فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال ششم، شماره سه، پاییز 1401

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 مصاحبه‌صورت گرفت که پس از انجام مصاحبه‌ها، اشباع نظری حاصل شد. روش پژوهش این تحقیق، به‌صورت 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 هشت‌بُعد 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 درنهایت 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 فارنزیک، الزامات استنادپذیری، استنادپذیری ادله، ابزارهای فارنزیکی.

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

۱- مقدمه و بیان مسئله

گوشی‌های هوشمند طی دو دهه گذشته پیشرفت‌های فزاینده‌ایی را پشت سر گذاشته‌اند و ازآنجاکه 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 رسانه‌های 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 رسانه‌های اجتماعی به‌طور مداوم در حال افزایش است و این افزایش به دلیل برنامه‌های گوشی‌های هوشمند می باشد [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 درنتیجه جرائم سایبری از طریق SNAها ایجاد کنند. این برنامه‌ها همچنین می‌توانند برای زورگیری‌سایبری[3]، تعقیب[4]، آزار جنسی[5]، کلاهبرداری سایبری[6] و توهین[7] 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 SNA ها تبدیل شده‌اند. این مصنوعات جمع‌آوری شده کاربران و محققان را قادر می‌سازد تا PII[8] (اطلاعات قابل شناسایی شخصی) را که 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 قسمت های مختلف گوشی، از طریق ابزارهای مربوطه تمرکز دارند. چنین یافته‌های مصنوع می‌توانند عامل را با جرم رخ‌داده 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 چالش ها و الزامات مربوط به این موضوع از طریق مصاحبه با خبرگان و کارشناسان این امر پرداخته شود که نتیجه این بررسی ها منجر به ایجاد چارچوبی برای شناسایی الزامات استناپذیری خواهد شد سپس در چارچوب ایجاد شده میزان اهمیت هر یک از مولفه ها بدست می آید و نهایتا راهکارهایی برای دستیابی به الزامات مطرح شده بیان می شود.

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 می کند که با توجه به رویکرد رو به جلو و نگاه به آینده در بررسی مؤلفه های تأثیرگذار در استنادپذیری می توان زمینه و بستر مناسبی را جهت سیاست گذاری و تصمیم گیری های بلندمدت در زمینه دستیابی به این الزامات و تسهیل سازی فرآیند استنادپذیری ادله دیجیتالی فراهم آورد لذا می توان عنوان کرد این مهمترین دلیل بر اهمیت بسیار زیاد این علم نوظهور می باشد. علاوه بر این، می توان با مشخص کردن میزان اهمیت

[1] Law enforcement agencies
[2] Social networking apps
[3] Cyber bullying
[4] Stalking
[5] Sexual harassment
[6] Cyber scam
[7] Insults
[8] Personally identifiable information

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

هر یک مولفه های الزامات استنادپذیری ادله دیجیتال آماده سازی سازمان ها و جامعه را بر اساس اولویت‌دهی های از قبل مشخص شده معین کرد تا با تصمیم گیری های کوتاه مدت و اقدامات جهادی، درک زودهنگام 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 حوزهٔ جرائم سایبری رو به رشد در گوشی‌های تلفن همراه و به طبع آن استنادپذیری ادله دیجتالی استخراجی از گوشی‌های 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 نسبتا جدیدی است که برخی عبارات و مفاهیم را در خود جای داده که در ادامه بیان می شود.

2 - 1 - فارنزیک و دیجیتال فارنزیک[1]

فارنزیک در لغت به معنای پزشکی قانونی بوده اما مفهوم آن به جرم‌شناسی اشاره دارد و دیجیتال فارنزیک در اصطلاح به کلیه اقداماتی گفته می‌شود 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].

2 - 2 - فرایند استخراج ادله دیجیتال استنادپذیر از گوشی‌های تلفن همراه

مراحل استنادپذیری ادله دیجیتال برای جرائم و شواهد مختلف متفاوت می باشد ولی به‌صورت کلی می توان در 4 مرحله کلی بیان کرد: جمع‌آوری، استخراج، تجزیه‌وتحلیل و گزارشکه در شکل 1 نیز نشان داده شده است(موسسه ملی استاندارد و فناوری (NIST)[2])[5].

شکل 1) فرآیند تجزیه‌وتحلیل فارنزیک بر مبنای NIST [5]

مراحل مربوط به استخراج و آنالیز اطلاعات مهم‌ترین و موثرترین مرحله در فرایند استنادپذیری می باشد که روش‌های استخراج محتویات گوشی‌ها عبارت‌لند از: روش دستی[3]، منطقی[4]، فایل سیستم[5]، فیزیکی[6]، مبتنی بر تراشه[7].

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 نمی‌تواند اطلاعات حذف شده را بازیابی کند اما می‌تواند رکوردی از صفحه‌های مختلف و رابط کاربری ارائه دهد[4].

استخراج به روش منطقی: اکتساب‌های منطقی گوشی تلفن همراه شامل استخراج تمام داده‌هایی است که دستگاه قادر به دسترسی به آن در سیستم ذخیره‌سازی خود دارد. این روش قابلیت استخراج و تجزیه وتحلیل داده ها در حالت قفل نیز داشته و بر اساس اصل به دست آوردن کپی بیت به بیت از فضاهای اختصاص‌یافته کار

[1] Digital Forensic
[2] National Institute of Standards and Technology
[3] manual
[4] logical
[5] filesystem
[6] physical
[7] Chip off-based

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

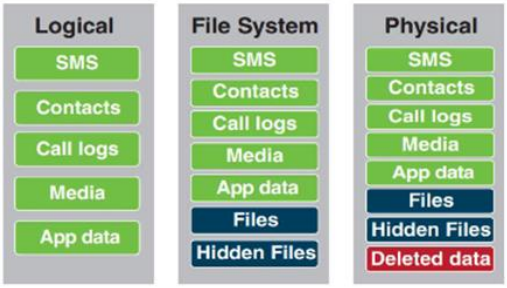
می‌کند و نمی‌توانند داده‌ها را از فضـــاهای شـــل بازیابی کنند لذا نمی‌توانند داده‌های حذف شده را به دست آورند [6].

