها لازم است.

دستیابی به الزامات چگونگی استخراج، حین استخراج، دسترسی به گوشی و محتوای استخراج شده:

سامانه های استنادپذیری ادله دیجیتال بر این مبنا ایجاد شده اند که اصالت داده ها را حفظ نمایند لذا با استفاده و تهیه این ابزار می توان گام مهمی در این زمینه برداشت ولی در رابطه با داده های رمز شده استخراجی و رمزگشایی آن ها که نیاز به دانش بالایی می باشد، پیشنهاد تهیه ابزارهایی است که در این خصوص توسط شرکت های صاحب نظر ایجاد شده اند موارد زیر را نیز برای دستیابی به الزامات مطرح شده می توان در نظر گرفت:

- تهیه ابزارهای مربوط به عبور کردن از رمز عبور گوشی های تلفن همراه ولی با توجه به وجود تحریم های مختلف کشورمان، دستیابی به چنین ابزارهایی بعضاً ممکن نمی باشد.

- برون سپاری عملیات رمزگشایی به شرکت هایی است که در این زمینه به صورت تخصصی در حال فعالیت می باشند.

- به روز رسانی مستمر ابزارهایی که برای دسترسی به اطلاعات گوشی در نظر گرفته شده اند و ابزارهایی که برای تحلیل اطلاعات استخراجی در نظر گرفته شده اند.

- اطمینان از عملکرد ابزارها و اقدامات فارتزیک با انجام مراحل تست بر روی گوشی هایی که بدین منظور در نظر

گرفته شده است (جلوگیری از وایپ شدن اطلاعات و شواهد و یا برگشت به حالت کارخانه گوشی).

دستیابی به الزامات ایرادات سخت‌افزاری دستگاه همراه:

دستیابی به الزاماتی که در ایرادات سخت‌افزاری گوشی‌های تلفن همراه دیده می‌شود در وهله اول نیازمند آموزش‌هایی می‌باشد که بتواند چنین ایراداتی را برطرف سازد که بعضاً هزینه تعمیرات گوشی‌های آسیب دیده بالا بوده و یا نیاز به تجهیزات و تجربه بالا می‌باشد ادامه راهکارهای جزئی تر در این خصوص بیان شده است:

- آموزش کارشناسان برای انجام تعمیرات سطح پایین.
- دسترسی به تجهیزات تعمیراتی گوشی‌های تلفن همراه برای انجام تعمیرات مورد نیاز استنادپذیری ادله دیجیتال.
- برخی مواقع ریسک انجام تعمیرات توسط کارشناسان بالا بوده لذا پیشنهاد می‌شود چنین مواردی برون سپاری شده و توسط افراد متخصص بیرون از شرکت صورت گیرد.
- برون سپاری تعمیرات تخصصی به علت بالا بودن هزینه تعمیرات و ریسک بالای از بین رفتن اطلاعات به هنگام فعالیت افراد کم تجربه.

دستیابی به الزامات بررسی برنامه‌های گوشی تلفن همراه:

- در بررسی استنادپذیری ادله استخراجی از برنامه‌های گوشی‌های تلفن همراه موانع بزرگی وجود دارد که مهم‌ترین آن‌ها عدم دسترسی به شواهد موجود در برنامه‌ها با توجه به وجود رمز عبور در نرم افزارهای مختلف می‌باشد که با توجه به رمز عبور دو مرحله بر مشکلات دسترسی به شواهد افزوده شده است شاید در حال حاضر نتوان راهکار فنی برای این منظور در نظر گرفت ولی می‌توان امید داشت که با راهکارهای غیر فنی و یا با گذر زمان بتوان بر این مشکلات فائق آمد. لذا می‌توان پیشنهادات زیر را در دستیابی به سایر الزامات برنامه‌های گوشی‌ها در نظر گرفت.
- بررسی راهکارهای غیر رسمی مطرح شده در اتاق‌ها و گروه‌های مجازی، در این خصوص باید دقت داشت که راهکارها در ابتدا بر روی سیستم‌هایی که بدین منظور در نظر گرفته شده تست شود.
 - استفاده از تکنیک‌های مهندسی اجتماعی برای دستیابی به اطلاعات برنامه‌های گوشی.

- استفاده از ظرفیت شرکت‌های سازنده نرم افزار با توجه به اهمیت موضوع.
- بررسی کامل برنامه‌ها و بررسی شواهد به جای مانده از آن‌ها در گوشی‌های تلفن همراه.

