استاندارد ملی ایران – ایزو
آی ای سی
۲۷۰۴۲
چاپ اول
۱۳۹۵

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standards Organization

INSO-ISO-IEC
27042
1st.Edition
2016
Identical with
ISO/IEC 27042: 2015

فناوری اطلاعات-
فنون امنیتی- راهنماهایی برای تحلیل و تفسیر شواهد رقمی (دیجیتالی)

Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

ICS: 35.040

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها واسط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و الزامات خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تحلیل و تفسیر شواهد رقمی (دیجیتالی)»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
دوست‌محمدی، وحید (کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی افتا
محمدیان، بهزاد (فوق لیسانس مهندسی برق)	کارشناس مرکز مدیریت راهبردی افتا
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

جوادزاده، غزاله

(کارشناسی ارشد مهندسی کامپیوتر)

پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

مغانی، مهدی

(فوق لیسانس ریاضی کاربردی)

کارشناس تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

ویراستار:

قسمتی، سیمین

(کارشناسی ارشد مهندسی فناوری اطلاعات)

مشاور مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تحلیل و تفسیر شواهد رقمی (دیجیتالی)» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و سی‌امین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۰۳/۰۸ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ISO/IEC 27042: 2015, Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

مقدمه

عمومی

این استاندارد ملی راهنمایِ هدایت تحلیل و تفسیر شواهد بالقوه رقمی (دیجیتالی) را ارائه می کند تا شواهد رقمی‌ای را که می‌تواند برای فهم رخداد کمک کنند، شناسایی و ارزشیابی کند. طبیعتِ داده‌ها و اطلاعاتی که شواهد بالقوه رقمی را می‌سازند به طبیعتِ رخداد و منابع شواهد رقمیِ درگیر در رخداد بستگی خواهد داشت.

هنگام استفاده از این استاندارد، کاربر فرض می‌کند که راهنماهای ارائه شده در استانداردهای ISO/IEC 27035-2 و ISO/IEC 27037:2012 پیروی شده است تمامی فرایندهای به کار رفته، با راهنماهای ارائه شده در استانداردهای ISO/IEC 27043:2015 و ISO/IEC 27041 سازگار است.

درباره این استاندارد ملی

این استاندارد ملی در پی ارائه تضمینی است که فرایند بررسی استفاده شده برای رخدادهای تحت بررسی و نتایج مورد نیاز مناسب باشد. همچنین به طور خلاصه مفهوم فرایندهای شکستن ظاهر پیچیده به مجموعه-ای از بخش‌های تفکیک ناپذیرکوچک‌تر، را که توصیه می‌شود به توسعه روش‌های بررسی ساده و در عین حال قوی کمک کند، تشریح مینماید. توصیه می‌شود این مورد به وسیله هر شخص صاحب اختیار، یا کسی که دستورالعمل می‌دهد، مدیریت می‌کند یا بررسی را هدایت می‌کند در نظر گرفته شود. توصیه می‌شود پیش از هر بررسی در زمینه اصول و فرایندها (تعریف شده در استاندارد ISO/IEC 27043:215) و آماده-سازی و طرح (تعریف شده در استاندارد ISO/IEC 27035-2) برای اطمینان از مناسب بودن روش‌های استفاده شده در فرایندهای بررسی تشریح شده در استانداردهای ISO/IEC 27037:2012 و ISO/IEC 27042:2015 به کار رود.

رابطه با سایر استانداردها

این استاندارد ملی در نظر دارد سایر استانداردها و اسنادی که راهنمایی در مورد بررسی و آماده‌سازی بررسی رخدادهای امنیتی اطلاعات ارائه می‌دهند را تکمیل کند. این یک راهنمایی جامع نیست اما اصول بنیادی معینی را وضع می‌کند که در نظر دارند از ابزار، فنون، و روش‌های انتخاب شده مناسب اطمینان حاصل کند و نشان دهد برای هدف نیاز به وجود آمده مناسب هستند.

همچنین این استاندارد ملی در نظر دارد تصمیم‌گیرندگانی که نیاز به تعیین قابلیت اطمینان شواهد رقمی دارند را آگاه سازد. این استاندارد برای سازمان‌هایی که نیاز به حفاظت، تحلیل و ارائه شواهد رقمی بالقوه دارند کاربردپذیر است. این استاندارد مربوط به نهادهای تعیین‌کننده خط مشی است که روش‌های اجرایی مربوط به شواهد رقمی، اغلب به عنوان بخشی از نهاد بزرگ‌تر شواهد را ایجاد و ارزیابی می‌کنند.

این استاندارد ملی قسمتی از فرایند جامع بررسی را تشریح می‌کند که شامل نواحی موضوعی زیر است اما به این‌ها محدود نمی‌شود:

- مدیریت رخداد شامل آماده‌سازی و طرح برای بررسی

- اداره کردن شواهد رقمی
- استفاده از، موارد ناشی از، ویرایش
- سامانه‌های آشکارسازی و جلوگیری از نفوذ شامل اطلاعاتی که می‌تواند از این سامانه‌ها به دست آید.
- امنیت ذخیره‌سازی شامل پاکسازی ذخیره‌ساز
- اطمینان از مناسب بودن روش‌های بررسی برای هدف
- انجام تحلیل و تفسیر شواهد رقمی
- درک اصول و فرایندهای بررسی شواهد رقمی
- مدیریت رویداد رخداد امنیتی شامل اشتقاق شواهد از سامانه‌های شامل شده در مدیریت رویداد رخداد امنیتی
- رابطه بین اکتشاف الکترونیکی و سایر روش‌های بررسی مانند استفاده از فنون اکتشافات الکترونیکی در سایر بررسی
- حاکمیت بررسی شامل بررسی قانونی[1]

به این نواحی موضوعی در قسمتی از استانداردهای ISO/IEC زیر پرداخته شده است:

– استاندارد ISO/IEC 27037:2012

این استاندارد ملی وسایلی که در مراحل اولیه بررسی شامل پاسخ اولیه، استفاده می‌شوند را تشریح می‌کند و می‌تواند اطمینان یابد که شواهد رقمی بالقوه مناسب گرفته شده‌اند تا به بررسی اجازه دهد به طور مناسب انجام شوند.

– استاندارد ISO/IEC 27038:2014

برخی اسناد می‌توانند حاوی اطلاعاتی باشند که نباید برای برخی نهادها فاش شود. اسناد اصلاح شده می‌توانند بعد از پردازش مناسب سند اصلی به این نهادها داده شوند. فرایند حذف اطلاعاتی که نباید فاش شود «ویرایش» نام دارد.

ویرایش رقمی اسناد منطقه نسبتاً جدیدی از عملیات مدیریت سند است که مخاطره‌های بالقوه و موضوعات منحصر به فردی را بالا می‌برد. در جایی که اسناد رقمی ویرایش شده‌اند، اطلاعات حذف شده نباید قابل بازیابی باشد. بنابراین باید مراقب بود اطلاعات ویرایش شده به طور دائمی از سند رقمی حذف شوند (مثلاً نباید به سادگی در قسمت غیرقابل نمایشی سند پنهان شود).

ISO/IEC 27038:2014 روش‌هایی برای ویرایش رقمی اسناد رقمی مشخص کرده است. همچنین الزاماتی برای نرم‌افزاری که برای ویرایش استفاده می‌شود را مشخص کرده است.

– استاندارد ISO/IEC 27040:2015

این استاندارد ملی جزئیات راهنمایی فنی در مورد اینکه چگونه یک سازمان می‌تواند سطح مناسبی از کاهش مخاطره را به وسیله به کارگیری یک رویکرد اثبات شده و سازگار در طرح، طراحی، سندسازی، و پیاده‌سازی

1- Forensic

امنیت ذخیره‌سازی داده تعریف کند، را فراهم می‌کند.
امنیت ذخیره‌سازی در حفاظت (امنیت) از اطلاعاتی که ذخیره شده‌اند و در امنیت اطلاعات منتقل شده در بین پیوندهای ارتباطات همبسته با ذخیره‌سازی به کار می‌رود. امنیت ذخیره‌سازی شامل امنیت افزاره‌ها و رسانه، امنیت فعالیت‌های مرتبط با افزاره‌ها و رسانه، امنیت برنامه‌های کاربردی و خدمات، و امنیت مرتبط با کاربران نهایی در طی طول عمر افزاره‌ها و رسانه و بعد از پایان استفاده از آن‌ها می‌باشد.
راه‌کارهای امنیتی مثل رمزنگاری و پاکسازی می‌توانند بر توانایی فرد در بررسی به وسیله‌ی معرفی راه‌کار مبهم و تاریک تأثیر گذارد. آن‌ها باید پیش از انجام بررسی یا در طی آن در نظر گرفته شدند. همچنین آن‌ها می‌توانند در حصول اطمینان از اینکه ذخیره‌سازی مواد مدرکی در طی بررسی و بعد از آن به طور مناسب آماده و امن شده‌اند، اهمیت داشته باشد.

- استاندارد ISO/IEC 27041:2015

نشان دادنِ مناسب بودن روش‌ها و فرایندهای استقراریافته در هنگام بررسی، اهمیت دارد.
این استاندارد ملی راهنماهایی را ارائه می‌کند. این راهنماها، چگونگیِ تضمین روش‌ها و فرایندها برای برآورده ساختن الزامات بررسی و همچنین مورد آزمون قرار گرفتن مناسب آن‌ها را ارائه می‌کند.