استخراج به روش فایل سیستم: استخراج به روش فایل سیستم به بررســی عمیق ســاختار فایل می پردازد و بیشــتر زمانی مورد استفاده قرار می گیرد که کاربر قصـد دارد با استفاده از API های مرتبط، به فایل خاصی در حافظه داخلی گوشی دسترسی پیدا کند. این روش استخراج معمولاً به‌عنوان ابزار اصـلی استنادپذیری ادله اســتخراجی در بازیابی فایل‌های داده از حافظه داخلی مانند فایل‌های پایگاه‌داده، بررســی تاریخچه مرورگر وب، اســتفاده از برنامه و ... استفاده می شود[7].

اسـتخراج به روش فیزیکی: اکتسـاب فیزیکی شـامل کپی بیت به بیت از کل فضـــای ذخیره‌ســـازی فیزیکی اســـت و برای بازیابی اطلاعات حذف شـــده موثر بوده و برای کنترل کامل نیاز به دسترسی روت داشته که دستیابی به دسترسی روت باعث تغییراتی در داده‌های دســـتگاه می شـــود و نیاز به ســـخت‌افزار و نرم‌افزار تخصـصـی برای این منظور می باشـد[8]. در صـورت روت بودن گوشـــی، دســـترســـی‌های لازم به ابزارهای اســـتنادپذیری جهت اسـتخراج بیشـتر اطلاعات و بازیابی محتویات پاک‌شـده و ... داده می‌شود.

استخراج بر پایه تراشه: این روش شـامل برداشتن فیزیکی تراشـه حافظه فلش از گوشـــی تلفن هوشـــمند و آماده‌ســـازی آن برای دسـتیابی به داده‌های خام موجود در تراشـه با اسـتفاده از تراشـه خوان می باشد. این روش امکان ایجاد یک تصویر باینری از تراشه حافظه را برای بررسـی‌کنندگان فراهم می‌آورد. ریسـک اسـتفاده از این روش بالا بوده و ممکن اسـت دسـتگاه تلفن هوشـمند دیگر قابل استفاده نباشد[5].

در مطالعات صـــورت گرفته، نویســـندگان روش‌های مختلفی از جمع‌آوری داده‌هـای دخیـل در فـارنزیـک تلفن همراه را ارائـه کرده‌اند. با توجه به این مطالعات، مشـخص شـده اسـت که اگر داده‌ها برای تجزیه‌وتحلیل ســریع نیاز به بازیابی داشـته باشـند، تکنیک اکتسـاب دسـتی یا منطقی مناسـب اسـت. بااین‌حال، در صـــورت نیـاز بـه تجزیـه‌وتحلیـل دقیق و در مورد تلفن‌هـای آسیب‌دیده، تکنیک‌های فیزیکی یا مبتنی بر تراشـه مناسـب‌ترین و در عین حال زمان‌برترین روش ها می باشند. در شکل (2) تفاوت و شباهت نتایج روش های مختلف نشان داده شده است[8].



شکل 2) تفاوت نتایج روش های استخراج[8]

۳- پیشینهٔ تحقیق

بررسـی تحقیقات انجام شـده توسـط محققان قبلی نشـان می دهد کـــه در حوزهٔ به استنادپذیری ادله دیجیتال استخراجی مطالعات پراکنده ای انجام شده اسـت؛ لذا در رابطه با موضوع این پژوهش، برای بالا بردن منابع تحقیقاتی، علاوه بر تحقیقات قبلی صـــورت گرفته در حوزه اسـتنادپذیری ادله دیجیتال اسـتخراجی در مجلات، پایگاه های علمی و سایر تحقیقات صورت گرفته در دانشگاه ها و مراکز علمی به مصاحبه با خبرگان و کارشناسانی که در این حوزه کارهای عملی انجام داده اند نیز پرداخته می شود. 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 اســتنادپذیری ادله استخراجی

مؤلفین در مقاله [9] به آینده پژوهی اســتنادپذیری ادله دیجیتال جرائم ســایبری مبتنی بر اینترنت اشــیا پرداخته اند که در آن چارچوب اصــلی کار خود را در چهارعُد اصــلی اســتنادپذیری جرائم سایبری مرتبط با اینترنت اشیاء، آینده پژوهی جرائم اینترنت اشـــیاء، محدودیت ها و نواقص و ناامنی ها با 10 مؤلفه و 36 زیر مؤلفه ارائه کردند که بر اســـاس یافته های پژوهـــش، برای فائق آمدن بر چالش های اکتساب شده پیشنهادات ذیل را عنوان کردند؛ اتخاذ زود هنگام تـــدابیر لازم و تجهیـــز مراکز قضایی، انتظامی و آموزشی بـــرای شناسایی چالش ها و اقدامات صورت گرفته در سایر مراکز علمی، بالا بردن بنیـه علمی مراکز قضایی و انتظامی در حوزه کشـف جرائم با رویکرد آینده پژوهی با برگزاری مانورهای

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

اجرایی و ارزیابی اقدامات صورت گرفته، عقد قراردادهای بین المللی چند جانبه برای ارائه خدمات زیرساختی و جولبدهی 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 مقاله پیش رو مصاحبه‌های 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 برنامه‌های گوشی‌های تلفن همراه