دستیابی به الزامات بررسی بدافزارها:

اولین و مهم‌ترین مرحله در بررسی بدافزارها شناسایی آن‌ها می‌باشد که معمولاً با کمک شواهد موجود انجام چنین عملی ممکن می‌گردد لذا برای استنادپذیری شواهد دیده شده در گوشی‌های تلفن همراه علاوه بر بررسی‌های استاتیک و پویا باید به مرحله شناسایی بدافزار هم دقت کافی داشت، پیشنهادات زیر جهت دستیابی به الزامات استنادپذیری بدافزارهای دیده شده در گوشی‌های تلفن همراه در نظر گرفته شده است:

- با توجه به نیاز فایل بدافزار برای بررسی در بسیاری از موارد دیده شده قربانی بعد از احساس وجود بدافزار در گوشی خود کلیه نرم افزارهای موجود را حذف می‌کند و یا به حالت کارخانه بر می‌گرداند که در این صورت کلیه شواهد لازم برای بررسی پاک شده و نمی‌توان آن را بررسی کرد، لذا لازم است آموزش‌های لازم در این خصوص داده شود.
- با توجه به اینکه بدافزارها در دوره‌های زمانی پیشرفت کرده‌اند باید راه‌های بررسی آن‌ها نیز پیشرفت کند لذا مطالعه مستمر و شرکت در دوره‌های بدافزار نویسی و بررسی و آموزش راه‌های مقابله با بدافزارها لازم و ضروری می‌باشد.
- با توجه به اینکه اطلاعات استخراجی از باج افزارها و بدافزارها به صورت رمز شده اغلب یافت می‌شوند لذا دستیابی به کلید رمزگشایی از اهمیت بالایی برخوردار است که بعد از مدتی شرکت‌های معتبر بین‌المللی در زمینه امنیت رایانه‌ها کلیدهای برخی از باج افزارها و بدافزارها را انتشار می‌کنند که می‌تواند برای رمزگشایی اطلاعات به کار رود. لذا بررسی سایت‌های معتبر بین‌المللی در این زمینه می‌تواند مثرتر باشد.
- با توجه به موارد بیان شده و لزوم بررسی الزامات استنادپذیری ادله استخراجی از گوشی‌های تلفن همراه لازم است مراکز با محوریت آینده پژوهی برای استنادپذیری توسط مبادی ذی ربط مانند سازمان‌های قضایی و ... ایجاد گردد که برای این مهم می‌توان

۹. سهلانی حسین، (1400)، "آینده پژوهی استنادپذیری ادله دیجیتال جرائم سایبری مبتنی بر اینترنت اشیا". فصلنامه علمی-پژوهشی فرماندهی و کنترل؛ ۵ (۳): ۳۸-۲۴.

۱۰. علی مظاهری، (1401)، "ارائه شیوه بهینه فارنزیک جهت واکنشی و تحلیل اطلاعات از شبکه های اجتماعی (مطالعه موردی پیام رسان واتساپ)"، پایان نامه کارشناسی ارشد، دانشگاه علوم انتظامی امین

از قطب های پژوهشی و دانشگاهی استفاده کرد. به غیر از مراکز دانشگاهی باید مطالعات مستمری در این زمینه در مراکز قضایی و انتظامی صورت پذیرد تا با کنار هم قرار دادن الزامات مختلف مانند به کار گیری نیروی انسانی متخصص، تجهیزات نرم افزاری و سخت افزاری، آموزش و تجربیات قبلی زیرساخت های مناسب را جهت بهینه سازی اقدامات استنادپذیری ادله استخراجی انجام داد.

منابع

1. Anoshia Menahil, Waseem Iqbal, Mohsin Iftikhar, Waleed Bin Shahid, Khwaja Mansoor, Saddaf Rubab. (2021). Forensic Analysis of Social Networking Applications on an Android Smartphone. *Wireless Communications and Mobile Computing*. Volume 2021. Article ID 5567592.
2. M Sharma, S Kaur. (2019). "Cyber crimes becoming threat to cyber security". *IASR Xournals*, vol. 2, no.1.
۳. سهلانی حسین، صادقی راشد رضا، (1396)، استنادپذیری ادله دیجیتال، تهران، دانشگاه علوم انتظامی امین.
4. Marcella albert j, Menendez Doug. (2014). *Cyber forensic book*. Cyber police.
5. Sundar Krishnan, Bing Zhou, Min Kyung An. (2019). *Smartphone Forensic Challenges*. *International Journal of Computer Science and Security (IJCSS)*, Volume (13) : Issue (5)
6. S. K. Reddy Mallidi and P. Palli. (2016). *A Comprehensive Analysis of Smartphone Forensics & Data Acquisitions*. *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 2, pp. 270-276, Feb. 216AD.
7. A. Aljahdali, N Alsaïdi, M Alsafrî (2021). *Mobile device forensics*. *Romanian Journal of Information Technology and Automatic Control*, Vol. 31, No. 3, 81-96, rria.ici.ro
8. SC Sathe, NM Dongre, (2018). *Data Acquisition Techniques in Mobile Forensics*. 2nd International conference on Inventive Systems and Control.