- استاندارد ISO/IEC 27043:2015

این استاندارد ملی اصول و فرایندهای کلیدی رایج و متضمن بررسی رخداد را معرفی کرده و الگو چارچوبی برای تمام مراحل بررسی فراهم می‌کند.
همچنین پروژه‌های ISO/IEC زیر نواحی موضوعی شناسایی شده در بالا را نشانی می‌دهند و می‌توانند منجر به انتشار استانداردهای مرتبط بعد از انتشار این استاندارد ملی شوند.

- استاندارد ISO/IEC 27035 (تمام قسمت‌ها)

این استاندارد ۳ قسمت دارد که رویکرد طرح و ساختاربندی شده به منظور مدیریت رخدادهای امنیتی برای سازمان‌ها فراهم می‌کند. این استاندارد از موارد زیر تشکیل شده است:

- استاندارد ISO/IEC 27035-1

این قسمت مفاهیم پایه و مراحل مدیریت رخداد امنیت اطلاعات را ارائه می‌دهد. این قسمت مفاهیم فوق را با اصولی در رویکرد ساختاربندی شده برای کشف، گزارش، ارزیابی، پاسخ و به کارگیری درس‌های آموخته شده ترکیب می‌کند.

- استاندارد ISO/IEC 27035-2

این قسمت مفاهیمی درباره طرح و آماده‌سازی پاسخ به رخداد ارائه می‌کند. مفاهیم شامل طرح و خط مشی مدیریت رخداد، تأسیس گروه پاسخگویی به رخداد، و جلسه آموزش آگاهی هستند و براساس مرحله طرح و آماده‌سازی الگو ارائه شده در استاندارد ISO/IEC 27035-1 می‌باشند. این قسمت مرحله «درس‌های آموخته شده» مدل را هم پوشش می‌دهد.

- استاندارد ISO/IEC 27035-3

این قسمت شامل مسئولیت‌ها و فعالیت‌های پاسخگویی به رخداد عملیاتی کارکنان در بین سازمان است. تمرکز ویژه‌ای به فعالیت‌های گروه پاسخگویی رخداد مثل پایشگری، اکتشاف، تحلیل و فعالیت‌های پاسخ-

گویی برای داده جمع‌آوری شده یا رخدادهای امنیتی اختصاص یافته است.

- استاندارد ISO/IEC 27044

این استاندارد رهنمودهایی برای سازمان‌ها در آماده‌سازی برای استقرار امنیت اطلاعات و سامانه‌ها/فرایندهای مدیریت رویداد ارائه می‌کند. مخصوصا، به انتخاب، استقرار و عملیاتِ SIEM می‌پردازد. این استاندارد قصد دارد به طور خاص برای برآورده شدن الزامات استاندارد ISO/IEC 27001 با توجه به پیاده‌سازی رویه‌ها و دیگر واپایش‌هایی که قابلیت توانمندسازیِ آشکارسازی و پاسخ به رخدادهای امنیتی دارند، کمک کند. این استاندارد قصد دارد پایش را اجرا و رویه‌ها را بازنگری کند تا تلاش‌ها و موفقیت‌های رخدادها و نقض‌های امنیتی را شناسایی کند.

- استاندارد ISO/IEC 27050 (تمام قسمت‌ها)

این استاندارد به فعالیت‌هایی در اکتشاف الکترونیکی می‌پردازد که شامل شناسایی، حفظ، جمع‌آوری، پردازش، مرور کلی، تحلیل و تولید الکترونیکی اطلاعات ذخیره شده[1] (ESI) می‌باشد اما محدود به آن‌ها نیست. به علاوه راهنمایی در اندازه‌گیری به دست آمده از تولید اولیه ESI از طریق وضعیت نهایی آن، که سازمان می‌تواند برای کاهش مخاطره و هزینه متقبل شود را فراهم می‌کند. توصیه می‌شود اکتشاف الکترونیکی به یک موضوع تبدیل گردد. این استاندارد به کارمندان فنی و غیرفنی شامل شده در برخی یا تمام فعالیت‌های اکتشاف الکترونیکی مرتبط است. یادآوری این نکته اهمیت دارد که این راهنمایی قصد تناقض یا جایگزینی با قوانین قضایی محلی و آیین نامه‌های تنظیمی را ندارد.

اکتشاف الکترونیکی اغلب به عنوان راه‌انداز بررسی، مانند فعالیت‌های اداره کردن و کسب شواهد خدمت عمل می‌کند، به علاوه گاهی حساس بودن و بحرانی بودن داده حفاظت‌هایی مانند امنیت ذخیره‌سازی در برابر نقض داده‌ها را ضروری می‌کند.

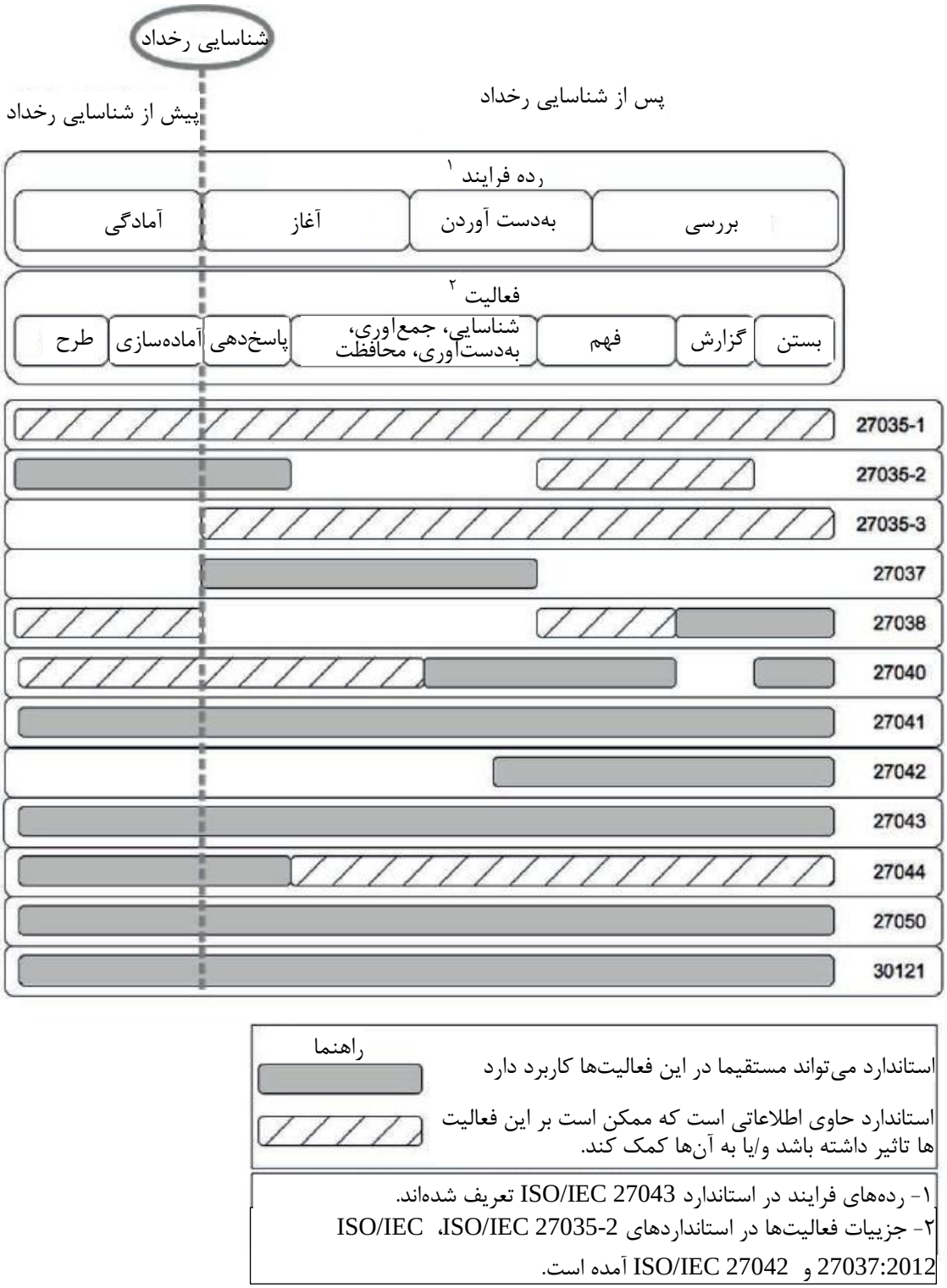
- استاندارد ISO/IEC 30121:2015

این استانداردهای چارچوبی برای نهادهای حاکمیت سازمان‌ها (شامل مالکان، اعضای هیئت مدیره، مدیران، شرکاء، مدیران ارشد یا مشابه) در بهترین حالت برای آماده‌سازی سازمان در بررسی رقمی قبل از رخداد آن فراهم می‌کند. این استاندارد ملی در توسعه فرایندهای (و تصیمات) راهبردی مرتبط با نگهداری، در دسترس بودن، و مقرون به صرفه بودن افشاء شواهد رقمی به کار می‌رود. این استاندارد ملی برای تمام انواع و اندازه-های سازمان کاربردپذیر است. استاندارد ملی درباره آماده‌سازی راهبردی محتاط برای بررسی رقمی یک سازمان است. اعلام آمادگی قانونی اطمینان می‌یابد که یک سازمان آماده‌سازی راهبردی مرتبط و مناسب برای پذیرش رخدادهای بالقوه یک ماهیت مدرکی دارد. ممکن است فعالیت‌ها به عنوان نتیجه نقض امنیت اجتناب ناپذیر، کلاهبرداری و ادعای شهرت رخ دهد. در هر وضعیتی فناوری اطلاعات (IT) باید برای بیشینه کردن تأثیر در دسترس بودن شواهد و مقرون به صرفه بودن به طور راهبردی گسترده شود.