مظاهری در پایان نامه خود [10] برای بررسی چالش های حوزه استنادپذیری ادله استخراجی از برنامه واتساپ گوشی‌های تلفن همراه آزمایشات مختلفی را بر روی 34 دستگاه گوشی تلفن همراه با نسخه‌های سیستم‌عامل متفاوت در حالات روت و غیر روت شده و نیز استفاده از برنامه‌های مختلف واتساپ با نسخه‌های متفاوت و روش‌های 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، watsapp key/DB extractor، whatsapp viewer 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 تقسیم‌بندی کرد:

۱- نقش نسخه‌های اندروید در فارنزیک واتساپ

بر اساس نتایج حاصل از آزمون‌های صورت گرفته می‌توان استنادپذیری ادله استخراجی از برنامه پیام‌رسان واتساپ را بر اساس تأثیر نسخه اندروید به دو دسته تقسیم نمود:

- فارنزیک گوشی‌های موبایل با نسخه‌های سیستم‌عامل اندروید هشت و پایین‌تر (صرف‌نظر از نوع رمزنگاری واتساپ)
- فارنزیک گوشی‌های موبایل با نسخه‌های سیستم‌عامل اندروید 9 و بالاتر

جدول 1) نتایج عملکرد فارنزیک 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 پایگاه‌داده در فارنزیک واتساپ

در بررسی‌های به عمل آمده مشخص گردید نسخه‌های رمزگذاری شده واتساپ تا نسخه crypt12، قابلیت استخراج کلید در گوشی‌های روت شده و غیر روت شده را داشته اما در مدل‌های crypt14 و با نسخه سیستم‌عامل اندروید 9 و بالاتر رمزگشایی پایگاه‌داده تقریباً مقدور نمی باشد.

۳- نقش روت بودن موبایل در نتیجه فارنزیک واتساپ

همان‌طور که از نتایج حاصل از آزمون‌ها به دست آمد، بیشترین اطلاعات استخراجی مربوط به گوشی‌های روت شده بود چراکه علاوه بر بازیابی و استخراج کلیه لاگ‌های واتساپ، استخراج کلید رمزگشایی و پایگاه‌داده واتساپ نیز در این مدل گوشی‌ها به نسبت گوشی‌های غیر روت محتمل‌تر می‌باشد.

٤- نقش فعال بودن پشتیبان‌گیری پایگاه‌داده واتساپ

پشتیبان‌گیری از پایگاه‌داده‌های واتساپ با توجه به پیشنهاد این برنامه می تواند در رمزگشایی و دستیابی به محتویات آن‌ها نقش به سزایی داشته باشد.

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

۴- روش شناسی تحقیق

برای انجام این تحقیق هم از مطالعـــــات کمی و هـــــم از مطالعـات کیفـی بـه عنـوان منبـع داده اسـتفاده شد. در این مرحله بـه بررسـی ایـده‌ها، رویکردهـا، نتـایج و یافته‌های پژوهش‌های کیفی و کمی پیشین با هدف طراحـی و توسعه چـارچوب مفهومی الزامـات اسـتنـادپـذیری ادلـه دیجیتـال استحراجی از گوشی‌های تلفن همراه پرداخته شده است و با برخورداری از نتایج یافته ها، می توان با اتخاذ تصـــمیمات درست و بهنگام، جهت حل مسائل و مشکلات استنادپذیری ادله دیجیتال در مواجهه با تهدیدات آینده تصـــمیمات و رویکردهای مناســـبی اتخاذ کرد لذا با توجه به اینکه هدف صـرفا بیان نظریه تئوری نمی باشـد، نوع تحقیق کاربردی و روش آن توصـیفی و از نوع پیمایشـی می باشـد و به‌صـورت ترکیبی در دو بخش کیفی و کمی و در ســـه گام انجام می شود که در شکل (3) به‌صورت مرحله به مرحله نمایش داده شده است.

شکل 3): فرایند تدوین الگوی مفهومی

در **گـام اول** این تحقیق ابتـدا بـه طور کیفی بـا روش مرور جامع به بررسـی کلیه مقالات و مطالعات موجود و سـوابق و اسـناد و مدارک مرتبط و مصـاحبه با خبرگان و افراد کلیدی در خصـــوص موضـــوع مولفه‌ها پرداخته شـــد و از روش مصاحبه نیمه ساختاریافته جهت گردآوری اطلاعات استفاده و قابلیت اعتماد مصـــاحبه‌ها نیز توســـط روش بازنگری متخصص بررسـی و مورد تأیید قرار گرفت و یک چارچوب مفهومی اولیه از این یافته‌ها بدسـت آمد که در شـکل (4) به نمایش گذاشته شده است.

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

در **گام دوم** تحقیق، با توجه به این که نظریه یا پژوهش‌های پیشین در رابطه با موضوع مورد بررسی بسیار ناقص بودند لذا محققین از روش کیفی با رویکرد نظرات خبرگان، متکی بر پژوهش‌های 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 سوالات پرسش نامه تهیه و تدوین گردید، چارچوب ثانویه و تکمیلی پژوهش، خروجی این مرحله می باشد که در شکل (5) قابل مشاهده می باشد.

