



جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization



استاندارد ایران-ایزو-آی ای سی

۲۷۰۳۷

چاپ اول

۱۳۹۳

INSO-ISO-IEC

27037

1st. Edition

2014

Identical with
ISO/IEC 27037: 2012

فناوری اطلاعات - فنون امنیتی -
راهنماهایی برای شناسایی، جمع آوری،
اکتساب و حفاظت از شواهد رقمی
(دیجیتال)

Information technology — Security
techniques — Guidelines for
identification, collection, acquisition, and
preservation of digital evidence

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است. تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می شود و پس از دریافت نظرها و پیشنهادات در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود. بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)^۱، کمیسیون بین المللی الکتروتکنیک (IEC)^۲ و سازمان بین المللی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین المللی بهره گیری می شود.

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامه تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات - فنون امنیتی - راهنمایی برای شناسایی، جمع آوری، اکتساب و حفاظت از شواهد رقمی (دیجیتال) »

رئیس:

ایزدپناه، سحرالسادات

(فوق لیسانس مهندسی فناوری اطلاعات)

دبیر:

میر اسکندری، سید محمدرضا

(لیسانس مهندسی کامپیوتر نرم افزار)

اعضاء: (اسامی به ترتیب حروف الفبا)

بخشایش، سعید

(فوق لیسانس مهندسی کامپیوتر)

رشتی، سید محمدرضا

(لیسانس مهندسی کامپیوتر نرم افزار)

سجادیه، علیرضا

(فوق لیسانس مهندسی کامپیوتر)

سعیدی، عذراء

(فوق لیسانس مهندسی مخابرات)

طی نیا، رضا

(فوق لیسانس مدیریت فناوری اطلاعات)

فولادیان، مجید

(فوق لیسانس مهندسی مخابرات)

قسمتی، سیمین

(فوق لیسانس مهندسی فناوری اطلاعات)

میرمعینی، علیرضا

(فوق لیسانس مهندسی صنایع)

ناظمی، اسلام

(دکترای مهندسی کامپیوتر)

سمت و / یا نمایندگی

کارشناس مسؤول سازمان فناوری اطلاعات ایران

مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات

مدیرعامل شرکت فناوران توسعه امن ناچی

مدیرعامل شرکت توسعه ارتباطات بهینه برنا

مدیرعامل شرکت پردازشگران

کارشناس تدوین استاندارد سازمان فناوری اطلاعات

مدیرعامل شرکت کاربرد سیستم

کارشناس تدوین استاندارد سازمان فناوری اطلاعات

کارشناس تدوین استاندارد سازمان فناوری اطلاعات

مدیرعامل پژوهش های راهبردی امن

استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا
(فوق لیسانس فناوری اطلاعات)

پژوهش گر دانشگاه شهید بهشتی

یوسف زاده، سمیرا
(فوق لیسانس کامپیوتر – نرم افزار)

پژوهش گر دانشگاه شهید بهشتی

فهرست مندرجات

صفحه	عنوان
ج	کمیسیون فنی تدوین استاندارد
ز	پیش‌گفتار
۱	۱ هدف و دامنه کاربرد
۲	۲ مراجع الزامی
۲	۳ اصطلاحات و تعاریف
۷	۴ کوتاه‌نوشت‌ها
۸	۵ مرور کلی
۸	۱-۵ زمینه جمع‌آوری شواهد رقمی
۸	۲-۵ اصول شواهد رقمی
۹	۳-۵ الزامات برای ساماندهی به شواهد رقمی
۹	۱-۳-۵ عمومی
۱۰	۲-۳-۵ قابلیت ممیزی
۱۰	۳-۳-۵ تکرارپذیری
۱۰	۴-۳-۵ قابلیت بازتولید
۱۱	۵-۳-۵ توجیه پذیری
۱۱	۴-۵ فرآیندهای ساماندهی شواهد رقمی
۱۱	۱-۴-۵ مرور کلی
۱۲	۲-۴-۵ شناسایی
۱۳	۳-۴-۵ جمع‌آوری
۱۳	۴-۴-۵ اکتساب
۱۴	۵-۴-۵ حافظت
۱۵	۶ مولفه‌های کلیدی شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی
۱۵	۱-۶ زنجیره توقیف
۱۶	۲-۶ احتیاط در محل رخداد
۱۶	۱-۲-۶ عمومی
۱۷	۲-۲-۶ کارکنان
۱۷	۳-۲-۶ شواهد رقمی بالقوه
۱۸	۳-۶ نقش‌ها و مسؤولیت‌ها
۱۸	۴-۶ شایستگی
۱۹	۵-۶ استفاده از مراقبت منطقی

۲۰	مستندسازی	۶-۶
۲۱	جلسات توجیهی	۷-۶
۲۱	عمومی	۱-۷-۶
۲۱	مخصوص شواهد رقمی	۲-۷-۶
۲۲	مخصوص کارکنان	۳-۷-۶
۲۲	رخدادهای بلادرنگ	۴-۷-۶
۲۳	سایر اطلاعات توجیهی	۵-۷-۶
۲۳	اولویت‌بندی جمع‌آوری و اکتساب	۸-۶
۲۴	حفاظت از شواهد رقمی بالقوه	۹-۶
۲۴	مرور کلی	۱-۹-۶
۲۵	حفاظت از شواهد رقمی بالقوه	۲-۹-۶
۲۵	بسته‌بندی افزارهای رقمی و شواهد رقمی بالقوه	۳-۹-۶
۲۷	انتقال شواهد رقمی بالقوه	۴-۹-۶
۲۸	مثال‌های شناسایی، جمع‌آوری، اکتساب و محافظت	۷
۲۸	رایانه‌ها، افزارهای جانبی و رسانه‌ی ذخیره‌سازی رقمی	۱-۷
۲۸	شناسایی	۱-۱-۷
۳۱	جمع‌آوری	۲-۱-۷
۳۶	اکتساب	۳-۱-۷
۴۲	حفاظت	۴-۱-۷
۴۳	افزارهای شبکه شده	۲-۷
۴۳	شناسایی	۱-۲-۷
۴۵	جمع‌آوری، اکتساب و حفاظت	۲-۲-۷
۴۹	حفاظت، اکتساب و جمع‌آوری دوربین‌های مدار بسته	۳-۷
۵۲	پیوست الف (اطلاعاتی) مهارت‌های اصلی DEFR و شرح صلاحیت	
۵۴	پیوست ب (اطلاعاتی) کمینه الزامات مستندسازی برای انتقال شواهد	
۵۵	کتاب‌نامه	

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- راهنماهایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی (دیجیتالی)» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و پنجمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۵ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مآخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27037: 2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

فناوری اطلاعات - فنون امنیتی - راهنماهایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی (دیجیتالی)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنماهایی برای فعالیتهای خاص در ساماندهی به شواهد رقمی (دیجیتالی) است. این فعالیتهای خاص، فعالیتهای شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی می‌باشند که ممکن است دارای ارزش استنادی باشند. این استاندارد ملی با توجه به موقعیتهای مشترک، راهنمایی را برای افراد فراهم می‌سازد که در فرآیند ساماندهی شواهد رقمی با آنها مواجه می‌شوند و به سازمان‌ها در راستای اجرای روش‌های اجرایی انضباطی و همین‌طور تسهیل در تبادل شواهد رقمی بالقوه بین حوزه‌های قضایی کمک می‌کند.

این استاندارد ملی برای افزارها و/یا کارکردهای زیر راهنمایی ارائه می‌دهد که در شرایط گوناگون مورد استفاده قرار می‌گیرند:

- رسانه‌های ذخیره‌سازی رقمی که در رایانه‌های استاندارد مورد استفاده قرار می‌گیرند، مانند رانه‌های سخت^۱، لوح‌های فلپی^۲، لوح‌های نوری^۳ و نوری مغناطیسی^۴، افزارهای داده با کارکردهای مشابه،

- تلفن‌های همراه، دستیاران رقمی شخصی (PDAs)^۵، افزارهای الکترونیک شخصی (PEDs)^۶، کارت‌های حافظه،

- سامانه‌های ناوبری سیار،

- دوربین‌های عکاسی رقمی و ویدیویی (برای مثال تلویزیون مدار بسته (CCTV)^۷)،

- رایانه استاندارد با اتصالات شبکه،

- شبکه‌های مبتنی بر قرارداد کنترل انتقال / قرارداد اینترنت (TCP/IP)^۸ و دیگر قراردادهای رقمی و

- افزارهای دارای کارکرد مشابه با موارد فوق.

یادآوری ۱- فهرست افزارهای بالا یک فهرست نمونه بوده و جامع نمی‌باشد.

1 - Hard drives

2 - Floppy disks

3 - Optical

4 - Magneto optical

5 - Personal Digital Assistants

6 - Personal Electronic Devices

7 - Closed-circuit television

8 - Transmission Control Protocol / Internet protocol

یادآوری ۲- در برخی شرایط، افزاره‌های فوق در شکل‌های گوناگون وجود دارند. برای نمونه، سامانه خودرو ممکن است شامل سامانه ناوبری سیار، ذخیره داده و سامانه حسگر باشد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۱-۲ استاندارد ملی ایران شماره ۱۷۰۲۵: سال ۱۳۸۶، الزامات عمومی برای احراز صلاحیت آزمایشگاه‌های آزمون و کالیبراسیون

2-2 ISO/TR 15801, Document management — Information stored electronically — Recommendations for trustworthiness and reliability

2-3 ISO/IEC 17020, Conformity assessment — Requirements for the operation of various types of bodies performing inspection¹

2-4 ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary²

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در ISO/IEC 27000، ISO/IEC 17020، ISO/IEC 17025 و ISO/TR 15801، اصطلاحات و تعاریف زیر نیز به کار می‌رود:

۱-۳

اکتساب

فرآیند به وجود آوردن رونوشت از داده، داخل یک مجموعه‌ی تعریف‌شده است.

یادآوری- محصول اکتساب، رونوشتی بالقوه از شواهد رقمی است.

۱ - استاندارد بین‌المللی ISO/IEC 17020:1998 در سال ۱۳۸۱ با شماره ملی ۱۷۰۲۰ منتشر شده است.

۲ - استاندارد بین‌المللی ISO/IEC 27000:2009 در سال ۱۳۹۱ با شماره ملی ۲۷۰۰۰ منتشر شده است.

۲-۳

فضای تخصیص یافته^۱

ناحیه‌ای روی رسانه‌ی رقمی است که شامل حافظه‌ی اصلی بوده و برای ذخیره‌سازی داده‌ای که شامل فراداده است، به کار می‌رود.

۳-۳

جمع‌آوری

فرآیند گردآوری اقلام فیزیکی است که شامل شواهد رقمی بالقوه است.

۴-۳

افزایه‌ی رقمی

تجهیزات الکترونیکی است که برای پردازش یا ذخیره‌ی داده‌ی رقمی به کار می‌رود.

۵-۳

شواهد رقمی

اطلاعات یا داده‌ای که در شکل دودویی ذخیره یا منتقل شده است، که ممکن است به آن‌ها به عنوان شواهد استناد شود.

۶-۳

رونوشت شواهد رقمی

رونوشت شواهد رقمی است که برای حفظ اطمینان‌پذیری شواهد، با لحاظ کردن شواهد رقمی و ابزار درستی‌سنجی تولید شده است که روش درستی‌سنجی می‌تواند تعبیه شده یا مستقل از ابزار مورد استفاده در درستی‌سنجی، باشد.

۷-۳

اولین پاسخگوی شواهد رقمی

^۲ (DEFR)

فردی است دارای اختیار، آموزش دیده و شایسته برای اقدام اول در صحنه‌ی وقوع، برای جمع‌آوری و اکتساب شواهد رقمی و مسؤول ساماندهی به شواهد است.

یادآوری - اختیار، آموزش و شایستگی الزامات مورد انتظاری هستند که برای تولید شواهد رقمی مطمئن ضروری هستند، ولی ممکن است شرایط ویژه به نحوی باشد که فرد به هر سه الزام وفادار نباشد. در این مورد توصیه می‌شود، قانون محلی، سیاست سازمانی و شرایط ویژه در نظر گرفته شوند.

1- Allocated space

2 - Digital Evidence First Responder

۸-۳

متخصص شواهد رقمی

^۱(DES)

فردی است که می‌تواند وظایف DEFR را انجام دهد و دانش، مهارت‌ها و توانایی‌های ویژه‌ای برای اداره‌ی حوزه‌ی وسیعی از مسایل فنی دارد.

یادآوری - ممکن است DES مهارت‌های دیگری نیز داشته باشد، مانند اکتساب شبکه، اکتساب RAM، نرم‌افزار سامانه عامل یا دانش پردازنده‌ی مرکزی.

۹-۳

محیط ذخیره‌سازی رقمی

افزارهای که داده‌ی رقمی مجاز می‌تواند بر روی آن ثبت گردد.

[استاندارد ملی ایران به شماره‌ی ۱۰۰۲۷: سال ۱۳۸۶]

۱۰-۳

تسهیلات حفاظت از شواهد

محیط امن یا مکانی که شواهد اکتساب شده یا جمع‌آوری شده، ذخیره شده است.

یادآوری - توصیه می‌شود تسهیلات نگهداری و حفاظت شواهد در معرض میدان‌های مغناطیسی، گرد و غبار، لرزش، رطوبت یا هر گونه عوامل محیطی دیگر (مانند دمای بالا یا رطوبت) قرار نگیرند، زیرا ممکن است موجب آسیب شواهد رقمی بالقوه‌ی درون تسهیلات شود.

۱۱-۳

مقدار درهم‌ساز^۲

رشته‌ای از بیت‌ها که خروجی تابع درهم‌ساز است

[استاندارد ملی ایران به شماره‌ی ۹۵۹۸-۱: سال ۱۳۸۶]

۱۲-۳

شناسایی

فرآیندی است که عبارت است از جستجو برای تشخیص و مستندسازی شواهد رقمی بالقوه.