شکل۱ فعالیت‌های نوعی پیرامون یک رخداد و بررسی آن را نشان می‌دهد. اعداد نشان داده شده در این

1- Electronically Stored Information

نمودار (مثل ۲۷۰۳۷) استانداردهای فهرست شده در بالا را مشخص می‌کنند و خط تیرها آنچه بیشتر کاربردپذیری مستقیم دارد یا تأثیری روی فرایند بررسی می‌گذارد را نشان می‌دهند (مثل تنظیم خط مشی یا ایجاد محدودیت‌ها). به هر حال توصیه می‌شود تمام آن‌ها پیش از مراحل طرح و آماده‌سازی رایزنی شوند. طبقات فرایند نشان داده شده به طور کامل در این استاندارد ملی تعریف شده‌اند و فعالیت‌های شناسایی شده مطابق با فعالیت‌های مطرح شده با جزئیات در استانداردهای ISO/IEC 27035-2 و ISO/IEC 27037:2012 می‌باشند.



شکل ۱- کاربست‌پذیری استانداردها در رده‌ها و فعالیت‌های فرایند بررسی

فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تحلیل و تفسیر شواهد رقمی (دیجیتالی)

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین راهنماهایی در زمینه تحلیل و تفسیر شواهد رقمی(دیجیتالی) است، به‌نحوی‌که به موضوعات تداوم[1]، اعتبار[2]، قابلیت‌بازتولید[3] و تکرارپذیری پرداخته شود. این استاندارد، بهروش‌هایی[4] را برای انتخاب، طراحی و اجرای فرایندهای تحلیلی و ثبت اطلاعات کافی به صورت یک‌جا مطرح می‌کند تا امکان دهد، درصورت نیاز، چنین فرایندهایی مورد وارسی مستقل قرار گیرند. همچنین، در مورد سازوکارهای مناسب جهت نشان دادن تخصص و شایستگی گروه بررسی، راهنماهایی را ارائه می‌کند.

تحلیل و تفسیر شواهد رقمی (دیجیتالی) می‌تواند فرایند پیچیده‌ای باشد. در برخی شرایط، روش‌های مختلفی می‌توانند به کار گرفته شوند و از اعضای گروه بررسی خواسته می‌شود که انتخاب یک فرایند خاص را توجیه کنند و نشان دهند چگونه این فرایند معادل فرایند دیگری است که توسط دیگر ماموران بررسی استفاده شده است. در شرایط دیگر، ممکن است لازم باشد ماموران بررسی روش‌های جدیدی را که قبلا مورد نظر نبوده‌اند، برای آزمون شواهد رقمی ابداع کنند. توصیه می‌شود ماموران بررسی نشان دهند که این روش تولید شده «مناسب برای هدف» است.

استفاده از یک روش خاص، می‌تواند روی تفسیر شواهد رقمی پردازش‌شده توسط آن روش، تاثیر بگذارد. شواهد رقمی دردسترس می‌تواند روی انتخاب روش‌هایی برای تحلیل بیشتر شواهد رقمی که تاکنون به‌دست‌آمده‌اند، تاثیر بگذارد.

این استاندارد ملی، برای عناصر تحلیلی و تفسیریِ ساماندهی رخدادهای امنیتی سامانه‌های اطلاعاتی، چارچوبی رایج را فراهم می‌آورد که می‌تواند جهت کمک در زمینه اجرای روش‌های جدید و فراهم آوردن یک استاندارد رایجِ کمینه برای شواهد رقمی تولیدشده از چنین فعالیت‌هایی، استفاده شود.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

1- Continuity
2- Validity
3- Reproducibility
4- Best practices

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سامانه‌های (سیستم‌های) مدیریت امنیت اطلاعات مرور کلی و واژگان

۲-۲ استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، فناوری اطلاعات -فنون امنیتی -راهنماهایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی (دیجیتال)

2-3 ISO/IEC 27041, Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف استاندارد ملی ایران شماره ۲۷۰۰۰ سال:۱۳۹۴، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

تحلیل[1]

ارزشیابی[2] *شواهد رقمی بالقوه* (۳-۱۵)، جهت ارزیابی[3] ارتباط آن با بررسی است.

یادآوری ۱- در صورتی که مرتبط بودن *شواهد رقمی بالقوه* (۳-۱۵) تعیین شود، به *شواهد رقمی* (۳-۵) تبدیل شوند.

یادآوری ۲- همچنین به شکل ۲ مراجعه شود.

۳-۲

کارخواه[4]

شخص یا سازمانی که به نمایندگی از او، بررسی صورت می‌گیرد.

1- Analysis
2- Evaluate
3- Assess
4- Client

۳-۳

شایستگی[1]

توانایی به کارگیری دانش و مهارت‌ها برای دستیابی به نتایج مورد نظر است.
[بند ۳-۷ ISO/IEC 17021:2011]

۴-۳

یادداشت‌های هم‌زمان[2]**/ سابقه هم‌زمان**[3]

سابقه مکتوب از اقدامات و تصمیمات، که هم‌زمان با اقدامات و تصمیمات، یا تا آن‌جا که ممکن است بلافاصله بعد از آن‌ها صورت می‌گیرد.

یادآوری ۱– در بسیاری از حوزه‌های قضایی، لازم است که یادداشت‌های هم‌زمان، در دفاتر یادداشت شواهد و با دست و به‌صورت پاک نشدنی نوشته شوند تا به قابل قبول بودن و رد نشدن یادداشت‌ها کمک شود.

۵-۳

شواهد رقمی[4]

اطلاعات یا داده‌های ذخیره شده یا انتقال داده شده در قالب دودویی، که از طریق فرایند تحلیل، مرتبط با بررسی تشخیص داده شده‌اند.

یادآوری ۱- توصیه می‌شود شواهد رقمی، با شواهد رقمی قانونی (۳-۱۴) یا شواهد رقمی بالقوه (۳-۱۵) اشتباه گرفته نشوند.

یادآوری ۲- همچنین به شکل ۲ مراجعه شود.

[منبع: استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، ۳-۵، تغییر داده شده است. – یادآوری‌های ۱ و ۲ اضافه شده‌اند، به‌منظور تشخیص بین شواهد مربوط به رخداد تحت بررسی و دیگر اطلاعات یا داده‌های غیر مرتبط، تعریف، سازگارتر شده است.]

۶-۳

همانندسازی[5]

تقلید درست، یا اجرا به همان صورتی که برنامه یا محیط دیگری اجرا می‌کند.

1- Competence
2- Contemporaneous notes
3- Contemporaneous record
4- Digital evidence
5- Emulate

۷-۳

آزمودن[1]

مجموعه‌ای از فرایندها، که به‌منظور شناسایی و بازیابی شواهد رقمیِ بالقوه‌ی مرتبط از یک یا چند منبع دیگر، مورد استفاده قرار می‌گیرند.

۸-۳

ایجاد ابهام در شواهد[2]

تاثیر عملیات انجام‌شده روی شواهد رقمی بالقوه که باعث می‌شود شواهد رقمی، به نحوی پنهان و یا مبهم شوند.

یادآوری ۱- این ابهام می‌تواند نتیجه یک کنش عمدی یا غیرعمدی باشد و ممکن است باعث آسیب‌گری شواهد رقمی شود یا نشود.

۹-۳

تفسیر[3]

ترکیبی از توضیحات در حدود مورد توافق، برای اطلاعات واقعی در مورد شواهد است. این اطلاعات، از مجموعه‌ای از آزمودن‌ها و تحلیل‌ها که بررسی را پدید می‌آوردند، نتیجه می‌شوند.

۱۰-۳

بررسی[4]

به کارگیری آزمودن‌ها، تحلیل‌ها، و تفسیر، برای کمک به فهم یک رخداد است.

۱۱-۳

رهبر بررسی[5]

فردی که بررسی را در سطحی راهبردی رهبری می‌کند.

1- Examination
2- Evidence obfuscation
3- Interpretation
4- Investigation
5- Investigative lead

۱۲-۳

گروه بررسی[1]

تمامی افرادی که به‌طور مستقیم در انجام بررسی دخیل هستند.

۱۳-۳

بررسی‌کننده[2]

عضو گروه بررسی، شامل *رهبر بررسی* (۳-۱۱) است.

۱۴-۳

شواهد رقمی قانونی[3]

آن نوع از *شواهد رقمی* (۳-۵) که در یک فرایند قضایی مورد قبول واقع شده‌اند.

یادآوری ۱- همچنین به شکل ۱ مراجعه شود.