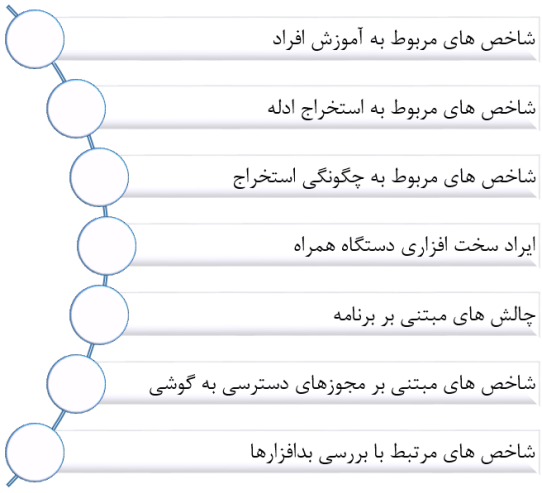
در **گام سوم** به منظور اعتبار سنجی کمی چارچوب تکمیلی، نظر خبرگان میانی که بصورت هدفمند انتخاب گردیده بودند گرفته شد و پس از تدوین پرسشنامه بر اساس چارچوب ثانویه، نسبت به بررسی روایی ابزار تحقیق از روایی محتوایی و برای بررسی پایائی ابزار تحقیق از روش آلفای کرونباخ استفاده شد. سپس عملیات جمع‌آوری اطلاعات از طریق پرسشنامه 66 سوالی با طیف لیکرت 5 سطحی در 8 بعد شاخص‌های مرتبط با بررسی بدافزارها، شاخص‌های مرتبط با آموزش افراد، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت‌افزاری دستگاه همراه، شاخص‌های مربوط به چگونگی استخراج و شاخص‌های مربوط به استخراج ادله با استفاده از مقیاس پایایی و روایی مورد بررسی قرار گرفت و نهایتا داده‌های 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.

۵- یافته های تحقیق و تجزیه‌وتحلیل آن‌ها

5 - 1 - تشریح پرسشنامه

بر اساس مطالعات کیفی انجام شده و بررسی مقالات و مطالعات موجود و سوابق و اسناد و مدارک نسبتا 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 هفت‌بُعد شاخص‌های مرتبط با بررسی بدافزارها، شاخص‌های مرتبط با آموزش افراد، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت‌افزاری دستگاه همراه، شاخص‌های مربوط به چگونگی استخراج و شاخص‌های مربوط به استخراج ادله قرار گرفتند(الگوی مفهومی پیشنهادی اولیه، نشان داده شده در شکل 4).

همان‌گونه 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 سوالات 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 گوشی‌های تلفن همراه

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

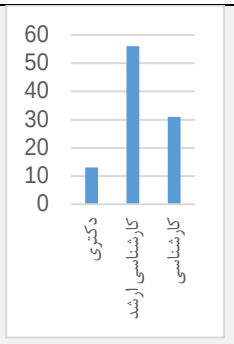
2 - 5 - سوالات جمعیت شناختی

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 خبره 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

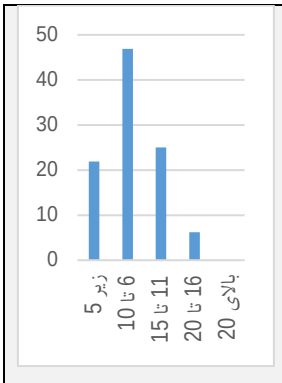
میزان تحصیلات نمونه آماری

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



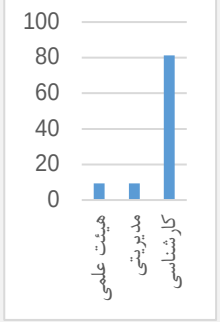
سابقه فعالیت نمونه آماری

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



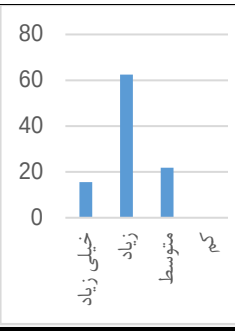
رده مسئولیتی نمونه آماری

رده مسئولیتی	فراوانی	درصد
عضو هیئت علمی	3	9.37
مدیریتی	3	9.37
کارشناسی	26	81.25
جمع	32	100



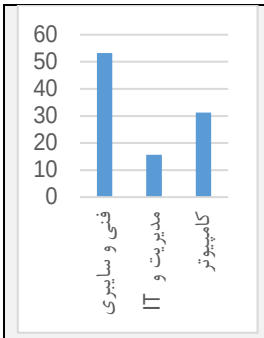
میزان آشنایی با موضوع نمونه آماری

میزان	فراوانی	درصد
خیلی زیاد	5	15.62
زیاد	20	62.5
متوسط	7	21.87
کم	0	0
جمع	32	100



رشته تحصیلی نمونه آماری

رشته	فراوانی	درصد
فنی و سایبری	17	53.125
مدیریت و IT	5	15.625
کامپیوتر	10	31.25
جمع	32	100