۱۳-۳

تصویرگیری^۳

فرآیند خلق یک رونوشت به صورت بیت به بیت از رسانه‌ی ذخیره‌سازی رقمی است.

1- Digital Evidence Specialist

2- Hash value

3- Imaging

یادآوری - یک رونوشت به صورت بیت به بیت، رونوشت فیزیکی نیز نامیده می‌شود.

مثال: هنگام تصویرگیری از راننده سخت ، DEFR از داده‌ای که حذف شده‌اند نیز رونوشت می‌گیرد.

۱۴-۳

افزازه جانبی^۱

افزاده‌ای است که برای توسعه کارکرد، به افزاره رقمی ملحق می‌شود.

۱۵-۳

حافظت

فرآیند نگهداری و محافظت از یکپارچگی و/ یا وضعیت اصلی شواهد رقمی بالقوه است.

۱۶-۳

اطمینان‌پذیری

ویژگی سازگاری با رفتار و نتایج مورد نظر.

[استاندارد ملی ایران به شماره‌ی ۲۷۰۰۰: سال ۱۳۹۱]

۱۷-۳

تکرارپذیری

ویژگی فرآیندی است که منجر به گرفتن نتایج یکسان از آزمون در همان محیط آزمون می‌شود (رایانه یکسان، لوح سخت یکسان، حالت عملکرد یکسان و غیره)

۱۸-۳

قابلیت بازتولید

ویژگی فرآیندی است که منجر به گرفتن نتایج یکسان آزمون در محیط آزمون متفاوت می‌شود (رایانه متفاوت، لوح سخت متفاوت، عملکرد متفاوت و غیره)

۱۹-۳

تبداه‌سازی^۲

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

۲۰-۳

زمان سامانه

زمانی است که به‌وسیله‌ی ساعت سامانه تولید شده و توسط سامانه عامل استفاده می‌شود، نه آن زمانی که

1 - Peripheral

2 - Spoliation

توسط سامانه عامل محاسبه می‌شود.

۲۱-۳

دست‌کاری^۱

اقدام عمدی به تغییر دادن یا اجازه به تغییر شواهد رقمی است (برای مثال تباه‌سازی عمدی یا هدفمند).

۲۲-۳

مُهر زمانی^۲

پارامتر متغیر زمان است که یک نقطه از زمان را با توجه به زمان مرجع مشترک مشخص می‌کند.

[ISO/IEC 11770-1:1996]

۲۳-۳

فضای تخصیص نیافته

ناحیه‌ای در رسانه‌ی رقمی، شامل حافظه‌ی اصلی، که توسط سامانه عامل اختصاص نیافته و برای ذخیره‌سازی داده‌ای چون فراداده، در دسترس است.

۲۴-۳

اعتبارسنجی

تایید از طریق ارائه مدرک عینی، که الزامات مورد نظر برای کاربرد یا استفاده خاص را تامین نماید.

[استاندارد ملی ایران به شماره ۱۴۰۹۶: سال ۱۳۸۹]

۲۵-۳

تابع درستی‌سنجی

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

یادآوری ۱- نباید حاصل اجرای تابع درستی‌سنجی دو مجموعه داده‌ی غیر یکسان، منجر به نتیجه انطباق (یکسانی) مجموعه‌ها با یکدیگر شود.

یادآوری ۲- توابع درستی‌سنجی به طور معمول با استفاده از توابع درهم‌ساز مانند MD5، SHA1 و مانند آن پیاده‌سازی می‌شوند، ولی روش‌های دیگری هم ممکن است استفاده شوند.

۲۶-۳

داده‌ی فرار^۳

داده‌ای است که به طور خاصی مستعد تغییر است و می‌تواند به راحتی تعدیل شود.

1- Tampering
2- Timestamp
3- Volatile data

یادآوری - تغییر می‌تواند خاموش کردن منبع یا گذر از یک میدان مغناطیسی باشد. داده‌ی فرآر همچنین می‌توانند شامل داده‌هایی نیز باشند که با تغییر حالت سامانه، تغییر می‌کند. داده‌ای که در RAM ذخیره شده‌اند و آدرس‌های IP پویا از جمله مثال‌های این نوع هستند.

۴ کوتاه‌نوشت‌ها

AVI	Audio Video Interleave	جای‌دهی صوت و تصویر
CCTV	Closed Circuit Television	تلویزیون مدار بسته
CD	Compact Disk	لوح فشرده
DNA	Deoxyribonucleic Acid	اسید دئوکسی ریبونوکلیک
DEFR	Digital Evidence First Responder	اولین پاسخگوی شواهد رقمی
DES	Digital Evidence Specialist	متخصص شواهد رقمی
DVD	Digital Video/Versatile Disk	لوح تصویری رقمی / همه کاره
ESN	Electronic Serial Number	شماره ترتیبی الکترونیکی
GPS	Global Positioning System	سامانه مکان‌یابی جهانی
GSM	Global System for Mobile Communication	سامانه جهانی برای ارتباطات سیار
IMEI	International Mobile Equipment Identity	هویت تجهیزات سیار بین‌المللی
IP	Internet Protocol	قرارداد اینترنت
ISIRT	Information Security Incident Response Team	گروه پاسخگوی رخداد امنیتی اطلاعات
LAN	Local Area Network	شبکه محلی
MD5	Message-Digest Algorithm 5	الگوریتم چکیده پیام شماره ۵
MP3	MPEG Audio Layer 3	لایه صوتی نماوادیس (MPEG) ۱ ^۱ سه
MPEG	Moving Picture Experts Group	گروه متخصصان تصویر متحرک (نماوادیس)
NAS	Network Attached Storage	ذخیره‌ساز پیوست شده به شبکه
PDA	Personal Digital Assistant	دستیار رقمی شخصی
PED	Personal Electronic Device	افزاره‌ی الکترونیکی شخصی
PIN	Personal Identification Number	شماره‌ی شناسایی شخصی
PUK	PIN Unlock Key	کلید بازگشایی PIN
RAID	Redundant Array of Independent Disks	آرایه‌ی افزونه از لوح‌های مستقل
RAM	Random Access Memory	حافظه دستیابی تصادفی
RFID	Radio Frequency Identification	شناسایی از طریق بسامد رادیویی

1 - Moving Picture Experts Group, Motion Picture Experts Group

SAN	Storage Area Network	شبکه ناحیه ذخیره‌سازی
SHA	Secure Hash Algorithm	الگوریتم درهم‌ساز امن
SIM	Subscriber Identity Module	پودمان هویت مشترک
USB	Universal Serial Bus	همه‌گذر
UPS	Uninterruptible Power Supply	منبع تغذیه‌ی وقفه‌ناپذیر
USIM	Universal Subscriber Identity Module	پودمان هویت مشترک جهانی
UV	Ultraviolet	فرابنفش
Wi-Fi	Wireless Fidelity	بی‌سیم

۵ مرور کلی

۱-۵ زمینه جمع‌آوری شواهد رقمی

شواهد رقمی در تعدادی از فرانامه‌های^۱ متمایز، قابل استفاده می‌باشند که هر کدام از این فرانامه‌ها، توازن متفاوتی را بین گردانندگان کیفیت استنادی، محورهای زمان تحلیل، بازسازی خدمات و هزینه جمع‌آوری شواهد رقمی داراست. بنابراین سازمان‌ها به یک فرآیند اولویت‌بندی نیازمند خواهند بود که احتیاجات را مشخص می‌کند و کیفیت استنادی، به‌موقع بودن و بازسازی خدمات را قبل از به کارگیری منابع DEFR به تعادل می‌رساند. یک فرآیند اولویت‌بندی عبارت است از انجام ارزشیابی مواد در دسترس ب، رای تعیین ارزش استنادی محتمل و توصیه برای اینکه با چه ترتیبی شواهد رقمی بالقوه جمع‌آوری، اکتساب یا محافظت شود. اولویت‌بندی برای کمینه کردن مخاطره‌ی از بین رفتن شواهد رقمی بالقوه و بیشینه کردن ارزش استنادی شواهد رقمی بالقوه‌ی جمع‌آوری شده، انجام می‌شود.

۲-۵ اصول شواهد رقمی

در بیشتر حوزه‌های قضایی و سازمان‌ها، شواهد رقمی تحت کنترل سه اصل بنیادی هستند: مرتبط بودن، اطمینان‌پذیری و کفایت. این سه اصل نه تنها برای شواهد رقمی قابل قبول در دادگاه، بلکه برای همه‌ی تجسس‌ها مهم هستند. شواهد رقمی زمانی مرتبط هستند که برای اثبات یا رد عنصری از مورد خاص در حال تجسس مورد استفاده قرار گیرند. با وجود این که تعریف تفصیلی «قابل اطمینان» در میان حوزه‌های قضایی، متنوع است، معنای عمومی این اصل که به صورت فراگیر پذیرفته شده این است: «اطمینان از این که شواهد رقمی همانی است که باید باشد». یک DEFR لزومی ندارد که همیشه همه‌ی داده را جمع‌آوری کند یا یک رونوشت کامل از شواهد رقمی اصلی بسازد. در بسیاری از حوزه‌های قضایی، مفهوم کفایت به این معناست که DEFR، شواهد رقمی بالقوه‌ی کافی را جمع‌آوری کند تا امکان بررسی یا تجسس مناسب در مورد عناصر موضوع فراهم شود. برای DEFR درک این مفهوم به منظور اولویت‌بندی مناسب تلاش در موقعی که زمان یا هزینه مورد نظر است، اهمیت دارد.

یادآوری- توصیه می‌شود DEFR اطمینان حاصل کند که جمع‌آوری شواهد رقمی بالقوه مطابق با آیین‌نامه‌ها و قوانین قضایی

محلی است، همان گونه که به وسیله‌ی شرایط محیطی خاص درخواست شده است.

توصیه می‌شود همه‌ی فرآیندها که به وسیله DEFR و DES استفاده شده‌اند، از قبل برای استفاده اعتبارسنجی شده باشند. اگر اعتبارسنجی از خارج انجام شود، توصیه می‌شود DEFR یا TDES تایید نماید که این اعتبارسنجی برای استفاده‌ی خاص آن‌ها از فرآیندها و محیط و شرایطی که فرآیندها در آن استفاده می‌شوند، مناسب است. همچنین توصیه می‌شود یک DEFR یا DES: الف- همه‌ی فعالیت‌ها را مستندسازی کند؛

ب- روشی را برای برقراری درستی و اطمینان‌پذیری رونوشت شواهد رقمی بالقوه در قیاس با منبع اصلی تعیین کند و به کار گیرد؛ و

پ- تشخیص دهد که اقدام محافظت از شواهد رقمی بالقوه نمی‌تواند همیشه بدون دخالت باشد.

۳-۵ الزامات برای ساماندهی به شواهد رقمی

۱-۳-۵ عمومی

اصولی که در زیربند ۵-۲ در بالا آمد، به صورت زیر قابل توجیه هستند:

- مرتبط بودن^۱: توصیه می‌شود که بتوان نشان داد که مدارک کسب شده با تجسس‌ها مرتبط هستند. برای مثال، شامل اطلاعات ارزشمندی جهت کمک به تجسس در مورد یک رخداد ویژه است و این که دلیل خوبی برای به دست آوردن آن وجود داشته باشد. توصیه می‌شود شخص DEFR بتواند از طریق ساماندهی و توجیه، رویه‌های دنبال شده را توصیف کرده و توضیح دهد که چگونه برای به دست آوردن هر قلم تصمیم گرفته است.

- اطمینان‌پذیری^۲: توصیه می‌شود همه‌ی فرآیندهایی که در ساماندهی به شواهد رقمی بالقوه استفاده می‌شوند، قابل ممیزی و تکرارپذیر باشند. توصیه می‌شود نتایج به کارگیری چنین فرآیندهایی قابلیت بازتولید داشته باشند.

- کفایت^۳: توصیه می‌شود شخص DEFR توجه داشته باشد که مدارک کافی برای فراهم کردن امکان اجرای یک تجسس مناسب گردآوری شده باشد. توصیه می‌شود شخص DEFR بتواند از طریق ممیزی و توجیه، شاخصی ارائه دهد که در مجموع چه مقدار از مدارک مورد ملاحظه قرار گرفته می‌شود و رویه‌ها به طور معمول تصمیم می‌گیرند که چه مقدار و از کدام مدارک اکتساب نمایند.

یادآوری- مدارک ممکن است از طریق فعالیت‌های اکتساب و/یا فعالیت‌های جمع‌آوری، گردآوری شوند.

1- Relevance
2- Reliability
3- Sufficiency

چهار جنبه‌ی کلیدی در ساماندهی به شواهد رقمی وجود دارد: قابلیت ممیزی^۱، توجیه‌پذیری^۲ و وابسته به شرایط ویژه‌ی محیطی، تکرار پذیری یا قابلیت بازتولید.

۲-۳-۵ قابلیت ممیزی

توصیه می‌شود امکان ارزیابی فعالیت‌های انجام شده توسط DES و DEFR، برای ارزیاب مستقل یا دیگر بخش‌های ذی‌نفع مجاز، فراهم باشد. این امر با مستندسازی مناسب همه فعالیت‌های انجام شده، ممکن است. توصیه می‌شود DES و DEFR قادر به توجیه فرآیند تصمیم‌گیری در انتخاب یک سری از فعالیت‌های انتخابی، باشند. توصیه می‌شود فرآیندهایی که توسط DES و DEFR اجرا شدند، برای ارزیابی مستقل در دسترس باشند تا معین گردند که روش یا فن یا رویه علمی مناسب پیگیری شده است.

۳-۳-۵ تکرارپذیری

تکرارپذیری وقتی برقرار است که نتایج یکسان آزمون تحت شرایط زیر تولید می‌شوند:

- استفاده از رویه و روش سنجش یکسان؛

- استفاده از وسایل یکسان تحت شرایط مشابه؛ و

- بتواند در هر زمانی بعد از آزمون اصلی تکرار شود.