۱۵-۳

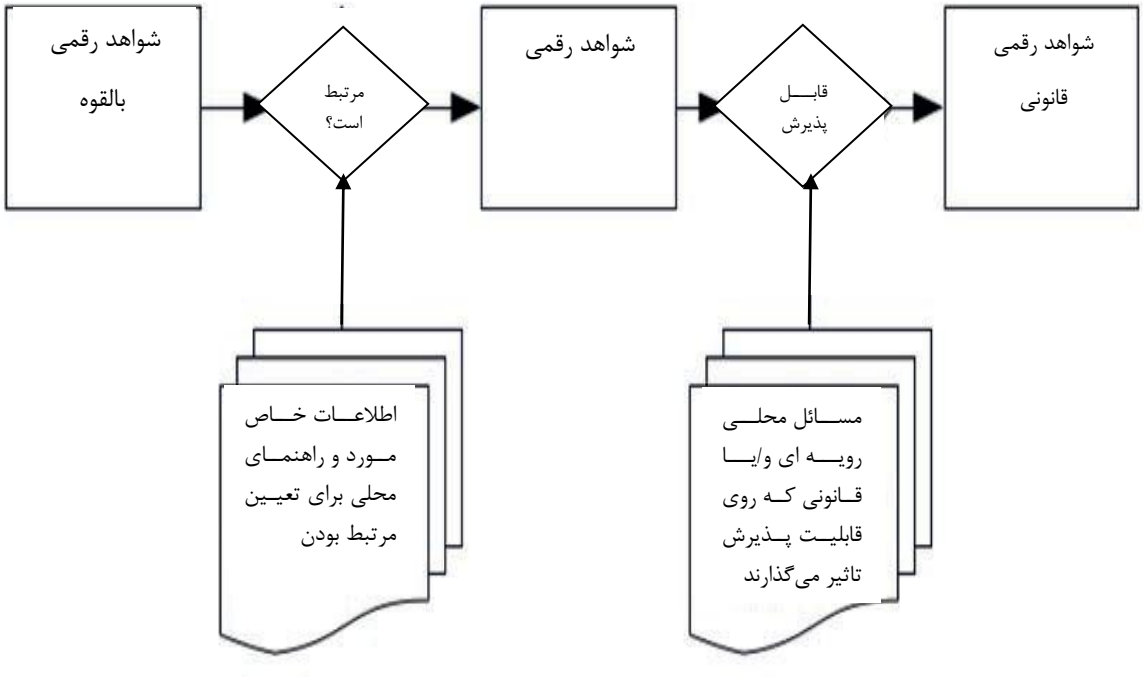
شواهد رقمی بالقوه[4]

اطلاعات یا داده‌های ذخیره شده یا انتقال داده شده در قالب دودویی، که از طریق فرایند تحلیل، هنوز مرتبط با بررسی تشخیص داده نشده‌اند.

یادآوری ۱- فرایند تحلیل، معلوم می‌کند که کدام یک از شواهد رقمی بالقوه، جزو شواهد رقمی (۳-۵) است.

یادآوری ۲- به شکل ۱ نیز مراجعه شود.

1- Investigative team
2- Investigator
3- Legal digital evidence
4- Potential digital evidence



شکل ۲- گذارهای[1] وضعیت شواهد رقمی

۳-۱۶

تخصص[2]

توانایی یک گروه بررسی برای تولید نتایجی معادل نتایج یک گروه بررسی متفاوت، با استفاده از منابع یکسانی از شواهد رقمی بالقوه است.

۳-۱۷

تکرارپذیری[3]

ویژگی فرایندی است که منجر به گرفتن نتایج یکسان از آزمون در همان محیط آزمون می‌شود.

یادآوری ۱- محیط آزمون یکسان، به معنی رایانه یکسان، سخت‌افزار یکسان، حالت عملیاتی یکسان و غیره است.

[استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، ۳-۱۷]

1- Transitions
2- Proficiency
3- Repeatability

۱۸-۳

قابلیت بازتولید[1]

ویژگی فرایندی است که منجر به گرفتن نتایج یکسان آزمون در محیط آزمون متفاوت می‌شود.

یادآوری ۱- محیط آزمایشی متفاوت، یعنی رایانه متفاوت، سخت‌افزار متفاوت، کارور[2] متفاوت و غیره.

[استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، ۳-۱۸]

۱۹-۳

آسیب‌گری[3]

اقدام به تغییر یا ایجاد امکان تغییر شواهد رقمی بالقوه است که موجب کاهش یافتن[4] ارزش استنادی[5] آن می‌شود.

[استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، ۳-۱۹]

۲۰-۳

اعتبارسنجی[6]

تایید از طریق ارائه شواهد عینی، به طوری که الزامات مورد نیاز برای استفاده و کاربرد معین براورده شده است.

[استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹[7]، ۳-۱۷]

۲۱-۳

درستی سنجی[8]

تایید از طریق ارائه شواهد عینی، از این جهت که الزامات خاص محقق شده است.

یادآوری ۱- درستی سنجی، تنها تضمین می‌کند که یک محصول از مشخصات آن پیروی می‌کند.

[استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹، ۳-۱۸، تغییر داده شده است – یادآوری اصلی حذف شده،

1- Reproducibility
2- Operator
3- Spoliation
4- Diminish
5- Evidential value
6- Validation

۷ - بر اساس منبع لاتین ISO/IEC 27004:2009

8- Verification

و یادآوری ۱ اضافه شده است.]

۲۲-۳

تابع درستی‌سنجی[1]

تابعی است که برای بررسی یکسانی دو مجموعه داده استفاده می‌شود.

[استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، ۳-۱۹، تغییر داده شده است – یادآوری‌ها حذف شده است.]

۲۳-۳

دستورالعمل[2]

شرح کامل چگونگی انجام و ثبت یک فرایند است.
[ISO/TR 10013:2001، 3-1 تغییر داده شده است – از جمع به مفرد تغییر داده شده است، به‌جای وظیفه از فرایند استفاده شده است.]

۴ کوته‌نوشت‌ها

CPD	continuing professional development	توسعه تخصصی مداوم
SMTP	simple mail transfer protocol	قرارداد ساده نامه‌رسانی

۵ بررسی

۵-۱ مرور کلی

هدف اصلی بررسی، گسترش درک رخداد است. قبل از اجرای بررسی این امکان وجود ندارد که تعیین کنیم در صورت توسعه‌ی فهم، کدام فعالیت، رخ خواهد داد. بررسی، می‌توانند منجر به بهبود بازسازی[3]، بهبود سنجه‌ها و واپایش‌های امنیتی برای آینده، اقدامات انضباطی در قبال کارمندان، یا دادگاه مدنی یا جزایی برای افراد مسئول رخداد شوند.
از آن‌جا که در مراحل ابتدایی بررسی، تعیین نتیجه نهایی می‌تواند مشکل باشد، مهم است که بررسی‌های انجام شده ذاتا قابل اعتماد باشند و شواهد رقمی تولید شده توسط آن‌ها دارای منشا قابل اعتماد باشند.

1- Verification function
2- Work instruction
3- Remediation

این هدف می‌تواند توسط ماموران بررسی شایسته و با استفاده از آزمودن‌هایی که از فرایندهای تحلیلی معتبر تشکیل شده‌اند انجام شود. این ماموران بررسی باید در این زمینه متخصص باشند و بتوانند اطمینان دهند که هر نمونه رقمی تولید شده، می‌تواند به منبع شواهد رقمی بالقوه‌ای که این نمونه‌ها از آن به دست آمده‌اند، ردیابی شود.

۵-۲ تداوم

همان‌طور که در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، بحث شده است، ثبت مناسب زنجیره حراست و فرایندهایی که در شواهد رقمی بالقوه به کار گرفته می‌شوند، به اطمینان از این موضوع کمک می‌کند که هیچ ادعایی در این زمینه نمی‌تواند وجود داشته باشد که در نتیجه دست‌کاری یک گروه ناشناس، آسیب‌گری رخ داده است. برای رسیدن به این هدف، تمام فرایندهای به کار برده شده باید به‌صورت کامل و مستحکم ثبت شوند، تا از یک منبع شواهد رقمی بالقوه، شواهد رقمی تولید شوند. در این مورد استفاده از یادداشت‌های هم‌زمان منافع بسیاری به همراه خواهد داشت، زیرا یادداشت‌های تهیه شده در زمان فرایند دقیق‌تر از یادداشت‌ها و ثبت‌هایی هستند که در زمانی پس از وقایعی که توصیف می‌کنند، تهیه شده‌اند.