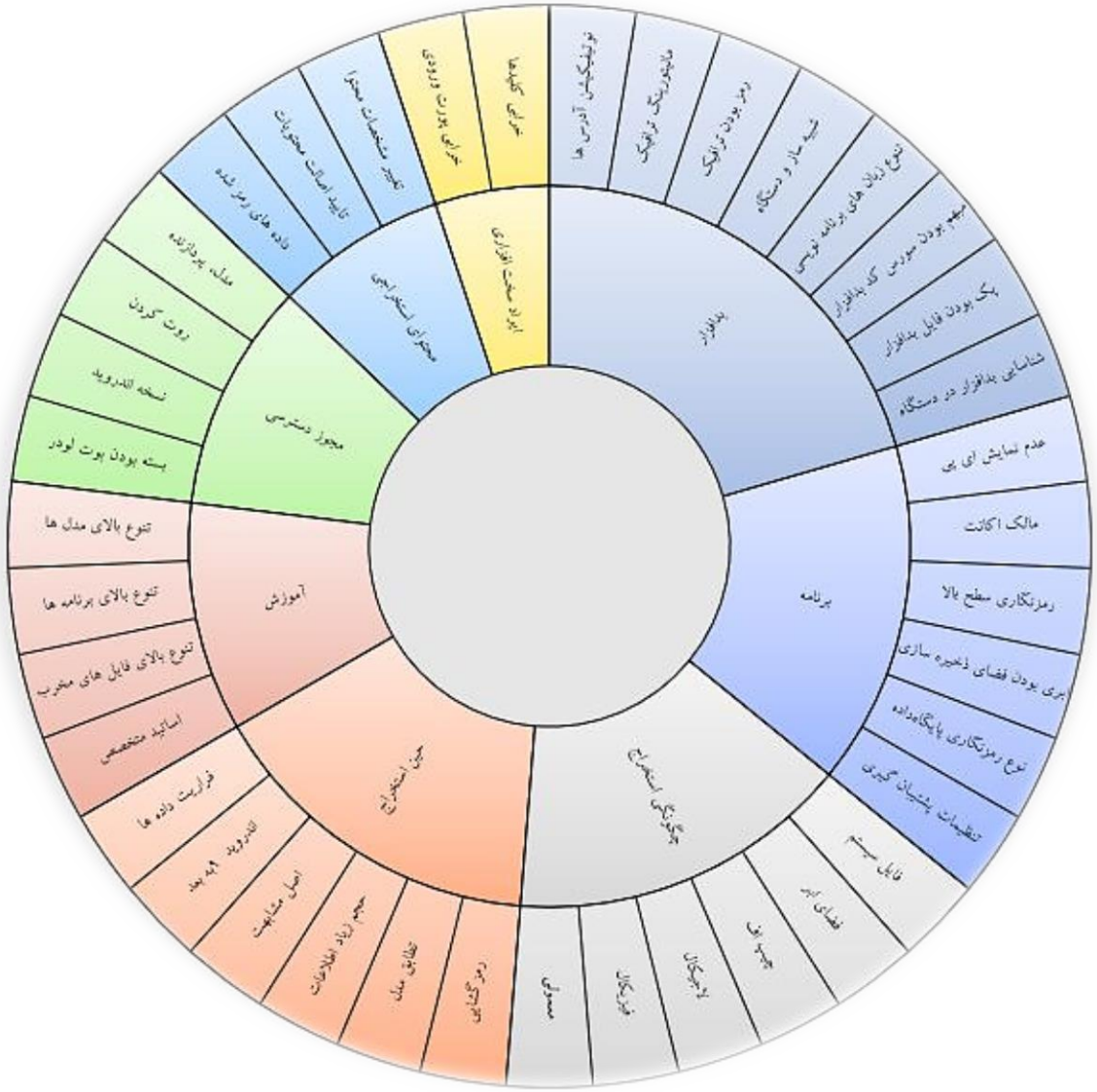
در جدول(2)، اطلاعات جمعیت‌شناختی کل خبرگان، مشتمل بر میزان تحصیلات، رشته تحصیلی، میزان آشنایی با موضوع تحقیق، سابقه یا سنوات خدمتی و رده مسئولیتی بیان گردیده است عنوان هر جدول بیانگر یکی از ویژگی های پرسش شوندگان بوده و مورد با بیشترین آمار به‌صورت خاص مشخص شده است.

3 - 5 - سوالات استنباطی تحقیق

لازم به یادآوری است که سوالات تحقیق 66 مورد در نظر گرفته شده که از طریق آن‌ها نظرات نخبگان میانی درباره شاخص‌های هر سؤال جمع‌آوری گردیده است. ابعاد و مولفه های مربوط به هرکدام از سوالات در جدول (3) آمده

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

است و با توجه به چارچوب مفهومی اولیه، چارچوب نهایی ذیل استخراج گردید که در شکل (5) به نمایش گذارده شده است(برای وضوح بیشتر نمودار از هر مولفه اصلی تنها برخی از زیر مولفه ها نشان داده شده است).



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 آن‌ها با کمک تعدادی از خبرگان و صاحب نظران استنادپذیری ادله دیجیتال موردبررسی قرار گرفت و در جهت رسیدن به یک پرسشنامه استاندارد، تغییرات لازم در آن‌ها 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 القاءکننده رعایت گردید. همچنین جهت اعتبار محتوایی پرسشنامه مواردی مانند اطمینان از برداشت یکسان از سؤالات، 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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

پرســـش‌نامه این تحقیق با محاســـبه آلفای کرونباخ، مورد سـنجش قرار گرفته اسـت. مقدار ضـریب آلفای کرونباخ کل 76.0 % به دســـت آمد که نشـــان دهنده وجود پایایی بالایی برای پرسشنامه می باشد(جدول 3).