توصیه می‌شود یک DEFR باتجربه و دارای مهارت بسیار، بتواند متعهد شود که همه‌ی فرآیندها، بدون راهنمایی یا تفسیر، در سند توصیف شده‌اند و به نتایج یکسان رسیده‌اند. توصیه می‌شود شخص DEFR از این موضوع آگاه باشد که ممکن است شرایطی وجود داشته باشد که نتوان در آن آزمون را تکرار کرد، برای مثال هنگامی که یک لوح سخت اصلی رونوشت شده است و بعد از آن لوح سخت، مجدد مورد استفاده قرار گرفته است، یا هنگامی که یک قلم دارای حافظه‌ی فرآر است. در این مورد، توصیه می‌شود DEFR از فرآیند تکرارپذیری، کنترل کیفیت و مستندسازی فرآیندی مطمئن شود.

۴-۳-۵ قابلیت بازتولید

قابلیت بازتولید هنگامی برقرار است که نتایج یکسان آزمون تحت شرایط زیر تولید گردد:

- استفاده از روش سنجش یکسان؛

- استفاده از وسایل متفاوت و تحت شرایط متفاوت؛ و

- قابلیت بازتولید در هر زمان بعد از آزمون اصلی.

نیازها برای بازتولید نتایج، مطابق با حوزه‌های قضایی و شرایط تغییر می‌کند، بنابراین نیاز است تا خود

1- Auditability

2- Justifiability

DEFR یا شخصی که بازتولید را انجام می‌دهد در مورد شرایط کاربرپذیر مطلع باشد.

۵-۳-۵ توجیه پذیری

توصیه می‌شود DEFR توانایی توجیه همه‌ی فعالیت‌ها و روش‌های به کار رفته در ساماندهی به شواهد رقمی بالقوه را داشته باشد. توجیه‌پذیر بودن می‌تواند با اثبات این که این تصمیم بهترین انتخاب برای به‌دست آوردن همه‌ی شواهد رقمی بالقوه بوده است، به‌دست آید. یک DEFR یا DES دیگر نیز می‌تواند این را به‌وسیله‌ی بازتولید موفق یا اعتبارسنجی فعالیت‌ها و روش‌های به کار رفته، اثبات کند.

بهترین حالت برای یک سازمان این است که یک DEFR یا DES با مهارت‌های اصلی و صلاحیت مشروح در پیوست الف از این استاندارد ملی را جذب نماید. این امر تضمین خواهد کرد که از فرآیندهای صحیح و رویه‌های صحیح، در هنگام ساماندهی به شواهد رقمی بالقوه پیروی می‌شود و تضمین خواهد کرد که از شواهد رقمی که ممکن است ارزش استنادی داشته باشند، محافظت می‌شود. همچنین این امر نیز تضمین خواهد کرد که سازمان‌ها قادر خواهند بود از شواهد رقمی بالقوه استفاده کنند، برای مثال در رویه‌های انضباطی خود یا تسهیل تبادل شواهد رقمی بالقوه بین حوزه‌های قضایی.

یادآوری - شایستگی شرح داده شده در پیوست الف، محدود به عملکرد DEFR است که همسو با نقش DES که در زیربند ۳-۸ شرح داده شده است، می‌باشد.

۴-۵ فرآیندهای ساماندهی شواهد رقمی

۱-۴-۵ مرور کلی

اگرچه فرآیند کامل ساماندهی به شواهد رقمی شامل فعالیت‌های دیگر است (یعنی ارائه، امحا و غیره)، اما حوزه‌ی این استاندارد ملی تنها مربوط به فرآیند ساماندهی اولیه است که متشکل از شناسایی، جمع‌آوری، اکتساب و محافظت از شواهد رقمی بالقوه است.

شواهد رقمی به طور طبیعی شکننده هستند و توسط آزمایش یا ساماندهی نامناسب، می‌تواند تغییر یابد و دست‌کاری یا نابود شود. توصیه می‌شود ساماندهی‌کنندگان شواهد رقمی، برای شناسایی و مدیریت مخاطرات و پیامدهای دوره‌های عمل بالقوه در زمان ساماندهی به شواهد رقمی، صلاحیت داشته باشند. خرابی در ساماندهی مناسب افزارهای رقمی می‌تواند منجر به غیرقابل استفاده شدن شواهد رقمی بالقوه‌ی ایجاد شده و مشمول در آن افزارهای رقمی شود.

توصیه می‌شود DEFR و DES از رویه‌های مستند شده پیروی کنند تا مطمئن شوند که یکپارچگی و اطمینان‌پذیری شواهد رقمی بالقوه حفظ می‌شوند. توصیه می‌شود رویه‌ها شامل راهنمایی‌های ساماندهی به منابع شواهد رقمی بالقوه باشند و توصیه می‌شود شامل اصول بنیادی زیر باشند:

- کمینه کردن ساماندهی به افزارهای رقمی اصلی یا شواهد رقمی بالقوه؛

- به حساب آوردن هرگونه تغییرات و مستندسازی اقدامات انجام شده (تا حدی که یک فرد خبره می‌تواند یک نظریه را با اطمینان‌پذیری شکل دهد)؛

- مطابقت با قواعد محلی شواهد؛ و

- توصیه نمی‌شود DEFR و DES بیشتر از صلاحیتشان اقدامی انجام دهند.

توصیه می‌شود شواهد، مطابق با این اصول بنیادین و الزامات ساماندهی به شواهد رقمی بالقوه حفظ شوند. به خصوص در مواردی که باید تغییرات غیرقابل اجتناب ایجاد شود، همه‌ی اقدامات و توضیحات نیاز به مستند شدن دارند. هر فرآیند ساماندهی به شواهد رقمی، که عبارتند از شناسایی، جمع‌آوری، اکتساب و محافظت، در بندهای بعدی به تفصیل شرح داده شده‌اند.

۵-۴-۲ شناسایی

شواهد رقمی در شکل فیزیکی و منطقی بازنمایی می‌شوند. شکل فیزیکی شامل بازنمایی داده درون یک افزاره‌ی محسوس است. شکل منطقی شواهد رقمی بالقوه به بازنمایی مجازی داده‌ی درون یک افزاره اشاره دارد.

فرآیند شناسایی عبارت از جستجو برای تشخیص و مستندسازی شواهد رقمی بالقوه است. توصیه می‌شود فرآیند شناسایی، رسانه‌ی ذخیره‌سازی رقمی و افزاره‌های پردازشی که ممکن است شامل شواهد رقمی بالقوه‌ی مرتبط با رخداد باشند را شناسایی کند. این فرآیند همچنین شامل فعالیتی برای اولویت‌بندی جمع‌آوری شواهد بر اساس فرآر بودنشان نیز هست. توصیه می‌شود فرآر بودن داده شناسایی شود تا به فرمان صحیح جمع‌آوری و اکتساب فرآیندها اطمینان دهد که خسارت بر شواهد رقمی بالقوه کمینه می‌شود و بهترین شواهد به دست می‌آیند. علاوه بر این توصیه می‌شود، فرآیند احتمال شواهد رقمی بالقوه‌ی مخفی را شناسایی کند. توصیه می‌شود DEFR و DES آگاه باشند که همه‌ی انواع رسانه‌های ذخیره‌سازی رقمی نمی‌توانند به راحتی شناسایی و مکان‌یابی شوند، برای مثال رایانش ابرین، NAS و SAN - که همگی یک مولفه‌ی مجازی به فرآیند شناسایی اضافه می‌کنند.

توصیه می‌شود DEFR به صورت نظام‌مند یک جستجوی کامل برای اقلامی که ممکن است شامل شواهد رقمی بالقوه باشند، انجام دهد. انواع مختلفی از افزاره‌های رقمی که ممکن است شامل شواهد رقمی بالقوه باشند می‌توانند به راحتی مورد چشم‌پوشی قرار گیرند (برای مثال به دلیل اندازه‌ی کوچک)، تغییر قیافه یابند یا در بین دیگر مدارک نامربوط آمیخته شوند.

زیربندهای ۶-۱ و ۶-۶ اطلاعات بیشتری در مورد زنجیره‌ی حفاظت، بسته‌بندی و جنبه‌های برچسب‌گذاری برای شناسایی شواهد رقمی مهیا می‌سازند. بند ۷ راهنمایی‌هایی را مشخص می‌کند که مرتبط با نمونه‌های خاص از شناسایی، جمع‌آوری، اکتساب و حفاظت شواهد رقمی هستند.

۳-۴-۵ جمع‌آوری

وقتی آن دسته از افزارهای رقمی که ممکن است شامل شواهد رقمی باشند، شناسایی می‌شوند، توصیه می‌شود DEFR و DES تصمیم بگیرند که آیا باید جمع‌آوری شوند یا در طول فرآیند بعدی اکتساب گردند. تعدادی از عوامل تصمیم‌گیری برای این مورد وجود دارد که در بند ۷ با جزئیات بیشتر شرح داده می‌شود. توصیه می‌شود تصمیم بر اساس شرایط موجود گرفته شود.

جمع‌آوری فرآیندی است در فرآیند ساماندهی به شواهد رقمی در مواقعی که افزارهایی که ممکن است شامل شواهد رقمی بالقوه باشند، از مکان اصلی خود حذف شده‌اند تا در آزمایشگاه یا یک محیط کنترل شده دیگر، مورد اکتساب یا تحلیل بعدی قرار گیرند. افزارهایی که شامل شواهد رقمی بالقوه هستند ممکن است در یکی از این دو حالت باشند: وقتی سامانه روشن است یا وقتی که سامانه خاموش است. بسته به حالت افزار، رویکردها و ابزارهای مختلفی مورد نیاز است. رویه‌های محلی می‌تواند به رویکردها و ابزارهای استفاده شده برای فرآیند جمع‌آوری، اعمال شود.

این فرآیند شامل مستندسازی کل رویکرد و نیز بسته‌بندی این افزارها قبل از انتقال می‌باشد. برای DEFR و DES مهم است که هر گونه مدارکی که ممکن است مربوط به اطلاعات رقمی بالقوه باشد را جمع‌آوری کند (برای نمونه، کاغذی که روی آن اسم‌رمزها نوشته شده است، رابط‌های مرتبط با برای افزارهای سامانه‌ی تعبیه شده). شواهد رقمی بالقوه ممکن است، در صورت عدم توجه منطقی و صحیح، آسیب‌دیده یا گم شوند. توصیه می‌شود DEFR و DES بهترین روش ممکن جمع‌آوری مبتنی بر موقعیت، هزینه و زمان را اتخاذ کنند.

یادآوری ۱- حذف رسانه‌ی ذخیره‌سازی رقمی همیشه توصیه نمی‌شود و توصیه می‌شود DEFR مطمئن شود که آن‌ها برای حذف رسانه‌ی ذخیره‌سازی مناسب هستند و تشخیص دهد که چه زمانی برای انجام این کار مناسب است و اجازه دارد.

یادآوری ۲- توصیه می‌شود جزئیات افزارهای رقمی که جمع‌آوری نمی‌شوند، همراه با توجیه دلایل کنارگذاری، مطابق با الزامات حوزه‌های قضایی کاربردپذیر مستند شوند.

۴-۴-۵ اکتساب

فرآیند اکتساب عبارت است از تولید یک رونوشت شاهد رقمی (برای مثال لوح سخت کامل، افراز، پوشه-های منتخب) و مستندسازی روش‌های به کار رفته و فعالیت‌های اجرا شده. توصیه می‌شود DEFR یک روش مناسب اکتساب مبتنی بر موقعیت، هزینه و زمان اتخاذ کند و تصمیم را برای استفاده‌ی یک روش یا ابزار ویژه به صورت مناسب مستند نماید.

توصیه می‌شود روشی که برای کسب شواهد رقمی بالقوه استفاده می‌شود، به وضوح و به تفصیل مستند شده باشند و تا زمانی که از نظر عملی امکان‌پذیر باشد، باید از سوی یک DEFR شایسته، قابل بازتولید یا قایل

درستی‌سنجی باشند. توصیه می‌شود DEFR یا DES شواهد رقمی بالقوه را با کمترین روش دست‌کاری به‌دست آورد تا از مطرح کردن تغییرات تا جایی که ممکن است، اجتناب کند. در اجرای این فرآیند، توصیه می‌شود DEFR مناسب‌ترین روش را برای استفاده در نظر بگیرد. اگر فرآیند به تبدیلات غیر قابل اجتناب در داده‌ی رقمی منتج شد، توصیه می‌شود فعالیت‌های اجرا شده مستند شوند تا برای تغییرات در داده منظور گردند.

توصیه می‌شود روش اکتساب استفاده شده، رونوشتی از شواهد رقمی بالقوه یا افزاره‌های رقمی که ممکن است شامل شواهد رقمی بالقوه باشند، تولید کند. توصیه می‌شود هم منبع اصلی و هم رونوشت شواهد رقمی با یک کارکرد درست‌سنجی اثبات شده، درست‌سنجی شوند (اثبات شده به طور دقیق در همان نقطه از زمان) که این برای فردی که از شواهد استفاده خواهد کرد، قابل پذیرش است. توصیه می‌شود منبع اصلی و هر رونوشت شواهد رقمی خروجی کارکرد درست‌سنجی یکسانی تولید کنند.

در شرایطی که فرآیند درست‌سنجی قابل اجرا نیست، برای نمونه هنگام اکتساب از سامانه‌ی در حال اجرا، هنگامی که رونوشت اصلی شامل خطا است یا زمان دوره‌ی اکتساب محدود است، توصیه می‌شود DEFR از بهترین روش در دسترس ممکن استفاده کند و بتواند انتخاب این روش را توجیه کند و از آن دفاع نماید. اگر تصویرگیری قابل درست‌سنجی نیست، پس باید مستند و توجیه گردد. در صورت لزوم، توصیه می‌شود روش اکتساب استفاده شده، توانایی به‌دست آوردن فضای تخصیص‌یافته و تخصیص نیافته را داشته باشد.