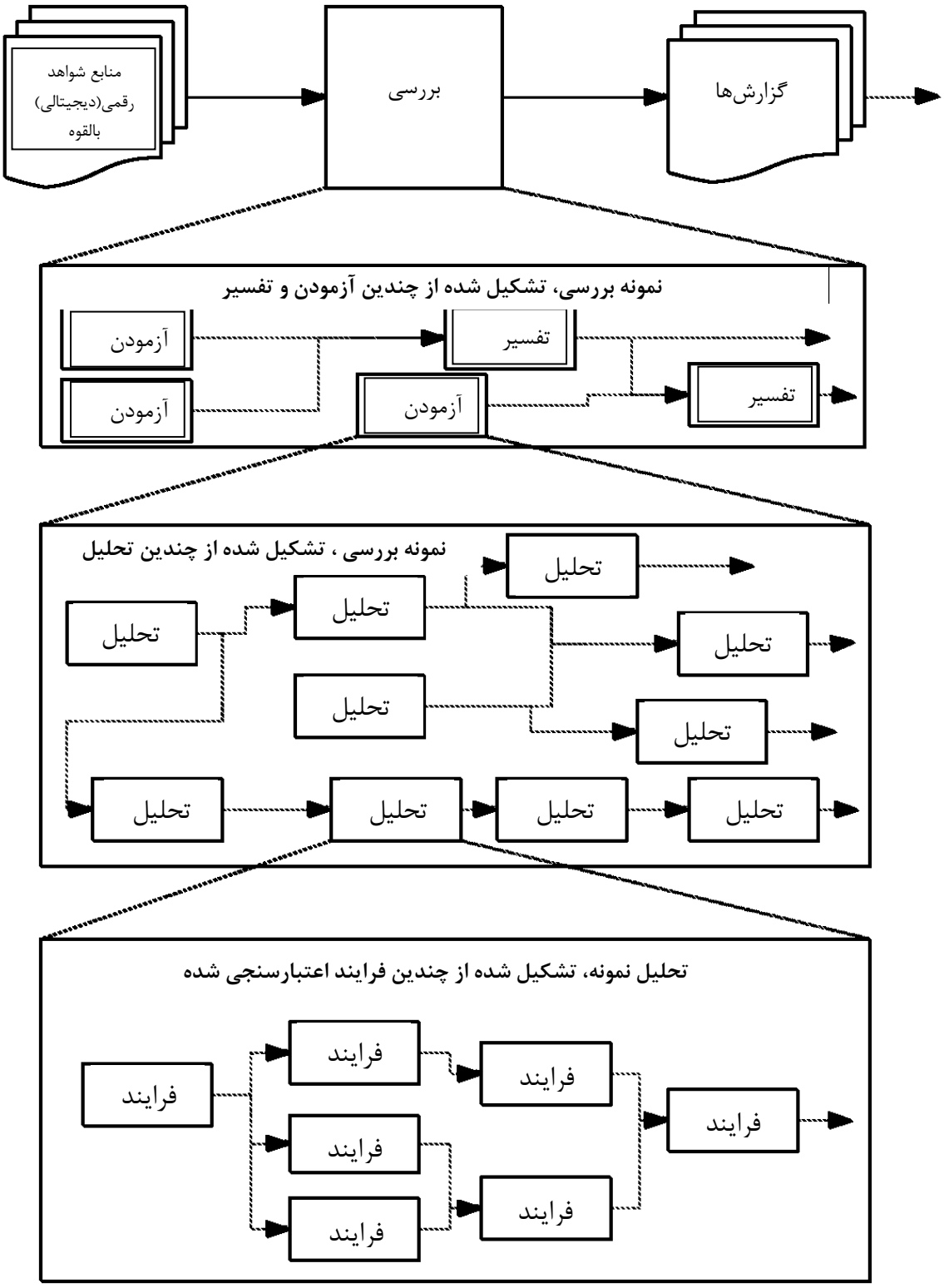
۵-۳ تکرارپذیری و قابلیت بازتولید

شواهد رقمی تولید شده با روش‌هایی که اصول تکرارپذیری و قابلیت بازتولید را برآورده نمی‌کنند به‌شدت در معرض چالش هستند و می‌توانند تخصص و شایستگی گروه بررسی که از آن‌ها استفاده می‌کند را مورد سوال قرار دهند. در حالی که نیاز است در حین بررسی، به منظور نظارت بر فناوری جدید یا نیاز بررسی ناشناخته قبلی، روش‌های جدیدی به‌کار گرفته شوند، به‌کارگیری اعتبارسنجی مناسب (به استاندارد ISO/IEC 27041 مراجعه شود) می‌تواند با نمایش آن روش‌ها، به تولید نتایج قابل اعتماد و بازتولید پذیر کمک کند تا نیازهای بررسی برآورده شود (به شکل ۱ مراجعه شود)

۵-۴ رویکرد ساخت‌یافته[1]

ماموران بررسی موظفند اطمینان ایجاد کنند که یافته‌های خود را تا حد امکان به‌صورت کامل و بی‌طرفانه گزارش می‌کنند. برای نیل به این مقصود، توصیه می‌شود یک رویکرد ساخت‌یافته نسبت به بررسی اتخاذ شود، که توصیه می‌شود توسط ماموران بررسی متخصص و شایسته اجرا شود و در آن منابع شواهد بالقوه مورد آزمودن قرار گیرند. این بررسی از تحلیل‌های مجزایی تشکیل شده است که مناسب افزاره‌ها و داده‌های مورد بررسی هستند. این ساختار در شکل ۲ نشان داده شده است و در بندهای بعدی نیز جزئیات بیشتری در مورد تحلیل، تفسیر، گزارش، شایستگی و تخصص ارائه شده است.

1- Structured



شکل ۳- ساختار یک بررسی نوعی[1]

1- Typical

۵-۵ عدم قطعیت

توصیه می‌شود ماموران بررسی از نواحی عدم قطعیت در یافته‌ها آگاه باشند. توصیه می‌شود عدم قطعیت در حمایت از یک فرضیه، به نسبت عکس با کیفیت و کمیت شواهد در نظر گرفته شود.
در برخی موقعیت‌ها، حضور تنها یک نمونه از شواهد رقمی، ممکن است برای اهداف بررسی کافی باشد (برای مثال تصاحب یک مدرک محرمانه توسط کاربری که اجازه این کار را ندارد.)، در حالی که، در شرایط دیگر، ممکن است شواهد بسیار زیادی مورد نیاز باشند تا فرضیه بررسی‌کننده را اثبات کنند (برای مثال تصاحب مجموعه‌ای بزرگ از مواد غیرقانونی).
درجایی که امکان دارد، باید راهنمایی‌های اضافی از کارخواه به دست آید. (به بند ۸ مراجعه شود)

۶ تحلیل

۶-۱ مرور کلی

تحلیل، از آن جهت مورد نیاز است که بسیاری از فرآورده‌های رقمی بامعنا[1]، در شکل ذاتی خود مخفی شده‌اند (برای مثال، باقی مانده‌های یک پرونده پاک‌شده در فضای آزاد، باید از روی فضای آزاد برداشته شده و بازسازی شوند). همان‌گونه که در ادامه به آن توجه شده است، تحلیل باید از فرایندهای معتبر (آن‌گونه که در استاندارد ISO/IEC 27041 تعریف شده‌اند) استفاده کند. این فرایندهای معتبر باید توسط کارمندان شایسته انجام شده و به‌صورت موشکافانه[2] مستندسازی شوند، تا اطلاعات دارای منشا[3] قابل دفاع و قابل ردیابی باشند.

۶-۲ اصول عمومی

تحلیل، مربوط به تشخیص و ارزیابی شواهد رقمی از منابع شواهد رقمی بالقوه می‌شود. ممکن است تحلیل به‌صورت یک فرایند تکراری باشد، زیرا هر نمونه‌ای از شواهد دیجیتال تشخیص داده شده می‌تواند موجب در نظر گرفتن مجدد شواهد رقمی دیگر شود. تشخیص و ارزیابی تنها می‌تواند در حضور اطلاعات کافیِ مرتبط با متن صورت پذیرد تا به بررسی‌کننده اجازه دهد که درباره هر نمونه مورد نظر، تصمیمات آگاهانه‌ای بگیرد (برای مثال، اطلاعات در مورد رخداد مورد ظن، سامانه مورد نظر و طبیعت منابع شواهد رقمی بالقوه مورد بررسی).
بنابراین، ماموران بررسی و کارکنان کمکی آن‌ها، باید برای انجام نقش‌هایشان در تحلیل، شایسته باشند. شایستگی می‌تواند به‌عنوان فرایندهای مجزایی که آن‌ها انجام خواهند داد یا به‌عنوان مجموعه‌ای از