جدول 3. پایایی جزئی پرسشنامه

متغیر	مـقـدار آلـفـای 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
چالش های 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

5 - 5 - تحلیل داده‌های استخراجی پرسش نامه‌ها

در تهیه سـوالات و شـاخص‌های پرسـش نامه از نقطه نظرات خبرگان در حوزه اسـتنادپذیری ادله دیجیتال اسـتفاده شـد که به روش نمونه گیری گلوله برفی از میان افراد خبره انتخاب شـدند. نحوه تکمیل پرسـشـنامه به این ترتیب بود که در ابتدا موضـــوع جهت مطالعه اولیه در اختیار خبرگان قرار می گرفت، سـپس خبرگان با توضـیحات حضـوری محقق و بر اساس مطالعه قبلی به مصاحبه پاسخ می دادند. پس از تکمیل مصـــاحبه با هر یک از خبرگان، فرد یا افراد دیگری را جهت مصـــاحبه انتخاب می گردید. انتخاب و مصـــاحبه با افراد تا جایی ادامه یافت که اشباع اطلاعاتی صورت گرفت و مفاهیم جدیدی برای تکمیل پرسـشـنامه ها مشاهده نشد، مصاحبه‌ها به‌صـــورت حضـــوری و مجازی با کارشـــناســـان و خبرگان استنادپذیری ادله دیجیتال طی جلسات مختلف انجام گردید. سپس به منظور اعتبارسنجی داده‌های جمع‌آوری شده در فاز بعدی از پرسـشـنامه استفاده شـد و نظرات هر یک از خبرگان در رابطه با اهمیت هر یک از الزامات اخذ گردید که در جدول (4) نتایج حاصـل از پرسـش نامه ها نشـان داده شـده است.

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

شاخص ها	مولفه ها	توصیف	میزان اهمیت (%)	رتبه
محتوای استخراج‌شده	تغییر مشخصات محتوا	تغییر ویژگی های فایل در اثر انتقال در بستر شبکه های اجتماعی؛ زمان ایجاد، زمان دسترسی و ...	78	3
	تایید اصالت محتویات	عملکرد ضـعیف ابزارهای تشـخیص اصـالت علی الخصـوص در فایل های چند رسانه ای	70	5
	داده‌های رمز شده	رمزنگاری پارتیشـن data از اندروید 7 به بعد که رمزگشـایی در پردازنده های جدید را بسیار مشکل می نماید	88	1
		داده ها و فایل های 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		
		عـدم انـالیز اتومـاتیـک محتوای شـــبکـه هـای اجتمـاعی بـه دلیـل رمزنگاری		

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

شاخص‌های مرتبط با آموزش افراد	تنوع بالای مدل ها	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	70	1
	تنوع بالای برنامه ها	آموزش و بررسی نکات کلیدی برنامه هم مشکل می باشد و هم زمانبر	55	4
	تنوع بالای فایل های مخرب	نیاز به مهارت و نفرات متخصص و متعدد می تولند جوابگوی تعداد بالای مخرب ها باشد	60	3
	اساتید متخصص	اساتید متخصص و بومی باید تربیت شوند	65	2
	روحیه اشتراک دانش	با توجه به انحصار طلبی و درآمدزایی بالا برخی از تکنیک ها و ترفندها آموزش داده نمی شوند	50	5
	درآمدزایی با دانش کم	با توجه به دانش کم هم بسیاری از کارشناسان کسب درامد می کنند لذا روحیه آموزش پذیری کمی دارند	45	6

پس از بررسی، الزامات استنادپذیری ادله دیجیتال استخراجی از گوشی‌های تلفن همراه در قالب هشت‌عُد ، شاخص‌های مرتبط با بررسی بدافزارها، شاخص‌های مرتبط با آموزش افراد، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت‌افزاری دستگاه همراه، شاخص‌های مربوط به چگونگی استخراج، شاخص‌های مربوط به ادله استخراج‌شده و شاخص‌های 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 جدول6):

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

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

جدول 6: مهم‌ترین چالش های استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های تلفن همراه

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

همان طور که در جدول (5) مشاهده می شود میانگین بار عاملی شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی مهم‌ترین الزام بوده که برای آینده‌نگری استنادپذیری گوشی‌های 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 سازمان‌های 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 **شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی** می باشد به عنوان مهم‌ترین الزام استنادپذیری ادله دیجیتالی استخراجی از گوشی‌های 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 گوشی‌های تلفن همراه باز کردن آن‌ها بیش از پیش سخت تر و بعضا غیر ممکن شده است.

6 - 5 - **تحلیل بلوغ بر مبنای** CMMI

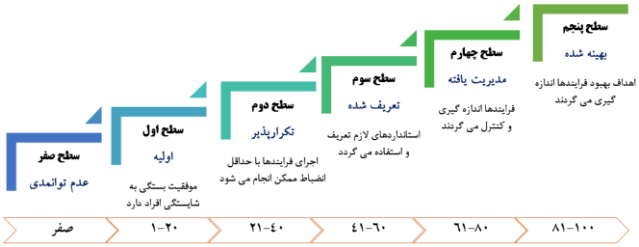
در این تحقیق مصاحبه در دو مرحله انجام گردید که در مرحله اول به منظور کشف مقوله های کلیدی و با طرح سوالات باز انجام شد و در مرحله دوم یک پرسشنامه نیمه ساختاریافته تهیه شد و به‌صورت حضوری و مجازی، توسط خبرگان تکمیل گردید. پرسشنامه آزمون خبرگی الگوی مفهومی پیشنهادی جهت اخذ تأییدیه خبرگان و تعیین میزان اهمیت 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، مصاحبه‌ها و مطالعات میدانی و همچنین تجزیه وتحلیل 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 آن‌ها 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 سطوع بلوغ در CMMI جایگاه کنونی یکی از سازمان‌های 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.

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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

بعد	میانگین نمره
شاخص‌های مربوط به آموزش افراد	67
شاخص‌های مربوط به محتوای استخراج‌شده	42
شاخص‌های مربوط به چگونگی استخراج	47
ایراد سخت‌افزاری دستگاه همراه	68
چالش های مبتنی بر برنامه	52
شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی	35
شاخص‌های مرتبط با بررسی بدافزارها	45
شاخص‌های مربوط به حین استخراج ادله	48



شکل 6. سطوح بلوغ در CMMI

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

شاخص‌های 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 گردد.