یادآوری ۱- هنگامی که فرآیند درست‌سنجی به موجب خطاهای درون منبع نتواند در کل منبع اجرا شود، درست‌سنجی با استفاده از قسمت‌هایی از منبع که می‌تواند با اطمینان خوانده شود، می‌تواند به کار گرفته شود.

ممکن است مواردی وجود داشته باشند که برای خلق یک رونوشت شواهد رقمی از یک منبع شواهد امکان‌پذیر یا مجاز نباشند، به‌عنوان مثال وقتی منبع بسیار بزرگ است. در این موارد، یک DEFR ممکن است یک اکتساب منطقی را اجرا کند که فقط گونه‌ها، راهنماها و مکان‌های داده‌ای خاص را مورد هدف قرار می‌دهد. این امر به طور معمول در سطح یک پوشه یا بخش، فضایی را اشغال می‌کند. در طول اکتساب منطقی، بسته به روش استفاده شده، ممکن است پوشه‌های فعال و موارد غیر پوشه‌ای که فضایی روی رسانه‌ی ذخیره‌سازی رقمی به آن‌ها تخصیص داده شده است، رونوشت شوند؛ پوشه‌های حذف شده و فضای تخصیص نیافته رونوشت نشوند. موارد دیگری که این روش می‌تواند برای آن‌ها مفید باشد، هنگامی است که سامانه‌های ماموریت-بحران درگیر شده نمی‌توانند بسته یا خاموش شوند.

یادآوری ۲- برخی از حوزه‌های قضایی ممکن است رفتار خاصی را برای داده نیاز داشته باشند، برای نمونه آن را در پیشگاه صاحب داده مهر می‌زنند. توصیه می‌شود مهر زدن مطابق با الزامات محلی صورت پذیرد (قانونی و رویه‌ای).

۵-۴-۵ حافظت

توصیه می‌شود شواهد رقمی بالقوه برای اطمینان از مفید بودن خود در تجسس، مورد حفاظت قرار گیرند.

حفاظت از یکپارچگی شواهد اهمیت دارد. فرآیند حفاظت شامل تامین امنیت شواهد رقمی و و حراست از آن دسته از افزاره‌های رقمی که ممکن است حاوی شواهد رقمی باشند در برابر دست‌کاری پنهانی یا تباه‌سازی می‌باشد. توصیه می‌شود فرآیند حفاظت در سراسر فرآیندهای ساماندهی به شواهد رقمی، راه‌اندازی شده و نگهداری گردد، که از شناسایی افزاره‌های رقمی که حاوی شواهد رقمی بالقوه هستند، شروع می‌شود.

در بهترین نمونه‌ی کاربری، توصیه می‌شود هیچ تباه‌سازی برای خود داده یا فراداده‌ی همراه آن اتفاق نیافتد (برای مثال تاریخ و مهرهای زمانی). توصیه می‌شود DEFR بتواند اثبات کند که شواهد از زمانی که جمع‌آوری شده‌اند یا کسب شده‌اند، تغییر نیافته‌اند یا در صورتی که تغییرات غیرقابل اجتناب بوجود آمده‌اند، توضیحات و فعالیت‌های مستند شده را تولید کند.

یادآوری - در بعضی نمونه‌ها، محرمانگی شواهد رقمی بالقوه یک الزام است، چه الزام تجاری یا چه الزام قانونی (برای مثال حریم شخصی). توصیه می‌شود شواهد رقمی بالقوه در روشی که محرمانگی داده را قطعی می‌سازد، محافظت شوند.

۶ مولفه‌های کلیدی شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی

۱-۶ زنجیره توقیف^۱

توصیه می‌شود DEFR در هر تجسس قادر باشد مسئولیت همه داده‌های کسب شده و افزاره‌ها را در زمان زنجیره‌ی توقیف توسط DEFR بپذیرد. ثبت زنجیره‌ی توقیف، سندی است که حرکت و ساماندهی به شواهد رقمی بالقوه را در طول زمان شناسایی می‌کند. توصیه می‌شود این امر از جانب فرآیند جمع‌آوری یا اکتساب نهادینه گردد. این کار به طور معمول توسط ردیابی تاریخیچه هر قلم از لحظه‌ای که شناسایی شده، جمع‌آوری گردیده و توسط گروه تجسس به‌دست آمده تا موقعیت و مکان فعلی، انجام خواهد شد.

ثبت زنجیره‌ی توقیف، یک سند یا دنباله‌ای از اسناد مربوط به هم است که زنجیره‌ی توقیف را به تفصیل شرح می‌دهد و ثبت می‌کند که چه کسی برای ساماندهی به شواهد رقمی بالقوه، چه در قالب داده‌ی رقمی یا چه در قالب‌های دیگر (برای مثال یادداشت‌های کاغذی)، مسئول بوده است. هدف از نگهداری یک ثبت از زنجیره‌ی توقیف، ایجاد امکان برای شناسایی دسترسی و حرکت شواهد رقمی بالقوه در هر نقطه از زمان می‌باشد. ثبت زنجیره‌ی توقیف، ممکن است خودش بیشتر از یک سند را در بر داشته باشد، برای مثال برای شواهد رقمی بالقوه توصیه می‌شود یک ثبت سند هم‌زمان از اکتساب داده‌ی رقمی در یک افزاره‌ی ویژه، حرکت آن افزاره و استخراج دنباله‌ی ثبت مستندات یا رونوشت‌های شواهد رقمی بالقوه برای تحلیل یا اهداف دیگر، وجود داشته باشد. توصیه می‌شود ثبت زنجیره‌ی توقیف حداقل حاوی اطلاعات زیر باشد:

- شناسایی کننده‌ی شواهد منحصر به فرد؛

- کسی که به شواهد دست یافت و زمان و مکانی که رخ داد؛

- کسی که درون یا خارج از ابزار محافظت از شواهد، شواهد را بررسی کرد و زمانی که این اتفاق افتاد؛

1- Chain of custody

- چرا شواهد واریسی شد (چه موردی و با چه هدفی) و اعتبار مرتبط، اگر قابل اجرا باشد؛ و
- هرگونه تغییرات غیرقابل اجتناب بر شواهد رقمی بالقوه و همچنین نام فرد مسؤول و توجیه برای معرفی این تغییر.

توصیه می‌شود زنجیره‌ی توقیف در طول عمر شواهد نگهداری شود و برای یک دوره‌ی زمانی مشخص بعد از عمر شواهد نیز محافظت گردد- این دوره‌ی زمانی می‌تواند مطابق با حوزه‌های قضایی محلی در جمع‌آوری و کاربرد شواهد، تنظیم شود. توصیه می‌شود این امر باید از لحظه‌ای که افزارهای رقمی و/یا شواهد رقمی بالقوه کسب شده‌اند، برقرار باشد و توصیه می‌شود فاش نگردد.

یادآوری- برخی از حوزه‌های قضایی ممکن است الزامات خاصی در برابر زنجیره‌ی توقیف داشته باشند. توصیه می‌شود DEFR به آن الزامات وفادار باشد.

۲-۶ احتیاط در محل رخداد

۱-۲-۶ عمومی

توصیه می‌شود DEFR برای ایجاد امنیت و حفاظت مکان شواهد رقمی بالقوه، به محض رسیدن به محل، فعالیت‌هایی را اجرا کند. توصیه می‌شود فعالیت‌ها موارد زیر را تحت نظر قوانین محلی، پوشش دهند:

- ایجاد امنیت و تحت کنترل گرفتن محلی که حاوی افزارها است؛

- مشخص کردن این که چه کسی مسؤول این مکان است؛

- اطمینان از این که افراد از افزارها و منابع قدرت به دور هستند؛

- هر کس که به مکان دسترسی دارد یا هرکس که ممکن است دلیلی برای شرکت در صحنه‌ی وقوع داشته باشد، مستند شود؛

- اگر وسیله روشن است خاموش نشود و اگر خاموش است روشن نشود؛

- در صورت امکان، از صحنه مستندسازی صورت پذیرد (برای مثال طرح، عکس یا تصویر)، که آیا همه‌ی مولفه‌ها و کابل‌ها در مکان اصلی خود هستند. اگر هیچ دوربین و/یا دوربین فیلم‌برداری در دسترس نیست، یک نقشه‌ی طرح از سامانه بکشید و کابل‌ها و درگاه‌ها را برچسب‌گذاری کنید به‌طوری که سامانه بعدها اعتبارسنجی شده و از نو ساخته شود؛ و

- در صورت اجازه داشتن، نواحی را برای اقلامی مانند یادداشت‌های یادآوری امور روزانه، خاطرات، برگه‌ها، رایانه‌های کتابی^۱، یا راهنمای نرم‌افزار و سخت‌افزار با جزییات حیاتی در مورد افزارهایی چون اسم‌رمزها و PIN ها، جستجو کنید.

یادآوری ۱- برخی از حوزه‌های قضایی ممکن است الزامات خاصی برای پذیرفتن شواهد تصویری یا عکس‌ها، داشته باشند. توصیه می‌شود یک DEFR به این الزامات وفادار باشد.

یادآوری ۲- باید DEFRها آگاه باشند که شواهد رقمی بالقوه ممکن است همیشه در مکان‌های آشکار وجود نداشته باشند، برای مثال ذخیره‌ساز مجازی یا توزیع شده.

توصیه می‌شود DEFR ابتدا همه مخاطرات مرتبط با اجرای همه‌ی فرآیندها در طول تجسس را بشناسد. توصیه می‌شود به حفاظت شواهد رقمی بالقوه و کارکنان در صحنه‌ی وقوع، توجه شود.

۲-۲-۶ کارکنان

انجام ارزیابی مخاطره راجع به ایمنی کارکنان پیش از شروع فرآیند بسیار مهم است، چرا که ایمنی کارکنان شرکت‌کننده در فرآیند، حیاتی است. در زیر مسایل مربوط به ارزیابی مخاطرات برای کارکنان در نظر گرفته شده‌اند ولی فقط به موارد زیر محدود نمی‌شوند:

- آیا افراد تجسس شده، حضور پیدا خواهند کرد؟ اگر حضور یابند، آیا تمایلی نسبت به خشونت دارند؟

- در طول چه زمانی از روز، عملکرد هدایت خواهد شد؟

- آیا صحنه‌ی وقوع می‌تواند در دید تماشاگران نباشد؟

- آیا اسلحه‌ای در آن ناحیه وجود دارد؟

- آیا هرگونه خطر فیزیکی برای فرد/افراد وجود دارد؟

- آیا چیزی هم‌چون افزاره می‌تواند در اطراف با قصد به وجود آوردن آسیب فیزیکی پیکربندی شده باشد، البته در صورتی که در یک روش غیر مناسب ساماندهی شده باشد؛ برای مثال تله‌ی پنهان شده؟

- آیا احتمال دارد که مدارک جمع‌آوری شده باعث هجوم یا آسیب روانی شود؟

- آیا ممکن است صحنه‌ی وقوع ناامن باشد؟

- آیا نواحی اطراف اثری بر عامل مخاطره دارند؟

۳-۲-۶ شواهد رقمی بالقوه

توصیه می‌شود DEFR هنگام استفاده از ابزار خاص برای جمع‌آوری یا به دست آوردن شواهد رقمی بالقوه، با احتیاط باشد. حساب نکردن مخاطرات قبل از اقدام ممکن است منجر به از دست رفتن قسمتی یا همه‌ی شواهد رقمی بالقوه به علت فناوری به کار رفته در طول جمع‌آوری یا اکتساب شود. توصیه می‌شود مخاطرات برای کاهش ادعاهای خسارت مورد ارزیابی قرار گیرند.

- ارزیابی مخاطره عبارت است از یک ارزشیابی نظام‌مند از مخاطرات و اثرات بالقوه که ممکن است در

تجسس شواهد رقمی موثر باشند. جنبه‌هایی که در طول ارزیابی مخاطره برای شواهد رقمی بالقوه ملاحظه می‌شوند شامل موارد زیر است، ولی به موارد زیر محدود نمی‌شوند:

- چه نوع روش‌های جمع‌آوری/اکتساب به کار گرفته می‌شود؟
- چه تجهیزاتی ممکن است در محل مورد نیاز باشد؟
- میزان فرآر بودن داده و اطلاعات مربوط به شواهد رقمی بالقوه در چه سطحی است؟
- آیا دسترسی از راه دور به هرکدام از افزاره‌های رقمی ممکن است و آیا این به‌عنوان یک راه چاره برای یکپارچگی شواهد مطرح است؟
- اگر داده/تجهیزات آسیب ببینند چه اتفاقی می‌افتد؟
- آیا داده قابل فاش شدن می‌باشد؟
- آیا افزاره‌ی رقمی می‌تواند طوری پیکربندی شود (برای مثال با استفاده از یک بمب منطقی) که در صورت قطع کلید یا دسترسی کنترل نشده، داده را خراب کند، از بین ببرد یا مبهم سازد؟

۳-۶ نقش‌ها و مسئولیت‌ها

نقش DEFR در بر دارنده‌ی شناسایی، جمع‌آوری، اکتساب و محافظت شواهد رقمی بالقوه در صحنه‌ی وقوع می‌باشد. این شامل جمع‌آوری و تدوین گزارش است ولی لزوماً گزارش تحلیل نیست. نقش DEFR همچنین با تضمین یکپارچگی و احراز اصالت شواهد رقمی بالقوه نیز درگیر می‌باشد. در تکمیل نقش خود، توصیه می‌شود DEFR تجربه، مهارت‌ها و دانش کافی برای ساماندهی به شواهد رقمی بالقوه داشته باشد. این امر بسیار سخت است زیرا شواهد رقمی بالقوه به راحتی قابل از بین رفتن هستند.

همچنین ممکن است DEFR در نواحی مرتبط، از کارکنان پشتیبان فنی، تقاضای کمک کند. نقش یک DES عبارت است از فراهم کردن پشتیبانی فنی برای DEFR در شناسایی، جمع‌آوری، اکتساب و محافظت از شواهد رقمی بالقوه در صحنه‌ی وقوع. یک DES افراد کارشناس متخصص را برای DEFR فراهم می‌کند. ماتریس شایستگی برای DEFR (به پیوست الف مراجعه شود) برای کمک به شناسایی سطوح شایستگی مرتبط آن‌ها ارائه شده است.