1- Meaningful digital artefacts
2- Scrupulously
3- Provenance

شایستگی‌های تعریف شده در برابر آنچه آنها ارزیابی می‌کنند، تعریف شود.
توصیه می‌شود، فرایندهای استفاده شده برای آزمودن نمونه‌های شواهد رقمی بالقوه، در زمینه نقش(ها)شان در بررسی، به‌طور کامل اعتبارسنجی شوند (به استاندارد ISO/IEC 27041 مراجعه شود).
توصیه می‌شود، فرایندهای مورد استفاده، محتویات هیچ منبعی از شواهد رقمی بالقوه مورد آزمودن را تغییر ندهند. وقتی که احتمال آسیب به شواهد رقمی بالقوه وجود دارد، توصیه می‌شود اندازه‌گیری‌های مناسبی انجام شوند تا احتمال یا اثرات هر آسیبی کاهش یابد (برای مثال برای کمینه کردن احتمال تغییر غیرعمدی محتویات یک لوح سخت که جزو شواهد است، از خط‌بند[1] استفاده شود). «با این وجود، اگر بروز چنین آسیبی غیرقابل اجتناب یا کاملا ضروری است، توصیه می‌شود گروه بررسی به‌قدری شایسته باشد که بتواند اثرات هرگونه فعالیت انجام شده که ممکن است موجب آسیب شده باشد، و همچنین دلایل چنین فعالیت-هایی و آسیب وارد شده را توضیح دهد.»
توصیه می‌شود اگر یکی از اعضای گروه بررسی باور داشته باشد که شواهدی از یک رخداد دیگر پیدا کرده است، رهبر بررسی را از این واقعیت آگاه سازد و منتظر دستورهای بعدی بماند. توصیه می‌شود آن دسته از رهبران بررسی که از چنین شواهدی آگاه شده‌اند، قبل از ادامه دادن بررسی، با مسئولین مرتبط مشورت کنند. اگر هر آسیبی به شواهد رقمی بالقوه مشاهده شود، توصیه می‌شود که در گزارش (نهایی) بیان شود.
یادآوری ۱- در بسیاری از حوزه‌های قضایی، فراتر رفتن از اختیارات مربوط به حکم بررسی، ممکن است موجب غیرقابل استفاده شدن تمام نتایج (نه فقط آن‌هایی که مربوط به رخداد تازه کشف شده هستند) در فرایندهای قانونی و اداری شود.
توصیه می‌شود اعضای گروه بررسی به تعهدات اجباری‌شده[2] محلی خود در مورد بی‌طرفی توجه داشته باشند. در جایی که چنین تعهداتی وجود دارد و در حین بررسی در مورد یک فرضیه، اگر گروه بررسی شواهدی پیدا کرد که برخلاف آن فرضیه و یا در حمایت از آن فرضیه باشند یا یک فرضیه خلاف را پیشنهاد دهند، توصیه می‌شود این فرضیه ها را به همراه شواهد تایید کننده، در گزارش خود بیان کند.
بررسی‌کنندهاتی مستقل که با تحلیل و تفسیر در ارتباط نیست، باید قادر باشد که فرایندها و تصمیم‌های گرفته شده توسط گروه بررسی اصلی را مورد بررسی قرار دهد و به نتایج یکسانی برسد. برای رسیدن به این هدف، توصیه می‌شود زنجیره‌ای از فرایندهای جزئی که به‌صورت مناسب مستندسازی شده‌اند (که به‌طور معمول در محیط فرایندهای اعتبارسنجی شده مجزا تعریف شده‌اند) و در یادداشت‌های هم‌زمان ثبت شده‌اند، دنبال شوند و با جزئیات مناسب ثبت شوند.
یادآوری ۲- در هنگام استفاده از این استاندارد ملی، کاربر فرض می‌کند که شواهد رقمی، مطابق توصیه‌های استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، جمع آوری شده‌اند، و برای نگهداری شواهد رقمی بالقوه در حین تحلیل، گام‌های مشابه گام‌های توصیف شده در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، مورد استفاده قرار خواهند گرفت.

1- Write blocker
2- Mandated

۶-۳ استفاده از ابزار

در فرایند تحلیل، ابزار (ترکیبی از نرم‌افزار، سخت‌افزار و ثابت‌افزار[1]) می‌توانند کمک شایانی باشند. توصیه می‌شود انتخاب ابزار بر اساس ملزومات مورد توافق و فرایندهایی (به استاندارد ISO/IEC 27041 مراجعه شود) که تشکیل دهنده تحلیل هستند صورت پذیرد. توصیه می‌شود کاربر برای استفاده از ابزار در محیط مرتبط، شایسته باشد.

توصیه می‌شود قبل از شروع به کار، فرایندهایی که شامل ابزار جدید هستند، قادر به پشت سرگذاری اعتبارسنجی و تایید باشند. توصیه می‌شود کاربران قبل از استفاده از ابزار جدید، به این مسئله بپردازند. توصیه می‌شود برای انتخاب ابزاری برای استفاده در فرایندهای اعتبارسنجی شده، فرایند مشخص شده در ISO/IEC 27041 دنبال شود.

یادآوری – برای مفهوم اعتبارسنجی، نیاز است استفاده مورد نظر از ابزار لحاظ شود. از این رو، این نوع الزامات صرفا برای اعتبارسنجی فرایندی می‌باشند که در بررسی مورد استفاده می‌گیرد. ممکن است ابزاری که ناقص بودن آن معلوم شده، همچنان مورد استفاده قرار گیرد؛ به شرط این که ابزار، مناسب مقصود مورد نظر فرایندی باشد که ابزار در آن مورد استفاده قرار می‌گیرد.

۶-۴ نگهداری سوابق

توصیه می‌شود در حین تحلیل، هر شخصی که فرایندی را انجام می‌دهد، یادداشت‌های هم‌زمان دقیق و مفصلی از فعالیت‌هایش و نتایج آن فعالیت‌ها تهیه کرده و علاوه بر آن، زنجیره نگهداری را نیز آن‌گونه که در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، توصیف شده است، ثبت کند. این کارها باید با جزئیات کافی صورت پذیرد تا اجازه دهد شخص دیگری که به همان اندازه شایسته است، آن فعالیت‌ها را تکرار کرده و به نتایج یکسانی برسد. توصیه می‌شود یادداشت‌ها شامل اطلاعات مرتبط دریافت‌شده و تصمیمات اتخاذ شده، ازجمله دلایل تصمیمات باشد.

۷ مدل‌های تحلیل

۷-۱ تحلیل ایستا[2]

معمولا توصیه می‌شود که تحلیل ایستا روی یک رونوشت[3] از شواهد رقمی بالقوه اصلی انجام شود (همان‌گونه که در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، توصیف شده است) تا از آسیب‌گری یا مبهم‌سازی تصادفی شواهد رقمی جلوگیری به عمل آید.

تحلیل ایستا، آزمودن شواهد رقمی بالقوه صرفا با استفاده از بازرسی[4] است، تا ارزش آن‌ها به‌عنوان شواهد

3- Firmware
1- Static
2- Copy
3- Inspection

رقمی معین شود (برای مثال تشخیص فرآورده‌های، ساخت جدول زمانی، ارزیابی محتویات پرونده و داده‌های پاک شده، و غیره). شواهد رقمی بالقوه، در فرم خام خود مورد بازرسی قرار می‌گیرند و از طریق فرایندهای مناسب تفسیر می‌شوند (برای مثال توسط بارگذاری در مناسب). اما کدهای قابل اجرا، اجرا نخواهند شد.
این روش تحلیل، به‌ویژه برای تحلیل داده‌های پی‌درپی[1] (برای مثال محتویات پرونده‌های ثبت، محتویات بسته‌های شبکه و محتویات برگرفت‌های حافظه) و فراداده‌ها (برای مثال اجازه‌های پرونده و مهرهای زمانی[2]) مناسب است. هرچند، در برخی موارد، ممکن است برای ماموران بررسی این امکان وجود نداشته باشد که تنها با استفاده از تحلیل ایستا، درک کاملی از اهمیت شواهد رقمی بالقوه به دست آورند (برای مثال ایجاد نفوذ[3] یا رفع پالایه[4] داده‌ها توسط بدافزار).

۷-۲ تحلیل زنده[5]

۷-۲-۱ موارد کلی

در برخی شرایط ممکن است لازم یا سودمند باشد که برای به دست آوردن درک درست، یک نسخه زنده از شواهد رقمی بالقوه مورد بررسی قرار گیرد. این کار به‌خصوص می‌تواند هنگام پرداختن به سامانه‌هایی مانند پیام‌رسانی لحظه‌ای، گوشی‌های هوشمند/ تبلت‌ها، نفوذ در شبکه، شبکه‌های پیچیده، افزاره‌های ذخیره‌سازی رمزگذاری شده یا کد چند ریخت مورد ظن[6]، مفید واقع شود.
دو نوع متفاوت از تحلیل زنده وجود دارد:
الف) تحلیل زنده سامانه‌هایی که قابلیت رونوشت‌گیری یا تصویرگیری[7] ندارند؛ و
ب) تحلیل زنده سامانه‌هایی که قابلیت رونوشت‌گیری یا تصویرگیری دارند؛

۷-۲-۲ تحلیل زنده سامانه‌های غیرقابل تصویرگیری یا رونوشت‌گیری

هنگامی که به خاطر دلایل فنی یا عملیاتی، رونوشت گرفتن یا تصویر گرفتن ممکن نیست (برای مثال سخت‌افزار منحصر به فرد یا تاثیر منفی روی تجارت) یا در صورت تلاش برای رونوشت گرفتن یا تصویر گرفتن خطر قابل توجهی در زمینه از دست دادن شواهد رقمی بالقوه وجود دارد (برای مثال تلاش برای رونوشت گرفتن داده‌ها از یک افزاره ذخیره‌سازی زنده با استفاده از ابزارهای موجود در سامانه مشکوک)، ممکن است ضروری باشد که بدون پیروی اولیه از گام‌های پیشنهاد شده در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، یک تحلیل زنده روی سامانه انجام شود.
در این شرایط، توصیه می‌شود ماموران بررسی مراقب کمینه کردن خطر وارد شدن آسیب به شواهد رقمی

4- Consequential
5- Timestamps
1- Intrusion
2- Exfiltration
3- Live analysis
4- Polymorphic code
5- Imaged

بالقوه باشند و اطمینان پیدا کنند که تمام فرایندهای اجرا شده را به‌صورت کامل و با جزئیات ثبت می‌کنند. توصیه می‌شود رهبران بررسی اطمینان پیدا کنند که هر شخصی که از وی خواسته شده یک تحلیل زنده را انجام دهد، برای این کار کاملا شایسته بوده و قادر به توضیح فرایندهای آن‌ها و هر تغییری در داده‌ها، شواهد رقمی بالقوه یا سامانه‌هایی که ممکن است در نتیجه فعالیت‌های آن‌ها ایجاد شده باشند، باشد.