شاخص‌های مربوط به محتوای استخراج‌شده: بعد محتوای استخراج‌شده به اطلاعاتی دلالت دارد که در اختیار کارشناس برای بررسی قرار می گیرد، بعضا حتی اطلاعات بازیابی شده از گوشی به‌صورت تغییر یافته و یا رمز شده بوده و نمی توان از آن‌ها 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 حدودا تعریف شده و تقریباً استفاده می شود ولی با توجه به موارد بیان شده جای کار دارد.

شاخص‌های مربوط به چگونگی استخراج: شاخص چگونگی استخراج اشاره به روش های موجود برای بررسی گوشی‌های تلفن همراه دارد که در این بین روش منطقی، بهترین حالت استخراج اطلاعات از گوشی‌های تلفن همراه می باشد که در اغلب موارد نیاز به روت بودن گوشی نیز می باشد علاوه بر این باید دقت داشت که ابزارهای فارنزیکی 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 حدودا تعریف شده و تقریباً استفاده می شود.

الزامات مربوط به ایراد سخت‌افزاری دستگاه همراه: بعد چالش های سخت‌افزاری اشاره به ایراداتی دارد که در عملیات استنادپذیری ادله استخراجی از گوشی همراه نیاز است بعضا نیاز است گوشی به حالت ریکاوری مد و یا دانلودینگ مد برود که لازمه آن استفاده از کلیدهای ولوم، پاور و هوم است که بعضا در گوشی ها این موارد آسیب دیده است یا ایراداتی دیده می شود که هزینه تعمیر آن‌ها 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 آن‌ها 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 آن‌ها روبرو است بعضا حتی بعد از دسترسی به شواهدی مانند پایگاه داده برنامه، با توجه به رمزنگاری سطح بالای آن عملا نمی تواند از آن‌ها استفاده کند. برابر تحلیل

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره تقریبی 52 در سطح سوم بوده یعنی استانداردهای لازم حدودا تعریف شده و تقریباً استفاده می شود ولی با توجه به موارد بیان شده علی الخصوص 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 دسترسی هاست لذا در صورت نداشتن چنین دسترسی باید یا چنین دسترسی هایی 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 CMMIبا نمره 35 در سطح دوم بوده اجرای فرایندها با حداقل انضباط ممکن انجام می گردد.

شاخص‌های مرتبط با بررسی بدافزارها: شناسایی و بررسی بدافزارها با توجه به پیشرفت های صورت گرفته در حوزه هک و نفوذ، کار سخت و زمانبر بوده و بعضا این بدافزارها در سایر نرم افزارها گنجانده می شوند که در این صورت تشخیص بدافزارها مشکل تر نیز می شود و در مواقعی نیز بعد از شناسایی با توجه به رمز بودن ترافیک شبکه امکان بررسی بدافزارها با مشکلات خاص خود روبرو می باشد، 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 می گردد.

شاخص‌های مربوط به حین استخراج ادله: ممکن است در حین استخراج داده ها با چالش های مربوط به حفظ اصالت داده ها و یا با اعمال روش های مختلف برای دستیابی به اطلاعات، گوشی به تنظیمات کارخانه برگردد و اطلاعات همگی از بین روند با 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 می گردد.

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 تصمیم گیری ها، سیاست گذاری ها و برنامه ریزی ها در ساختار مدیریتی، آموزشی، پژوهشی و فناوری خواهد بود. لذا با وجود مراکز امنیتی انتظامی و قضایی در حوزه های استنادپذیری ادله دیجیتال در سطح کشور، می توان توسعهٔ تکنولوژیکی در مجموعهٔ برنامه ریزان و کارکنان این نهادها را انتظار داشت.

لذا یافته های مرتبط با **شاخص ها و الگوی های 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، همان طور که در جدول (5) مشاهده می شود 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 پرسش نامه ها و نظرات خبرگان راهکارهای دستیابی به الزامات مطرح شده در قالب هشت‌بُعد ، شاخص‌های مرتبط با بررسی بدافزارها، شاخص‌های مرتبط با آموزش افراد، شاخص‌های مبتنی بر مجوزهای دسترسی به گوشی، چالش های مبتنی بر برنامه، ایراد سخت‌افزاری 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 پیشنهاد ها 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، **پیاده سازی 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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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 استلنداردهای 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 آینده‌نگری 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 طبیعتا الزامات آن هم به طور متقابل، همواره با تغییر فناوری علی الخصوص در گوشی‌های 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 گوشی‌های تلفن همراه، با توجه به نتایج به دست آمده از تجزیه وتحلیل داده‌های جمع‌آوری شده، مورد تائید خبرگان قرار گرفت و با استناد به مطالب جمع‌آوری 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 گوشی‌های تلفن همراه، ارائه گردید.

دستیابی به الزامات آموزشی:

در حوزه آموزشی، دوره های آکادمیک مربوط به تعمیرات گوشی‌های تلفن همراه، استنادپذیری ادله دیجیتالی استخراجی از انواع گوشی‌های تلفن همراه، آموزش بررسی برنامه‌های مربوط به استنادپذیری ادله دیجیتال و ... به‌صورت 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.

- توسعهٔ دانش در زمینهٔ تجهیزات و امکانات سخت‌افزاری و نرم افزاری موردنیاز واحدهای استنادپذیر 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 آن‌ها به تغییر بینش کارکنان و ایجاد تعلق خاطر و دلبستگی آنان به سازمان و ارتقاء حس مسئولیت و مالکیت آن‌ها لازم است.