یادآوری- در زمینه ساماندهی به رخداد، در جایی که یک ISIRT وجود دارد، نقش DEFR و/یا DES به‌عنوان یک عضو تیم ISIRT در استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، مورد بحث قرار گرفته است.

۴-۶ شایستگی

توصیه می‌شود DEFR و/یا DES شایستگی‌های فنی و قانونی مرتبط را داشته باشند (مانند موارد پیوست

الف) و توصیه می‌شود بتوانند اثبات کنند که بخوبی آموزش دیده‌اند و درک فنی و قانونی مطلوبی از ساماندهی مناسب به شواهد رقمی بالقوه داشته باشند. این امر شامل درک فرآیندها و روش‌هایی است که برای مدیریت منابع بالقوه‌ی شواهد رقمی، مناسب هستند. آموزش کافی، DEFRها را قادر به مدیریت افزارهای رقمی حاوی شواهد رقمی بالقوه می‌سازد. اگر DEFR برای اجرای وظایف شایسته نباشد، داشتن بهترین مجموعه‌ی ابزار، کیفیت شواهد رقمی را تضمین نخواهد کرد.

برخی از حوزه‌های قضایی، تعیین کرده‌اند که توصیه می‌شود DEFRها چگونه صلاحیت‌شان را برقرار کنند. این مسئولیت DEFR است که مطمئن شود که حوزه‌های مربوطه از نحوه‌ی انجام وظایف آگاه شده‌اند. توصیه می‌شود در صورت نیاز، DEFR و/یا DES بتواند اثبات کند که آن‌ها شایسته‌ی ساماندهی به شواهد رقمی بالقوه با استفاده از ابزار و روش‌های انتخاب شده برای اجرای وظایف، هستند. این امر نیز بدان نیاز دارد که DEFRها بتوانند شواهد شایستگی در حال پیشرفت خود را فراهم کنند. برخی از پیش شرط‌ها برای DEFR عبارتند از:

- توصیه می‌شود آن‌ها به‌طور مناسب و کافی برای اداره کردن افزارهای رقمی در زمینه فعالیت‌های تجسس، آموزش دیده باشند؛
- توصیه می‌شود آن‌ها مهارت‌ها و شایستگی خود را برای گرفتن اختیارات در ناحیه‌ی مربوط ساماندهی به شواهد رقمی بالقوه، اثبات و حفظ کنند؛ و
- این مسئولیت فرد یا افراد و کارفرما است که اطمینان حاصل کند آن‌ها به اندازه‌ی کافی آموزش دیده‌اند و مهارت‌ها و شایستگی حفظ شده است.

یادآوری- شایستگی یک DEFR ممکن است از دید حوزه‌های قضایی مختلف، متفاوت باشد.

۵-۶ استفاده از مراقبت منطقی

از هر گونه اقدام خواسته یا ناخواسته که منجر به تباہ‌سازی شواهد رقمی بالقوه ذخیره شده درون افزارهای رقمی می‌شود، اجتناب کنید. به‌عنوان مثال، در معرض میدان‌های مغناطیسی گذاشتن ممکن است شواهد رقمی بالقوه‌ی حاوی رسانه‌ی ذخیره‌سازی مغناطیسی را نابود کند. توصیه می‌شود DEFR به افزارهای رقمی دسترسی نداشته باشد، برای مثال خالی کردن حافظه از یک افزارهای رقمی در حال کار، مگر این‌که شایستگی لازم را داشته باشند و از فرآیندهای مطمئن و معتبر استفاده کنند.

برخی شرایط وجود دارند که در آن‌ها جمع‌آوری یا به‌دست آوردن شواهد رقمی بالقوه غیر عملی است. توصیه می‌شود DEFR به شرایط زیر توجه کند، ولی شرایط فقط محدود به موارد زیر نیست:

- اگر هیچ حق یا اختیار قانونی برای جمع‌آوری افزارهای رقمی وجود ندارد؛
- اگر اجبار برای استفاده از روش‌های دیگر وجود دارد (برای مثال جهت اجتناب از به‌تعویق انداختن یک کسب‌وکار)؛

- اگر DEFR بخواهد روش عملکرد یک مظنون را در طول سواستفاده از یک سامانه، پیگیری کند؛
- اگر جمع‌آوری یا اکتساب توصیه می‌شود به صورت محرمانه انجام شود، اگر توسط حوزه‌ی قضایی قانونی شناخته شود؛
- اگر افزاره‌ی رقمی برای مأموریت بحرانی وجود دارد که نمی‌تواند هیچ مدت استراحتی را تحمل کند؛
- اگر اندازه‌ی فیزیکی افزاره‌ی رقمی بسیار بزرگ است، برای مثال یک سرور در یک مرکز داده یا سامانه‌ی RAID؛
- اگر افزاره‌ی رقمی ایمنی حیاتی وجود دارد که اگر متوقف شود، زندگی به خطر می‌افتد؛ و
- اگر افزاره‌ی رقمی ای وجود دارد که به بخش‌های غیرمرتبط با موضوع نیز خدمت ارائه می‌کند.

۶-۶ مستندسازی

- مستندسازی در هنگام سازماندهی آن دسته از افزاره‌های رقمی که ممکن است حاوی شواهد رقمی بالقوه باشند، بحرانی است. توصیه می‌شود DEFR در طول مستندسازی به این نکات وفادار بماند:
- هر فعالیت صورت گرفته توصیه می‌شود مستند گردد. این امر برای آن است که اطمینان حاصل شود هیچ یک از جزئیات در طول فرآیندهای شناسایی، جمع‌آوری، اکتساب و محافظت، جا نمانده است. این برای یک تجسس فرامرزی نیز کمک کننده است که از طریق آن شواهد رقمی بالقوه‌ی جمع‌آوری شده از دیگر مناطق زمین بالطبع قابل ردیابی هستند؛
 - توصیه می‌شود DEFR در صورتی که افزاره‌های رقمی روشن هستند، در مورد زمان و تاریخ تنظیم حساس باشد. تنظیم زمان را با یک منبع مطمئن زمان مقایسه کنید، برای مثال یک زمان که با منبع زمان مطمئن و قابل ردیابی همگام شده است. توصیه می‌شود این تنظیمات زمان در صورت وجود هر گونه تفاوت، مستند و ثبت شوند. بعضی سامانه‌ها به تعامل بیشتر کاربر برای دستیابی به تنظیمات زمان و تاریخ، نیاز دارند. توصیه می‌شود DEFR محتاط باشد که سامانه را دست کاری نکند. توصیه می‌شود فقط کارکنانی که بخوبی آموزش دیده‌اند بتوانند این تنظیمات را بازیابی کنند؛
 - توصیه می‌شود DEFR هر چیزی که روی صفحه‌ی افزاره‌ی رقمی قابل مشاهده است را مستند کند: برنامه‌ها و فرآیندهای فعال و همچنین اسامی اسناد باز. توصیه می‌شود این مستندسازی شامل یک توصیف از آن چه که به عنوان برنامه‌های خرابه کارانه قابل مشاهده است که ممکن است به شکل نرم‌افزار معمول در بیاید، صورت پذیرد؛
 - توصیه می‌شود هر حرکتی از افزاره‌های رقمی مطابق با الزامات محلی، مستند شود؛ و
 - همه‌ی شناسه‌های منحصر به فرد افزاره‌های رقمی و بخش‌های کمک کننده مانند شماره‌های ترتیب‌ها و

نشانه‌گذاری‌های منحصر به فرد، مستند می‌شوند.

مثال‌هایی از یک مجموعه‌ی کمینه‌ی مستندسازی برای تعویض متقابل اداری-قضایی شواهد رقمی بالقوه، در پیوست ب نشان داده شده است.

یادآوری- برای اطلاعات بیشتر از مستندسازی، به بند مدیریت سند و بند مدیریت ثبت از استاندارد ملی ایران شماره‌ی ۱۷۰۲۵: سال ۱۳۸۶ شود

۷-۶ جلسات توجیهی

۱-۷-۶ عمومی

شخص DES و DEFR باید پیش از اجرای وظایفشان توسط فرد مجاز مرتبط توجیه شوند، ضمن این که به همه‌ی قوانین و محدودیت‌های محرمانگی توجه کنند (به عبارتی نیاز است که مبنا را بدانند). داشتن یک جلسه توجیهی برای درک رخداد دارای اهمیت بسیار است: این که چه چیزی در طول تجسس انتظار می‌رود و چه چیزی انتظار نمی‌رود و همین‌طور یک یادآوری کننده در مقابل دست‌کاری یا تباه‌سازی شواهد. توصیه می‌شود جلسات توجیهی برای اعضا در زمینه ادای بهتر نقش‌ها و مسؤولیت‌هایشان باشند در نتیجه از استخراج تمامی شواهد رقمی بالقوه اطمینان حاصل می‌شود.

۲-۷-۶ مخصوص شواهد رقمی

جلسه‌ی توجیهی به صراحت درمورد راهنمای خاص شواهد رقمی که برای مطلع کردن DES و DEFRها از جزئیات مربوط به تجسس مورد نیاز است، تمرکز دارد. در طول جلسه‌ی توجیهی، توصیه می‌شود DES و DEFR با اطلاعات و دستورات مفصل مربوط به شواهد رقمی بالقوه‌ی جمع‌آوری شده یا اکتساب شده، آماده شوند. این امر ممکن است شامل موارد زیر گردد:

- نوع رخداد (اگر معلوم است)؛

- تاریخ و زمان رخداد (اگر معلوم است)؛

- نقشه‌ی تجسس (جمع‌آوری و/یا اکتساب، فعالیت شناخته شده‌ی شبکه، الزامات شناخته شده‌ی داده و غیره)؛

- توجه به این که شواهد رقمی بالقوه کجا و چگونه بعد از جمع‌آوری یا اکتساب ذخیره می‌شوند/انتقال می‌یابند؛

- ابزارهای خاصی که برای به دست آوردن شواهد رقمی بالقوه نیاز داشته‌اند؛

- شواهد رقمی بالقوه که به انواع خاص تجسس مربوط است؛

- ابزار و کتابچه‌های راهنمای مربوط به افزاره‌های رقمی؛ و

- یادآوری به اعضای گروه برای خاموش کردن هر گونه بلوتوث یا Wi-Fi بر روی گوشی‌ها یا رایانه‌های خود که در این صورت نمی‌توانند سهواً تعاملی با افزاره‌های رقمی داشته باشند، به جز گوشی‌ها یا رایانه‌هایی که برای کشف اتصالات استفاده می‌شوند؛

- اهمیت مستندسازی در کل تجسس؛ و

- قانون کاربردپذیر یا عوامل دیگری که ممکن است از جمع‌آوری هر گونه افزاره یا شواهد رقمی بالقوه‌ای که درون افزاره‌هاست، ممانعت کند.

این جلسه‌ی توجیهی خاص ممکن است موجب شکل دهی بخشی از جلسه‌ی توجیهی عمومی شود، همان‌گونه که در زیربند ۶-۷-۱ توضیح داده شد.

۳-۷-۶ مخصوص کارکنان

جلسه‌ی توجیهی به صراحت در مورد راهنمای خاص شواهد رقمی که برای مطلع کردن DEFR ها از جنبه-های مربوط به بخش‌های شرکت‌کننده در تجسس مورد نیاز است، تمرکز دارد. در طول جلسه‌ی توجیهی، گروه تجسس با دستورهای مرتبط به همه کارکنان، مهیا خواهد شد. این امر ممکن است شامل موارد زیر باشد:

- واگذاری‌ها، نقش‌ها و مسئولیت‌های اعضای گروه تجسس در صحنه‌ی وقوع؛

- آیا مورد انتظار است که افراد مجاز دیگر (کارکنان پزشکی، بازرسان قانونی بیولوژی و غیره) در تجسس شرکت داده شوند؛

- اعضای گروه پشتیبان نباید کمک فنی از هر فرد غیر مجاز را بپذیرند؛ و

- اعضای گروه پشتیبان باید به صورت جدی از رویه برای کمینه کردن مخاطره‌ی نابودی شواهد رقمی بالقوه پیروی کنند، به‌عنوان مثال از به کارگیری هرگونه ابزار یا مدارکی که ممکن است الکتریسیته‌ی ساکن تولید یا ساطع کند یا یک میدان مغناطیسی اجتناب بعمل آید چراکه این موارد ممکن است موجب آسیب دیدن یا خراب شدن شواهد رقمی بالقوه شوند.

این جلسه‌ی توجیهی خاص ممکن است بخشی از جلسه‌ی توجیهی عمومی را شکل دهد که در زیربند ۶-۷-۱ توصیف شد.

۴-۷-۶ رخدادهای بلادرنگ

بسیار مطلوب است که تجسس یک رخداد توصیه می‌شود در حالت پیشرفته طرح‌ریزی شود ولی شرایطی وجود دارد (برای مثال هنگامی که یک رخداد در حال پیشرفت است و به صورت بلادرنگ به آن واکنش نشان داده می‌شود) که در آن‌ها ممکن است طرح‌ریزی کامل ممکن نباشد. در این مواقع، توصیه می‌شود

گروه با راهبردها و راه‌کنش‌های اولیه برای تجسس، توجیه شود و اجازه دهد که راهبردها و راه‌کنش‌های جدید برای پاسخگویی به شرایط غالب، توسعه یابند. اطلاعات راجع به رخداد، همچنان که ارتقا می‌یابد، توصیه می‌شود در بین گروه تا حدی که ممکن است با سرعت به اشتراک گذاشته شود تا اطمینان حاصل شود که تصمیمات گرفته شده بر فعالیت‌ها می‌توانند بهره‌وری ایجاد کنند.