۷-۲-۳ تحلیل زنده سامانه‌های قابل تصویرگیری یا رونوشت‌گیری

در جایی که یک سامانه قابل تصویرگیری یا رونوشت‌گیری باشد، ممکن است مناسب یا ضروری باشد که آن سامانه، توسط تعامل مستقیم یا مشاهده آن حین فعالیت، مورد بررسی قرار گیرد. در چنین شرایطی، توصیه می‌شود ماموران بررسی دقت لازم را داشته باشند، تا بتوانند تا آن‌جایی که ممکن است از محیط اصلی، از لحاظ سخت‌افزاری و نرم‌افزاری، تقلید کنند. آن‌ها این کار را با استفاده از ماشین‌های مَجازی اعتبارسنجی شده (به استاندارد ISO/IEC 27041 مراجعه شود)، رونوشت‌هایی از سخت‌افزار اصلی و حتی سخت‌افزار اصلی واقعی انجام می‌دهند تا امکان تحلیل زنده فراهم شود. جایی که از همانندسازی استفاده می‌گردد، باید اطمینان داشت که برابری تا حد ممکن شبیه سامانه اصلی انجام گرفته باشد. توصیه می‌شود گام‌هایی اتخاذ شوند، تا اطمینان پیدا شود که تغییراتی که برای اجازه رونوشت‌گیری در همانندسازی مورد نیاز است، عملکرد سامانه و شواهد رقمی بالقوه تحت تحلیل را خیلی تغییر نمی‌دهد.

یادآوری – هنگامی که به آلودگی بدافزاری مظنون هستیم، لازم است در استفاده از تقلید مراقب باشیم، زیرا برخی از گونه‌های بدافزار می‌توانند تشخیص دهند که در یک محیط مَجازی در حال اجرا هستند و در نتیجه می‌توانند رفتار خود را تغییر داده یا از اجرا شدن صرف نظر کنند.

۸ تفسیر

۸-۱ عمومی

هدف از تفسیر، دریافت معنا از شواهد رقمی توسط ارزیابی داده‌ها و تحلیل آن‌ها در شرایط به‌خصوص است. تفسیر توسط فرایندهای آزمودن و تحلیل، شامل یافتن حقایق و در برخی موارد نظر دادن در مورد حقایق می‌شود. بسته به نتایج تفسیر، ممکن است لازم باشد تحلیل و یا جمع‌آوری شواهد رقمی بالقوه تکرار شوند. توصیه می‌شود گروه بررسی به خاطر داشته باشد که مسئولیت ابتدایی آن‌ها، ارائه یک تفسیر منصفانه و دقیق از حقایقی است که کشف می‌کنند.

۸-۲ اعتباربخشی به حقایق

در هنگام ارزیابی شواهد، بایستی دقت شود حقایقی که کشف شده‌اند و حقایقی که استنباط شده‌اند، از هم تمایز داده شوند.

مثال : وجود یک پرونده باقی مانده از قبل در یک افزاره، یک حقیقت محسوب می‌شود. اگر آن پرونده، ضمیمه‌ای به یک رایانامه در یک جعبه ورودی رایانامه بوده است، می‌توان استنباط کرد به علت این که پرونده در یک رایانامه دریافت شده بوده، آن پرونده در خود افزاره ساخته شده است؛ از این رو، این نوع اطلاعات، استنباط شده است. هرچند، اگر پرونده در یک

دایرکتوری ساخته شده توسط کاربر پیدا شده باشد و نام پرونده را هم کاربر تعیین کرده باشد، می‌توان استنباط کرد که کاربر تصمیم آگاهانه‌ای برای ایجاد یا ذخیره پرونده اتخاذ کرده است. استنباط در مورد پرونده‌هایی مانند این، می‌تواند توسط بررسی قسمت‌های دیگر سامانه پرونده تایید شود، تا بدین وسیله بتوان اطلاعات بیشتری به دست آورد.

تفاوت میان حقایق و اطلاعات استنباط شده را باید همواره به خاطر داشت، و باید مراقب بود حقایق مورد نیاز برای دفاع از هر استنباطی در جای خود قرار داشته باشند و مورد تایید واقع شوند. در هنگام گزارش حقایق و اطلاعات استنباط شده، تفاوت میان این دو باید بیان شود و فرایندهای منطقی که باعث هر استنباط شده‌اند نیز باید واضح و تکرارپذیر باشند.

۸-۳ عواملی که روی تفسیر تاثیر می‌گذارند

تفسیر هرگونه شواهد رقمی، به اطلاعات در دسترس در مورد محیط خلق آن نمونه از شواهد رقمی بستگی دارد. برای ارائه یک تفسیر مناسب، ممکن است گروه بررسی نیاز به اطلاعات اشخاصی داشته باشد که هر روزه در به کار اندازی سامانه‌های تحت بررسی دخالت دارند. به هر حال، توصیه می‌شود برای آزمایش این گونه اطلاعات تامین شده و تضمین این که ارزشهای آزمایشی معین این قابلیت اطمینان را بازتاب می‌دهند، مراقبت انجام گیرد.

علاوه بر این، گروه بررسی نیاز به اطلاعاتی در مورد هدف بررسی و دامنه فعالیت‌های خود دارند، ازجمله هدف و مخاطبین مقصود گزارش نهایی.

توصیه می‌شود گروه بررسی در طول تحلیل و تفسیر، کیفیت شواهد رقمی بالقوه را تحت نظر داشته باشند (برای مثال کامل بودن، منبع و هدف اصلی، و احتمال استفاده از اقداماتی برای مبهم سازی شواهد).

هدف از مرحله تفسیر، ارائه توصیفی از حقایق یافت شده در طول تحلیل و در محیط فراهم شده برای گروه بررسی است. اگر بیش از یک توصیف معقول وجود دارد، توصیه می‌شود توصیف‌های جایگزین نیز گزارش شوند. اگر اطلاعات مربوط به محیط تغییر پیدا کنند، ممکن است لازم باشد تفسیر نیز تغییر داده شود. اگر حقایق منجر به بیش از یک تفسیر می‌شوند، توصیه می‌شود تمامی آن‌ها – یا کمینه آن‌هایی که موجه‌تر[1] هستند – به‌عنوان نتیجه‌ای از تحلیل ارائه شوند؛ و اگر ممکن باشد، احتمال هرکدام از آن‌ها نیز بیان شود.

۹ گزارش

۹-۱ آماده‌سازی

توصیه می‌شود پیش از شروع بررسی، ماهیت و هدف گزارش نهایی توسط رهبر بررسی معلوم شود. انجام این کار از آن جهت توصیه می‌شود که باعث هدایت فرایند بررسی می‌گردد و ممکن است شامل مجموعه‌ای از سوالاتی که باید پاسخ داده شوند، یا اشاره به خوانندگان احتمالی گزارش، و یا جزئیات هر حد و حدود یا محدودیتی که در بررسی وجود دارند، باشد. توصیه می‌شود رهبر بررسی یک برنامه یا راهبرد بررسی

1- Plausible

مستندسازی شده را آماده کند تا به تعیین منابع، انتخاب فرایندها و ابزار، و هدایت گروه بررسی کمک کند.
توصیه می‌شود گزارش‌ها شامل تمامی اطلاعات خواسته شده توسط خط‌مشی‌های محلی یا قانون[1] باشند.
برخی از محتویات توصیه شده، در ۹-۲ آمده‌اند.
استفاده از قالب‌های گزارش با قالب استاندارد، فهرست‌های انتخاب، و علائم نگارشی برای متن‌های معمولی، ممکن است برای اطمینان از این که اطلاعات کافی در گزارش لحاظ شده‌اند، مفید باشد.

۹-۲ محتویات پیشنهادی برای گزارش

اگر خط‌مشی‌های محلی یا قانون محتویات گزارش را تعیین نمی‌کند، توصیه می‌شود که گزارش کمینه دارای موارد زیر باشد:

- بیان واضح شایستگی یا کاردانی نویسنده برای مشارکت در بررسی و تولید گزارش؛
- بیان واضح اطلاعات قرار گرفته در دسترس گروه بررسی قبل از شروع بررسی (ازجمله ماهیت گزارشی که باید تولید شود)؛
- ماهیت رخداد تحت بررسی؛
- زمان و طول رخداد؛
- موقعیت مکانی رخداد؛
- هدف بررسی؛
- اعضای گروه بررسی، نقش‌ها و فعالیت‌هایشان؛
- زمان و طول بررسی؛
- موقعیت مکانی بررسی؛
- جزئیات حقیقی از شواهد رقمی یافت شده در هنگام بررسی؛
- هرگونه آسیبی که در طول بررسی به شواهد رقمی بالقوه وارد شده، و تاثیرات آن بر گام‌های بررسی بعدی؛
- محدودیت‌های هر تحلیل صورت گرفته (برای مثال مجموعه اطلاعات ناکامل، محدودیت‌های زمانی/عملیاتی)؛ و
- فهرستی از فرایندهای استفاده شده و هر جا که مناسب باشد، شامل هرگونه ابزار استفاده شده.
- برخی از گزارش‌ها ممکن است شامل این‌ها نیز باشند:
- تفسیر شواهد رقمی آن‌گونه که توسط بررسی‌کنندهاتی درک شده است (برای مثال بیان این که چگونه یک حمله بیرونی ممکن است انجام شده و باعث حضور شواهد رقمی شده باشد). اگر امکان بیش از یک تفسیر وجود دارد، توصیه می‌شود تمامی تفسیرهای محتمل و عملی گنجانده شوند و احتمال نسبی هرکدام از آن‌ها نیز بیان شود. اگر هم نیاز باشد، تفسیر را نیز می‌توان در قالب یک

2- Legislation

نظر ارائه کرد.