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

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 داده‌های رمز شده استخراجی و رمزگشایی آن‌ها 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 گوشی‌های تلفن همراه ولی با توجه به وجود تحریم های مختلف کشورمان، دستیابی به چنین ابزارهایی بعضا ممکن نمی باشد.
- برون سپاری عملیات رمزگشایی به شرکت هایی است که در این زمینه به‌صورت 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 فارنزیکی با انجام مراحل تست بر روی گوشی‌هایی که بدین منظور در نظر

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

گرفته شـده اسـت(جلوگیری از وایپ شـدن 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 می شـود در وهله اول نیازمند آموزش هایی می باشـد که بتواند چنین ایراداتی را برطرف سازد که بعضا هزینه تعمیرات گوشی‌های آسیب دیده بالا بوده و یا نیاز به تجهیزات و تجربه بالا می باشـد ادامه راهکارهای جزئی تر در این خصـوص بیان شـده است:

- آموزش کارشناسان برای انجام تعمیرات سطح پایین.
- دسترسی به تجهیزات تعمیراتی گوشی‌های تلفن همراه برای انجام تعمیرات مورد نیاز اسـتنادپـذیری ادله دیجیتال.
- برخی مواقع ریسک انجام تعمیرات توسط کارشناسان بالا بوده لذا پیشـنهاد می شـود چنین مواردی برون سپاری شده و توسط افراد متخصص بیرون از شرکت صورت گیرد.
- برون سـپاری تعمیرات تخصـصـی به علت بالا بودن هزینه تعمیرات و ریسـک 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 کـه مهم‌ترین آن‌هـا عـدم دسـترسـی به شـواهد موجود در برنامه ها با توجه به وجود رمز عبور در نرم افزارهای مختلف می باشـد که با توجه به رمز عبور دو مرحله بر مشکلات دسترسی به شواهد افزوده شده است شاید در حال حاضـر نتوان راهکار فنی برای این منظور در نظر گرفت ولی می توان امید داشـت که با راهکارهای غیر فنی و یا با گذر زمان بتوان بر این مشکلات فائق آمد. لذا می توان پیشنهادات زیر را در دستیابی به سایر الزامات برنامه‌های گوشی ها در نظر گرفت.

- بررسی راهکارهای غیر رسمی مطرح شده در اتاق ها و گروه های مجازی، در این خصـوص باید دقت داشـت که راهکارها در ابتدا بر روی سـیسـتم هایی که بدین منظور در نظر گرفته شده تست شود.
- استفاده از تکنیک های مهندسی اجتماعی برای دستیابی به اطلاعات برنامه‌های گوشی.
- اسـتفاده از ظرفیت شـرکت های سـازنده نرم افزار با توجه به اهمیت موضوع.
- بررسـی کامل برنامه ها و بررسـی شـواهد به جای مانده از آن‌ها در گوشی‌های تلفن همراه.

دستیابی به الزامات بررسی بدافزارها:

اولین و مهم‌ترین مرحله در بررسـی بدافزارها شـناسـایی آن‌ها می باشـد که معمولا با کمک شـواهد موجود انجام چنین عملی ممکن می گردد لذا برای استنادپذیری شـواهد دیده شـده در گوشـی‌های تلفن همراه علاوه بر بررسـی های اسـتاتیک و پویا باید به مرحله شـناسـایی بدافزار هم دقت کافی داشـت، پیشـنهادات زیر جهت دسـتیابی به الزامات اسـتنادپذیری بدافزارهای دیده شـده در گوشی‌های تلفن همراه در نظر گرفته شده است:

- با توجه به نیاز فایل بدافزار برای بررسی در بسیاری از موارد دیده شـده قربانی بعد از احسـاس وجود بدافزار در گوشـی خود کلیه نرم افزارهای موجود را حذف می کند و یا به حالت کارخانه بر می گردانند که در این صورت کلیه شواهد لازم برای بررسی پاک شده و نمی توان آن را بررسـی کرد، لذا لازم اسـت آموزش های لازم در این خصوص داده شود.
- با توجه به اینکه بدافزارها در دوره های زمانی پیشرفت کرده اند باید راه های بررسی آن‌ها نیز پیشرفت کند لذا مطالعه مستمر و شرکت در دوره های بدافزار نویسی و بررسـی و آموزش راه های مقابله با بدافزارها لازم و ضروری می باشد.
- با توجه به اینکه اطلاعات اسـتخراجی از باج افزارها و بدافزارها به‌صورت رمز شده اغلب یافت می شوند لذا دستیابی به کلید رمزگشایی از اهمیت بالایی برخوردار است که بعد از مدتی شرکت های معتبر بین المللی در زمینه امنیت رایانه ها کلیدهای برخی از باج افزارها و بـدافزارهـا را انتشـار می کننـد کـه می توانـد برای رمزگشایی اطلاعات به کار رود. لذا بررسی سایت های معتبر بین المللی در این زمینه می تواند مثمرثمر باشد.

با توجه به موارد بیان شـده و لزوم بررسـی الزامات اسـتنادپذیری ادله اسـتخراجی از گوشـی تلفن همراه لازم اسـت مراکزی با محوریت آینده پژوهی برای اسـتنادپذیری توسـط مبادی ذی ربط مانند سازمان‌های قضایی و ... ایجاد گردد که برای این مهم می توان

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]

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 سخت‌افزاری، 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 Alsaidi, M Alsafri (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.

۹. سهلانی حسین، (1400)، "آینده پژوهی استنادپذیری ادله دیجیتال جرائم سایبری مبتنی بر اینترنت اشیا". فصلنامه علمی- پژوهشی فرماندهی و کنترل; ۵ (۳) :۳۸-۲٤.

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

[Downloaded from mail.ic4i-journal.ir on 2026-06-22]