۵-۷-۶ سایر اطلاعات توجیهی

جدا از شواهد رقمی و کارکنان، اطلاعات مهم دیگری که باید برای گروه‌های تجسس توجیه شوند، عبارتند از:

- شناسایی ناحیه‌ی تحت تجسس، از جمله نام سازمان، آدرس و نقشه‌ی مکان (اگر در دسترس است)؛
- حکم تجسس؛
- جزئیات گواهی‌های جستجو و دیگر مجوزهای کاربرپذیر برای تجسس، از جمله حدود جستجو و تصرف؛
- جنبه‌ها و مفاهیم قانونی؛
- شکل زمانی تجسس؛
- لازم است که تجهیزات برای تجسس به صحنه‌ی وقوع آورده شوند؛
- اطلاعات منطقی؛ و
- ناسازگاری بالقوه‌ی علاقه.

توصیه می‌شود DEFR از موقعیت‌هایی که اتهامات گرایش ذاتی را می‌توانند بوجود آورند، اجتناب کند. یک مثال از گرایش ذاتی زمانی است که DEFR از یک رایانه رونوشت می‌گیرد و از دیگری نمی‌گیرد (که بعدها باعث می‌شود که شامل شواهد تبرئه شده باشد) که در واقع بر اساس یک ادراک شکل گرفته در جلسات توجیهی است.

۸-۶ اولویت‌بندی جمع‌آوری و اکتساب

در اولویت‌بندی جمع‌آوری و اکتساب شواهد رقمی بالقوه، برای DEFR ضروری است که علت این که شواهد رقمی جمع‌آوری یا اکتساب می‌شوند را درک کند. به عنوان یک اصل عمومی، توصیه می‌شود DEFR برای بیشینه کردن مقدار داده‌ای که به وسیله‌ی فعالیت‌های جمع‌آوری و اکتساب حفاظت می‌شوند تلاش کند، هر چند که ممکن است ضروری باشد که اقلام توسط فرار بودن و/یا مرتبط بودن/ ارزش استنادی بالقوه‌ی اولویت‌بندی شوند. اقلام دارای مرتبط بودن/ ارزش استنادی بالقوه بالا، آن‌هایی هستند که به احتمال زیاد حاوی داده‌هایی می‌باشند که به طور مستقیم به رخداد تحت تجسس مربوط می‌شوند.

اولویت‌بندی براساس خاصیت فرّار بودن، زمانی کاربردپذیر است که شرایط خاص نمونه‌ی در حال تجسس ایجاب کند. شواهد رقمی بالقوه می‌تواند به دو دسته تقسیم شود: فرّار و غیر فرّار. داده‌های فرّار، اگر توجه مقتضی به حفاظت داده انجام نشود، می‌توانند به راحتی خراب شوند یا برای همیشه مفقود شوند. برای مثال، حذف منبع تغذیه از یک افزاره‌ی رقمی ممکن است منجر به از دست رفتن داده‌ی فرّار شود. داده‌های غیر فرّار حتی اگر منبع تغذیه حذف شود، روی رسانه باقی می‌مانند. از آن جا که برخی از انواع شواهد رقمی ممکن است طول عمر کوتاهی داشته باشند، شواهد رقمی بالقوه می‌توانند به راحتی مورد دست‌کاری قرار گیرند یا از بین بروند. جایی که واضح نیست که آیا افزاره‌های رقمی حاوی شواهد رقمی بالقوه هستند یا کدام اقلام بیشتر از بقیه مربوطند، ضرورت دارد که آن‌ها را پیش از جمع‌آوری، با استفاده از یک فرآیند برای تشخیص اولویت، آزمایش کنیم. افزاره‌های رقمی که برای جمع‌آوری ملاحظه می‌شوند شامل این موارد است که البته به این‌ها محدود نمی‌شود: تجهیزات IT و رسانه‌ی ذخیره‌سازی رقمی، سامانه‌های CCTV، PEDها، سامانه‌های خودرو، سامانه‌های کنترل و الکترونیکی‌های تعبیه شده. در ابتدا فرّارترین شواهد رقمی بالقوه مانند RAM، فضای تبادل، فرآیندهای در حال اجرا و غیره، کسب می‌شود. توصیه می‌شود DEFR یک دانش بی‌نقص برای اولویت‌بندی مطابق با فرّاری، داشته باشد.

به محض شناسایی، توصیه می‌شود DEFR :

- شواهد رقمی بالقوه‌ای که در صورت حذف منبع تغذیه، برای همیشه مفقود می‌شوند را اولویت‌بندی کند؛

و

- برای جمع‌آوری و اکتساب این داده‌ها با استفاده از روش‌های معتبر، اقدامات سریعی اتخاذ کند.

یادآوری ۱- برخی از داده‌های فرّار ممکن است به علت عواملی از جمله مکان، زمان و تغییرات در افزاره‌های رقمی اطراف، تغییر کنند- مطمئن شوید که این داده‌ها پیش از حرکت افزاره، محافظت شده‌اند.

یادآوری ۲- افزاره‌های رقمی که در حال حاضر حاوی شواهد رقمی بالقوه هستند ممکن است یک مدرک فیزیکی باشند (برای مثال اثر انگشت‌ها، DNA و غیره). افراد DEFR ها باید مراقب باشند که چنین شواهدی را از بین نبرند و با گردآورندگان شواهد مرتبط پیش از اقدام به فعالیت‌های بعدی، هماهنگی بعمل بیاورند.

یادآوری ۳- زمانی که رمزبندی یا بدافزاری مورد ظن قرار گرفت، مطلوب است که داده‌های فرّار را امتحان کنید.

در این شرایط ممکن است که زمان، یک عامل محدود کننده در طی تجسس باشد. در این موارد، توصیه می‌شود اولویت به شواهد رقمی بالقوه‌ای داده شود که به عنوان شواهد مرتبط با رخداد خاص، شناخته شده‌اند.

۹-۶ حافظت از شواهد رقمی بالقوه

۱-۹-۶ مرور کلی

در حافظت شواهد رقمی بالقوه‌ی کسب شده و افزاره (ها)ی رقمی جمع‌آوری شده در طول بسته‌بندی،

امن سازی این اقلام مهم است. به طوری که امکان تباه سازی و دست کاری حذف شود. تباه سازی می تواند بر اثر کاهش مغناطیسی، کاهش الکتریکی، گرما، در معرض گذاری رطوبت کم یا زیاد و همچنین تکان دادن یا لرزش باشد. دست کاری می تواند در اثر یک اقدام عمدی برای ایجاد یا اجازه ی تغییر در شواهد رقمی بالقوه باشد. پس بسیار مهم است که از شواهد رقمی بالقوه به بهترین نحو ممکن حفاظت کنیم و از داده های اصلی تا حد امکان کمتر استفاده کنیم. همین طور مهم است که DEFR با الزامات بسته بندی خاص برای حوزه های قضایی مرتبط، آشنا باشد.

۶-۹-۲ حفاظت از شواهد رقمی بالقوه

توصیه می شود همه ی افزاره های رقمی جمع آوری شده و شواهد رقمی بالقوه ی کسب شده تا جایی که ممکن است به دور از مفقود شدن، دست کاری و تباه سازی، حفاظت شوند. مهمترین فعالیت در فرآیند حفاظت، حفظ یکپارچگی و احراز اصالت شواهد رقمی بالقوه و زنجیره ی توقیف آن است.

توصیه می شود افزاره (ها)ی رقمی جمع آوری شده و شواهد رقمی بالقوه ی کسب شده در یک وسیله ی حفاظت که کنترل های امنیتی فیزیکی را به کار می برد، ذخیره شوند، مانند سامانه های کنترل دسترسی، سامانه های نظارت، سامانه های تشخیص نفوذ یا محیط کنترل شده ی دیگر برای محافظت از شواهد رقمی. اهداف اصلی امنیت فیزیکی، حفاظت و جلوگیری از مفقودی، آسیب و دست کاری و همچنین فعال کردن قابلیت نظارت، می باشند.

توصیه می شود افزاره (ها)ی رقمی در یک بسته بندی مقتضی و مناسب با ماهیت افزاره، بسته بندی یا مکان دهی شوند تا از آلودگی افزاره های رقمی پیش از انتقال به مکان های دیگر اجتناب شود. بسته بندی مقاوم در برابر لرزه می تواند برای اجتناب از آسیب فیزیکی به هر مولفه ای از افزاره (ها) استفاده شود.

- توصیه می شود DEFR به حساسیت افزاره ی رقمی در برابر اکتیسیته ی ساکن توجه داشته باشد. اگر این امر باعث نگرانی است، توصیه می شود افزاره در یک کیف ضد الکتریسیته ساکن حفاظت شود؛ و

- واحدهای اصلی سامانه و رایانه های کتابی باید در یک جایگاه مناسب محافظت شوند تا از دست کاری پنهانی یا تباه سازی شواهد رقمی بالقوه که ممکن است در آن مقیم باشد، اجتناب شود.

یادآوری- استفاده از کیف فارادی یا یک بسته بندی روکش دار بسامد رادیویی دیگر، می تواند میزان استفاده از باتری گوشی همراه را بالا ببرد. در صورت اجازه ی منبع، ممکن است احتیاج به فراهم کردن نیروی کمکی برای افزاره در زمانی که درون کیف است، باشد.

۶-۹-۳ بسته بندی افزاره های رقمی و شواهد رقمی بالقوه

۶-۹-۳-۱ فعالیت های خط پایه: بسته بندی شواهد رقمی بالقوه

توصیه می شود فعالیت های خط پایه هدایت شده باشند مگر این که یک دلیل خوب برای عدم هدایت وجود داشته باشد. این دلیل می تواند همان کمینه کردن فعالیت های اتخاذ شده باشد. در طول بسته بندی، توصیه

- می‌شود DEFR فعالیت‌های خط پایه‌ی زیر را بخاطر سپرده و فراهم سازد:
- نوار مغناطیسی را لمس نکنید، بلکه بهتر است نوارها را با جعبه‌های حفاظ یا از نواحی‌ای که حاوی داده نیستند (برای مثال لبه‌های لوح نوری)، بلند کنید. این کار تنها در صورتی توصیه می‌شود که DEFR دستکش‌های بدون پرز پوشیده است.
 - **یادآوری** - نواحی خاص در رسانه‌ی ذخیره‌سازی که به‌عنوان نواحی فاقد داده شناخته می‌شوند، به نوع رسانه بستگی دارند. این مسئولیت DEFR است که فناوری جاری را شناخته و به اداره کردن رسانه‌ی ذخیره‌سازی آشنا باشد.
 - برای اطمینان از شناسایی صحیح، توصیه می‌شود DEFR همه‌ی شواهد رقمی بالقوه را برچسب‌گذاری کند. برخی از حوزه‌های قضایی الزامات خاصی راجع به قالب برچسب زنی مدارک استنادی دارند. توصیه می‌شود DEFR از این الزامات آگاهی داشته و آن‌ها را به اجرا بگذارد. توصیه می‌شود DEFR همه‌ی شواهد رقمی بالقوه، افزاره (ها)ی رقمی و هر بخش سختی که با افزاره‌های دارای برچسب دست‌کاری آشکار سروکار دارد را برچسب‌گذاری کند. توصیه نمی‌شود برچسب به صورت مستقیم روی بخش‌های مکانیکی افزاره‌ی رقمی قرار گیرد و توصیه نمی‌شود اطلاعات مهم شناسایی را بپوشاند یا پنهان کند. با روشی برای مطمئن شدن از یکپارچگی شواهد، توصیه می‌شود همه‌ی شواهد رقمی بالقوه جمع‌آوری شده در افزاره (ها) کسب شده و ذخیره شوند.
 - در صورت امکان، توصیه می‌شود افزاره‌های رقمی با دهانه‌ها و مولفه‌های قابل حرکت با برچسب‌های دست‌کاری-آشکار^۱ که برای افزاره‌ها مناسب هستند، مهروموم شوند و توصیه می‌شود DEFR این مهروموم را امضا می‌کند.
 - افزاره‌هایی که به باتری‌ها همراه با داده‌هایی که فرار هستند متصل می‌شوند، توصیه می‌شود به صورت مرتب بررسی شوند تا اطمینان حاصل شود که افزاره‌ها همیشه منبع نیرو کافی دارند.
 - شناسایی و تامین امنیت افزاره (ها)ی رقمی در یک محفظه، برای ماهیت افزاره در مقابل تهدیدات بالقوه، مناسب است.
 - توصیه می‌شود رایانه‌ها و افزاره‌های رقمی از طریقی بسته‌بندی شوند که در برابر آسیب‌ها از لرزش، تکان خوردن، ارتفاع زیاد و در معرض قرار گرفتن تا بسامد رادیویی در طول انتقال، محافظت شوند.
 - توصیه می‌شود رسانه‌ی ذخیره‌سازی مغناطیسی در بسته‌بندی‌ای ذخیره شود که از نظر مغناطیسی راکد است، ضد الکتریسیته ساکن بوده و فاقد ذرات است.
 - افزاره‌های رقمی همچنین ممکن است حاوی شواهد نهفته، ردیابی یا زیستی باشند. همین‌طور، لازم است فعالیت‌های مناسبی اجرا شوند تا از شواهد رقمی بالقوه حافظت کنند. توصیه می‌شود تصویرگیری شواهد رقمی بعد از این که فرآیندهای جمع‌آوری شواهد نهفته، ردیابی یا زیست‌سنجشی روی افزاره‌ها هدایت

1- Tamper-evident

می‌شوند، انجام شوند. به هر حال، توصیه می‌شود تصمیم‌گیری برای اولویت‌بندی جمع‌آوری شواهد برای حفاظت شواهد، به طور کامل ارزشیابی شود.

۶-۳-۲ فعالیت‌های افزوده: بسته‌بندی شواهد رقمی بالقوه

فعالیت‌های افزوده به فعالیت‌هایی اشاره دارد که به شدت توصیه می‌شود که اجرا شوند. در طول بسته‌بندی، توصیه می‌شود DEFR در جایی که کاربردپذیر است، بر فعالیت‌های افزوده‌ی زیر ملاحظه و نظارت کند:

- پوشیدن دستکش‌های بدون پرز و اطمینان از این که دست‌ها تمیز و خشک هستند.