- نتیجه‌گیری‌ها.
- توصیه‌هایی برای کارهای بررسی یا جبرانی بیشتر.

وقتی که یک گزارش شامل یک یا چند نظر است، توصیه می‌شود نویسنده به‌طور واضح بین حقایق و نظرات تمایز قائل شود و برای هر نظر بیان شده، توجیهی ارائه دهد.

در برخی موارد، طراحی گزارش می‌تواند در رده‌های فرایند آماده‌سازی و شروع، صورت پذیرد (به استاندارد ISO/IEC 27043 مراجعه شود). هر جا که مناسب باشد، فرایند طراحی قالب می‌تواند با استفاده از چارچوب توصیف شده در ISO/IEC 27041 اعتبارسنجی شود.

۱۰ شایستگی[1]

۱-۱۰ مرور کلی

توصیه می‌شود تمام گام‌های گنجانده شده در بررسی دربارهٔ رخداد، توسط افرادی که برای تکمیل وظایف محول شده به آن‌ها به‌وضوح شایسته هستند، انجام شود. توصیه می‌شود آن‌ها با ابزار، روش‌ها و فنونی که مورد استفاده آن‌ها است، به اندازه کافی آشنا بوده و در مورد آن‌ها تجربه داشته باشند، تا قادر باشند با کمینه نظارت با آن‌ها کار کنند. همچنین توصیه می‌شود از محدودیت‌های توانایی‌های خود نیز آگاه باشند. اگر یک بررسی‌کنندهاتی از محدودیتی در توانایی‌های خود آگاه شود، موضوع باید به فردی ارشدتر یا شایسته‌تری ارجاع داده شود تا اقدامات مناسب انجام شوند.

حضور فردی که شایستگی لازم را ندارد در یک بررسی، ممکن است تاثیر منفی روی نتایج بررسی گذاشته و باعث تاخیر در کامل شدن بررسی و یا ایجاد نتایج نادرست شود.

یک مثال از تعریف شایستگی، در پیوست الف آمده است.

۲-۱۰ نشان دادن شایستگی

توصیه می‌شود شایستگی در مقابل مجموعه‌ای از مهارت‌های مرکزی که برای هر فرایند مشخص شده در بررسی که توسط فردی که عضوی از بررسی است انجام می‌شود، تعریف شود. توصیه می‌شود شواهد عینی شایستگی‌ها و تجربه فرد، مطالبه شوند. این شواهد می‌توانند به‌صورت آزمون‌ها یا گواهینامه‌های رسمی شایستگی، شایستگی‌های دانشگاهی، سابقه کار، شواهد حضور فعال در رویدادهای ترکیبی مانند اجلاس‌ها، دوره‌های مهارت‌آموزی، یا توسعه ابزار، روش‌ها، فنون، فرایندها، یا استانداردهای جدید باشند.

۳-۱۰ ثبت شایستگی

توصیه می‌شود شایستگی فرد، در بازه‌های زمانی منظم بازبینی شود تا اطمینان حاصل شود که اطلاعات

1- Competence

مربوط به شایستگی فرد دقیق بوده‌اند. توصیه می‌شود بازبینی، عرصه‌ها و سطوح جدید شایستگی که فرد به آن‌ها نائل شده است را نیز در نظر بگیرد و همچنین شایستگی‌هایی که دیگر مرتبط با فرد مورد نظر نیستند را نیز نادیده بگیرد؛ خواه دلیل آن این باشد که دانش و یا مهارت‌های مورد نظر دیگر مطرح نیستند یا این که فرد مورد نظر، از آخرین زمان بازبینی، فرصت این را نداشته که آن‌ها را به حد کافی تمرین کند.
اگر شایستگی یک فرد در یک زمینه خاص، برای ایفای نقش خود در یک بررسی کافی نیست، توصیه می‌شود گام‌هایی اتخاذ شود تا هر چه سریع‌تر از طریق فعالیت‌های ترکیبی، آن سطح از شایستگی افزایش یابد.

۱۱ تخصص

۱-۱۱ مرور کلی

یک گروه بررسی شایسته، متخصص محسوب شود اگر تحلیلش با داشتن شواهد رقمی بالقوه نمونه، نتایجی تولید کند که هم‌ارز نتایج تولید شده توسط گروه بررسی شایسته دیگری باشند که از تحلیل مشابهی استفاده کرده است.
سوابق‌ای که نشان دهنده تخصص یک گروه بررسی هستند، در نشان دادن این که تحلیل‌های استفاده شده دقیق، قابل اعتماد، بازتولیدپذیر و مناسب هستند، کمک می‌کند.

۲-۱۱ سازوکارهایی[1] برای نشان دادن تخصص

تخصص می‌تواند از طریق مشارکت در یک فرایند به آزمون گذاری تخصص (استاندارد ملی ایران شماره ۱۷۰۴۳ : سال ۱۳۹۳) که تحت نظارت یک طرف سوم مستقل است، نشان داده شود. در چنین فرایندی، نمونه‌های مشابهی برای تحلیل، در اختیار تمامی گروه‌های بررسی قرار خواهند گرفت. نتایج مورد انتظار تحلیل، توسط طرف سومِ مستقل پیش‌بینی خواهند شد و طرف سومِ مستقل مسئول مقایسه نتایج تمامی گروه‌های بررسی شرکت‌کننده با نتایج پیش‌بینی‌شده و نتایج تولید شده توسط تمامی گروه‌های بررسی دیگر در گروه آزمون خواهد بود. آن دسته از گروه‌های بررسی که برای نمونه‌های مشابه، نتایج هم ارزی تولید کنند، در زمینه تحلیل‌های استفاده شده برای تولید آن نتایج، به‌طور یکسان متخصص در نظر گرفته خواهند شد.

یادآوری – در بین گروه‌های بررسی متخصصی که نتایج هم ارزی تولید می‌کنند، نتیجه‌گیری‌هایی که در گزارش بیان می‌شوند، ممکن است همیشه هم ارز نباشند.

توصیه می‌شود آزمون‌های تخصص در بازه‌های زمانی منظم برای نشان دادن حفظ تخصص تکرار شوند.
اگر هیچ آزمون طرف سومِ مستقل مناسبی در دسترس نیست، ممکن است یک گروه بررسی مستقیما به گروه‌های بررسی دیگر مراجعه کند تا یک طرح آزمون مناسب برای نیازهایشان را طراحی کنند. توصیه می-

1- Mechanisms

شود چنین طرحی، در حالت مطلوب، تحت موشکافی مستقل قرار گیرد تا اطمینان حاصل شود که طرح مناسبی است.

پیوست الف

(آگاهی‌دهنده)

نمونه‌هایی از مشخصات شایستگی و تخصص

الف-۱ مثال مشخصات شایستگی

شایستگی عمومی	تحلیل رخدادهای کارساز *ارسال نامه*
شایستگی‌های خاص	قادر باشد: – پرونده‌های ثبت ارسال نامه را موقعیت‌یابی، تجزیه و تفسیر کند – صندوق‌های پستی کاربران را موقعیت‌یابی، تجزیه و تفسیر کند – سرآیندهای SMTP که در پیام‌های پستی یافت می‌شوند را موقعیت‌یابی، تجزیه و تفسیر کند – پرونده‌های پیکربندی ارسال نامه را موقعیت‌یابی، تجزیه و تفسیر کند – حالت‌های خرابی‌های معمول ارسال نامه و استفاده‌های معمول در نسخه‌های مرتبط با ارسال نامه را توصیف کند

الف-۲ مثال مشخصات تخصص

تخصص عمومی	تحلیل رخدادهای ارسال نامه
تخصص‌های خاص	▪ شناسایی و انتشار موفق گزارش‌ها مربوطه از: – پرونده‌های سوابق – صندوق‌های پستی کاربران – پیام‌های پستی – پرونده‌های پیکربندی – پرونده های اصلی ▪ بتواند تعاملات[1] با دیگر نرم‌افزارها، سامانه‌ها و کاربران را با موفقیت شناسایی و مشخص کند

1- Interaction

کتابنامه

[۱] استاندارد ملی ایران شماره ۱۷۰۲۴ : سال ۱۳۹۳، ارزیابی انطباق -الزامات عمومی برای نهادهای گواهی کننده اشخاص

[۲] استاندارد ملی ایران شماره ۱۷۰۲۵ : سال ۱۳۸۶، الزامات عمومی برای احراز صلاحیت آزمایشگاه های آزمون و کالیبراسیون

[۳] استاندارد ملی ایران شماره ۱۷۰۴۳ : سال ۱۳۹۳، ارزیابی انطباق-الزامات عمومی آزمون مهارت

[4] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[۵] استاندارد ملی ایران شماره ۲۷۰۳۵ : سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

[6] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3ed. New York: Academic Press, 2011.