- حفاظت افزاره‌های رقمی از نفوذ منابع الکترومغناطیسی (برای مثال مخابرات رادیویی پلیس، بلندگوها، ماشین‌های اشعه ی X). توصیه می‌شود محیط بسته‌بندی عاری از الکتریسیته‌ی ساکن باشد.

- توصیه می‌شود بسته‌بندی محیط عاری از گرد و غبار، روغن و آلاینده‌های شیمیایی باشد که اکسیده شدن را بدتر می‌کند و موجب جمع شدن بیشتر رطوبت بر روی لایه‌ی مغناطیسی می‌شود.

- کمینه کردن احتمال چاپ از میان (انتقال یک سیگنال از یک حلقه نوار به یک حلقه‌ی مجاور) که ممکن است هنگامی اتفاق بیافتد که نوارها برای دوره‌های طولانی بدون کاربرد فعال هستند که ناشی از کیفیت سیگنال پایین است.

- جایی که ضرورت دارد، توصیه می‌شود نواحی بسته‌بندی عاری از نور UV باشند. نور UV ممکن است باعث از هم پاشیدگی DNA شود یا به برخی از انواع رسانه آسیب بزند. توصیه می‌شود DEFR توجه کند که آیا UV به عنوان یک مخاطره برای شواهد رقمی، پیش از انتخاب ناحیه‌ی بسته‌بندی، مطرح است.

- توصیه می‌شود افزاره‌های رقمی در مقابل شوک گرمایی، به شدت محافظت شوند.

۶-۹-۴ انتقال شواهد رقمی بالقوه

توصیه می‌شود DEFR از افزاره‌های رقمی جمع‌آوری شده و شواهد رقمی بالقوه‌ی اکتساب شده در طول انتقال، محافظت کند. توصیه می‌شود شواهد رقمی بالقوه در طول فرآیند انتقال بدون حضور رها شود. توصیه می‌شود DEFR از زنجیره‌ی توقیف در سراسر فرآیند انتقال نگهداری کند تا از دست‌کاری یا تباه‌سازی احتمالی جلوگیری کند و یکپارچگی و صحت افزاره‌های رقمی و شواهد رقمی بالقوه را حفظ کند. اگر شواهد رقمی بالقوه به وسیله‌ی DEFR یا DES منتقل نمی‌شود، توصیه می‌شود که از رمزبندی استفاده شود.

یادآوری- توصیه می‌شود DEFR مطمئن شود که جمع‌آوری اطلاعات شخصی یا حساس، مطابق با قوانین و دستورات محلی در مورد محافظت داده است.

در طی بسته‌بندی و انتقال، نیاز است DEFR از وجود احتمالی تخلیه‌ی الکتریکی که ممکن است به ارزش استنادی شواهد رقمی بالقوه صدمه بزند، آگاه باشد. توصیه می‌شود DEFR مطمئن باشد که رایانه‌ها و افزاره-

های رقمی در طول انتقال، به صورت امن بسته‌بندی شده‌اند تا از مخاطره‌ای نظیر تکان تا لرزش جلوگیری کند.

توصیه می‌شود فرآیند انتقال برای محیط کنترل شده و مساعد اجازه داده شود. توصیه می‌شود سطح رطوبت، نم و دما برای افزارهای رقمی مناسب باشند. از نگهداری شواهد رقمی بالقوه و افزارهای رقمی در حامل انتقال برای دوره‌های طولانی اجتناب شود و از در معرض قرار گرفتن آن‌ها در برابر اشعه UV اجتناب شود.

در برخی از حوزه‌های قضایی، وقتی شرایط مجاز نیستند، DEFR قادر به همراهی با شواهد نیست. در این گونه موارد، به کارگیری مکانیسم‌های ترابری مجاز و مناسب، برای بیمه کردن امنیت کافی شواهد در طول انتقال، می‌توانند مورد استفاده قرار گیرند. توصیه می‌شود اسناد انتقال و درستی‌سنجی یکپارچگی بسته بخشی از زنجیره‌ی توقیف باشند.

۷ مثال‌های شناسایی، جمع‌آوری، اکتساب و محافظت

۱-۷ رایانه‌ها، افزارهای جانبی و رسانه‌ی ذخیره‌سازی رقمی

۱-۱-۷ شناسایی

۱-۱-۱-۷ جستجو و مستندسازی صحنه‌ی وقوع فیزیکی

در ادامه، رایانه‌ها به عنوان افزارهای رقمی مستقلی ملاحظه می‌شوند که داده را دریافت می‌کنند، پردازش کرده، ذخیره می‌کنند و نتایج را تولید می‌کنند. این افزارهای رایانه‌ای به شبکه متصل نیستند، اما شاید به افزارهای جانبی متصل شده باشند مانند چاپگرها، پوشگرها، وب بین‌ها، پخش‌کننده‌های MP3، سامانه‌های موقعیت‌یابی جهانی، افزارهای تایید هویت و غیره. یک افزارهای رقمی که واسط شبکه دارد ولی در زمان جمع‌آوری یا اکتساب متصل نشده باشد توصیه می‌شود به عنوان یک رایانه‌ی مستقل مورد ملاحظه قرار گیرد (در راستای هدف این استاندارد ملی). در جایی که یک رایانه با واسط شبکه ولی بدون ارتباط آشکار، پیدا می‌شود، توصیه می‌شود فعالیت‌ها برای شناسایی افزارها که به طور احتمالی کدام یک از آن‌ها اخیراً متصل شده باشند، انجام شوند.

به طور معمول صحنه‌های رخداد شامل انواع مختلف رسانه‌ی ذخیره‌سازی رقمی خواهند بود. رسانه‌ی ذخیره‌سازی رقمی برای ذخیره داده از افزارهای رقمی، استفاده می‌شود و از لحاظ گنجایش حافظه متفاوت هستند. مثال‌های رسانه‌ی ذخیره‌سازی رقمی شامل این موارد است ولی به این‌ها محدود نمی‌شود: لوح‌های سخت، راننده فلش، لوح‌های فشرده، لوح‌های همه کاره، لوح‌های Blu-ray، لوح‌های نرم، نوارهای مغناطیسی و کارت‌های حافظه.

قبل از این که هرگونه جمع‌آوری یا اکتسابی قابل انجام باشد، لازم است که جنبه‌های ایمنی شواهد رقمی بالقوه مورد ملاحظه قرار گیرند. این جنبه‌ها در زیربند ۱-۲-۶ و ۲-۲-۶ توصیف می‌شوند. با این حال، توصیه می‌شود DEFR جهت اطمینان خود مراقب باشد که یک افزارهای رقمی ظاهراً مستقل به تازگی به شبکه

متصل نشده است. وقتی شک داریم که افزاره‌ی ظاهراً مستقل، اخیراً از شبکه قطع شده است، توصیه می‌شود ملاحظه شود که با آن به‌عنوان یک افزاره‌ی شبکه شده رفتار شود تا اطمینان حاصل شود که دیگر بخش-های شبکه به‌درستی مدیریت می‌شوند. توصیه می‌شود DEFR کمینه موارد زیر را به‌یاد داشته باشد و ثبت کند:

- توصیه می‌شود DEFR نوع و نمانام هرگونه افزاره رقمی استفاده شده را مستند کند و همه‌ی رایانه‌ها و افزاره‌های جانبی که به طور احتمالی احتیاج دارند که در طول این مرحله‌ی اولیه جمع‌آوری یا اکتساب شوند، را شناسایی کند. شماره‌های ترتیب، توصیه می‌شود شماره‌های مجوز و علائم شناسایی دیگر (شامل آسیب فیزیکی) در هر جا که ممکن است، مستند شوند.

- در مرحله‌ی شناسایی، توصیه می‌شود موقعیت رایانه‌ها و افزاره‌های جانبی همان‌گونه که هست، باقی بماند. اگر رایانه‌ها و افزاره‌های جانبی خاموش هستند، DEFR نباید آن‌ها را روشن کند. اگر رایانه‌ها و افزاره‌های جانبی روشن هستند، توصیه می‌شود DEFR آن‌ها را خاموش نکند که در غیر این صورت ممکن است شواهد رقمی بالقوه نابود شود.

- اگر رایانه‌ها روشن هستند، توصیه می‌شود DEFR عکس بگیرد یا یک سند نوشته شده از آن‌چه روی صفحه‌های نمایش نشان داده می‌شود، بسازد. توصیه می‌شود هر سند نوشته شده شامل یک توصیف از آن‌چه واقعاً قابل مشاهده است، باشد (برای مثال مکان‌ها، عناوین و محتویات تقریبی پنجره)

- افزاره‌ای که دارای باتری‌هایی است که ممکن است تمام شوند باید در حالت گرفتن شارژ باقی بمانند تا اطلاعات از بین نرود. یک DEFR باید باتری پرکن‌های بالقوه و کابل‌ها را در این شناسایی و جمع‌آوری کند.

- همچنین توصیه می‌شود DEFR به استفاده از یک ردیاب سیگنال بی‌سیم برای شناسایی و کشف سیگنال‌های بی‌سیم متعلق به افزاره‌های بی‌سیم که ممکن است پنهان باشند، توجه کند. به طور احتمالی نمونه‌هایی وجود دارد که در آن‌ها ردیاب سیگنال بی‌سیم به‌علت محدودیت‌های زمانی و هزینه استفاده نمی‌شود و توصیه می‌شود DEFR آن‌ها را مستند کند. اگر هر کدام از افزاره‌های شبکه شده پیدا شوند، توصیه می‌شود DEFR با فرآیند ساماندهی به شواهد ادامه دهد، همان‌گونه که در زیربند ۷-۲-۲-۲ این سند توصیف شد. در جایی که توصیه می‌شود پویش فعال (به‌عبارتی همه پخشی و/یا کاوش) برای افزاره‌های شبکه استفاده شود، افزاره‌های پویش باید تا زمانی که یک ارزیابی بر احتمالات افزاره در تعامل با دیگر افزاره‌های درون صحنه تشخیص داده شده است، باید خاموش باشند. توصیه می‌شود اعضای گروه به خاطر داشته باشند که افزاره‌های حتمی در صحنه می‌توانند حضور افزاره‌های اسکن فعال را شناسایی کنند و استفاده از پویش فعال ممکن است فعالیت‌هایی را راه‌اندازی کند که شاید شواهد رقمی بالقوه را نابود کنند و می‌توانند در شرایط نهایی، موجب فعال شدن تله‌های مخفی شوند.

یادآوری ۱- در برخی از حوزه‌های قضایی، روشن کردن افزاره‌های رقمی در یک صحنه مجاز است، تا اگر تعداد زیادی افزاره-

ی رقمی حضور دارند، مرتبط بودن آن با تجسس معین شود. این امر با در نظر گرفتن زمان و هزینه پردازشی صورت می‌گیرد که ممکن است در صورت کسب افزارهای رقمی نامرتب رخ دهد. اگر یک افزاره برای ارزشیابی روشن است، توصیه می‌شود DEFR مطمئن شود که همه‌ی یادداشت‌های فعالیت‌های اتخاذ شده، در طول فرآیند نگهداری می‌شوند.

یادآوری ۲- در نگهداری موقعیت قدرت افزارهای رقمی، توصیه می‌شود فرآری و نتایج فرآیند اولویت‌بندی مرتبط مورد توجه قرار گیرند. اگر تصمیم گرفته می‌شود که اطلاعات غیر فرآر، بحرانی ترین اطلاعات روی لوح است، پس آن سامانه‌ی در حال اجرا ممکن است از صفحه کنسول خود تصویر گرفته باشد و روشن باشد. اگر اطلاعات فرآر درون حافظه مهم باشد، آنگاه روشن نگه داشتن سامانه در جهت فراهم کردن امکان اکتساب آن، ضروری است.

۷-۱-۱-۲ جمع‌آوری شواهد غیر-رقمی

توصیه می‌شود DEFR به جمع‌آوری شواهد غیر رقمی توجه کند. برای فعال‌سازی این امر، توصیه می‌شود رهبر گروه افرادی را که در قبال امکانات درون صحنه مسؤول هستند، شناسایی کند. این فرد ممکن است بتواند اطلاعات و مستندات افزوده‌ای مانند اسم‌رمزهای افزارهای رقمی و جزئیات مرتبط دیگر، را فراهم کند. یک DEFR لازم است که نام و نقش این فرد را مستند کند.

همچنین ممکن است DEFR لازم باشد با صحبت با افرادی که به طور احتمالی اطلاعات مفید یا مرتبطی درباره‌ی شواهد رقمی بالقوه یا افزارهای رقمی جمع‌آوری شده دارند، بعضی شواهد را جمع‌آوری کند. توصیه می‌شود هر گونه پاسخ به دقت مستند شود. این افراد ممکن است شامل مدیر سامانه، صاحب افزاره و کاربران رایانه و افزارهای جانبی باشند. در طول این جمع‌آوری شواهد لفظی، ممکن است DEFR اطلاعاتی مانند پیکربندی سامانه و اسم‌رمز مدیر/ریشه، را درخواست کند. این اطلاعات افزوده شاید در مرحله تحلیل شواهد رقمی بالقوه، کمک کننده باشند. توصیه می‌شود این مکالمات مستند شوند تا اطمینان دهد که جزئیات دقیق هستند و بیانیه‌ی مستند شده نمی‌تواند تغییر داده شود. یک DEFR باید با الزامات حوزه‌های قضایی مرتبط که به جمع‌آوری شواهد غیر رقمی مرتبط هستند، آشنا باشد.

۷-۱-۱-۳ فرآیند تصمیم‌گیری برای جمع‌آوری یا اکتساب

- در تصمیم‌گیری برای جمع‌آوری یک افزارهای رقمی یا اکتساب شواهد رقمی بالقوه، توصیه می‌شود چندین عامل در نظر گرفته شود که شامل موارد زیر است ولی به این موارد محدود نیست: فرآر بودن شواهد رقمی بالقوه که در زیربندهای ۴-۵ و ۶-۸ توصیف شد،

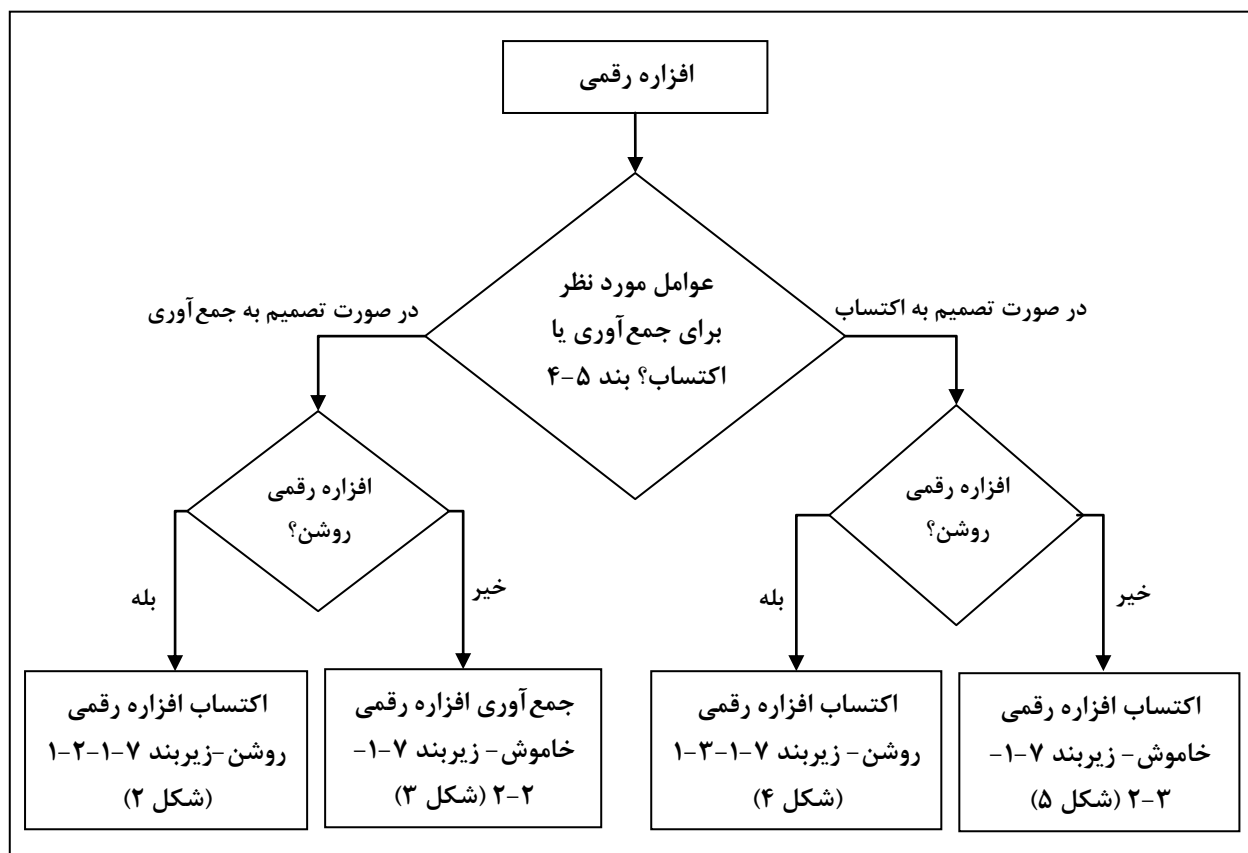
- وجود رمزبندی کامل لوح یا مجله‌های رمزبندی شده در شرایطی که عبارت ورود یا کلیدها ممکن است به‌عنوان داده‌ی فرآر در RAM، نشانه‌های خارجی، کارت‌های هوشمند، دیگر افزارها یا رسانه، ساکن باشند،

- حیاتی بودن سامانه که در زیربندهای ۴-۵ و ۷-۲-۱ و ۷-۳-۱ توصیف شد،

- الزامات قانونی یک حوزه‌ی قضایی، و

- منابعی مانند اندازه‌ی ذخیره‌ساز مورد نیاز، دسترس‌پذیری کارکنان، محدودیت‌های زمانی.

شکل ۱ مرور کلی بر فرآیند تصمیم‌گیری برای انجام جمع‌آوری یا اکتساب را نشان می‌دهد.



شکل ۱- راهنمایی‌های تصمیم‌گیری برای جمع‌آوری یا اکتساب شواهد رقمی بالقوه

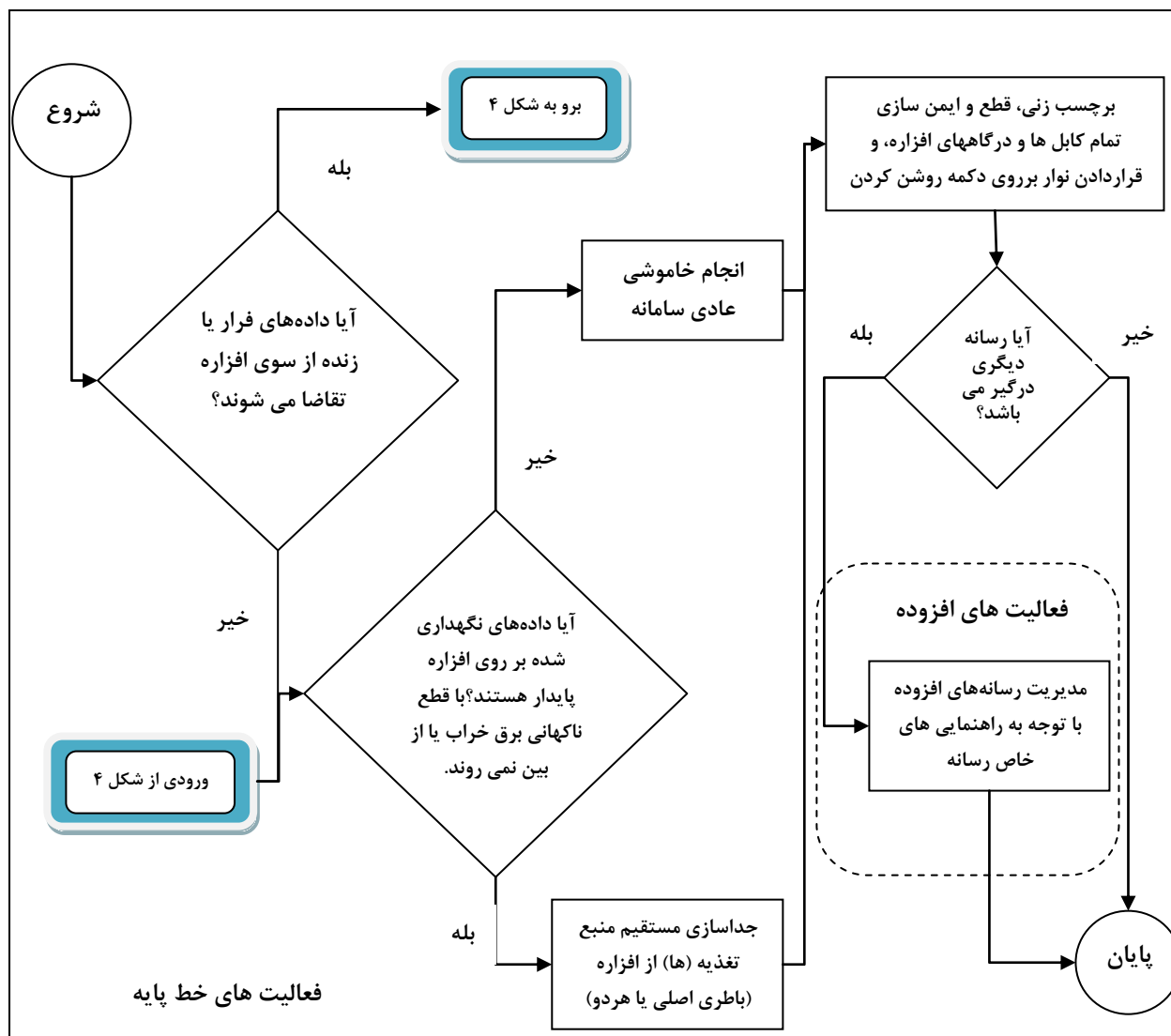
۲-۱-۷ جمع‌آوری

۱-۲-۱-۷ افزاره‌های رقمی روشن

۱-۱-۲-۱-۷ مرور کلی

هنگامی که افزاره‌ی رقمی روشن است، DEFR می‌تواند از تعدادی از راهنمایی‌ها جهت جمع‌آوری، پیروی کند. همه‌ی راهنمایی‌ها برای هر نمونه‌ای ایده‌آل و مناسب نیست، برخی از راهنمایی‌ها تنها مربوط به نمونه‌های خاص هستند. از این رو، راهنمایی‌ها می‌توانند به دو دسته‌ی خط پایه و افزوده تقسیم شوند. توصیه می‌شود فعالیت‌های خط پایه در همه‌ی شرایط به کار گرفته شوند در حالی که توصیه می‌شود فعالیت‌های افزوده بسته به افزاره‌ی مستقل یا شرایط، هنگامی که مرتبط و کاربرپذیر هستند، به کار گرفته شوند.

شکل ۲ فعالیت‌های خط پایه و افزوده‌ای که برای جمع‌آوری افزاره‌ی روشن کاربرپذیر است را نشان می‌دهد.



شکل ۲- راهنمایی‌هایی برای جمع‌آوری افزاره‌ی رقمی روشن

یادآوری- توصیه می‌شود همه‌ی این فعالیت‌ها مطابق با قوانین و قواعد حوزه‌ی قضایی محلی باشند.

این مسؤولیت DEFR است که فناوری جاری را بداند و با راهنمایی‌های اداره کردن رسانه‌ی ذخیره‌سازی آشنا باشد.

۲-۱-۲-۱-۷ فعالیت‌های خط پایه: جمع‌آوری افزاره‌ی رقمی روشن

فعالیت‌های خط پایه‌ی زیر توصیه می‌شود توسط DEFR برای همه‌ی نمونه‌هایی که شامل شواهد رقمی بالقوه هستند، پیروی شوند. این راهنمایی‌ها وقتی به کار می‌روند که DEFR تصمیم گرفته است که یک افزاره‌ی رقمی روشن، توصیه می‌شود جمع‌آوری شود:

- پیش از خاموش کردن سامانه، به اکتساب داده‌های فرار و حالت جاری افزاره‌ی رقمی توجه کند. کلیدهای رمزبندی و داده‌های قاطع، ممکن است در حافظه‌ی فعال یا حافظه‌ی غیر فعالی که هنوز پاک نشده

است، ساکن شوند. وقتی رمزبندی مورد شک قرار می‌گیرد، به اکتساب منطقی توجه کنید. وقتی این نمونه وجود دارد، به ذهن بسپارید که سامانه عامل میزبان زنده ممکن است غیر قابل اعتماد باشد، بنابراین به استفاده از ابزار مناسب قابل اعتماد و معتبر، توجه کنید.

- پیکربندی افزاری رقمی تعیین می‌کند که آیا DEFR نیاز دارد که افزاره را از طریق رویه‌های عادی مدیریتی ببندد و در واقع خاموش کند یا آیا توصیه می‌شود دوشاخه ی افزاره از سوکت برق کشیده شود. یک DEFR ممکن است نیاز داشته باشد که با یک DES مشورت کند تا بهترین راهکار شرایط خاص مفروض را معین کند. اگر تصمیم گرفته شد که دوشاخه کشیده شود، DEFR باید کابل منبع تغذیه را با جدا کردن سر انتهایی متصل به افزاری رقمی و نه سر انتهایی متصل به سوکت، بردارد. مطلع باشید که یک افزاری متصل شده به یک تامین کننده برق بی‌وقفه ممکن است داده‌ای داشته باشد که اگر سیم توان از دیوار و نه از افزاره برداشته شود، عوض شود.

یادآوری ۱- اگر منبع برق از یک افزاری رقمی روشن، حذف می‌شود، هرگونه شواهد رقمی بالقوه‌ی ذخیره شده در مجلدهای رمزبندی شده، خارج از دسترس خواهند بود، مگر این که کلید رمزگشایی به‌دست آمده باشد. داده‌های زنده‌ی با ارزش بالقوه نیز می‌توانند مفقود شوند، در واقع به سمت ادعای خسارت یا اتلاف حیات انسان سوق می‌یابد، از قبیل داده‌های شرکتی یا تجهیزات کنترل کننده افزاری رقمی و وسایل پزشکی. بنابراین، توصیه می‌شود DEFR مطمئن باشد که داده‌های فرآر، پیش از حذف منبع تغذیه، جمع‌آوری شده‌اند.

یادآوری ۲- برخی افزاره‌های سخت‌افزاری وجود دارند که به افزاری روشن اجازه می‌دهند که از منبع تغذیه جدا شود و به تامین کننده برق بی‌وقفه قابل حمل، بدون ایجاد وقفه‌ی قدرت برای افزاره، انتقال یابد. همچنین موشواره‌هایی وجود دارند که می‌توانند در جهت جلوگیری از فعال شدن محافظ صفحه‌ی نمایش استفاده شوند. هر دوی این افزاره‌ها، ابزارهای مفیدی را برای هنگامی که با یک افزاری روشن در ارتباط هستند، در جاییکه رمزبندی ممکن است فعال باشد، فراهم می‌کنند. هنگامی که یک افزاری روشن، چنان جمع‌آوری می‌شود که قدرت حفظ شود، بسته‌بندی و انتقال یک سامانه‌ی در حال اجرا باید بر مسایل وابسته به تدارک خنکی، محافظت در برابر شوک مکانیکی و غیره نظارت کند.

- همه‌ی کابل‌های افزاری رقمی را برچسب‌گذاری، قطع و امن کنید و درگاه‌ها را برچسب‌گذاری کنید تا سامانه بتواند در مرحله‌ی بعدی نوسازی شود.

- اگر جلوگیری از تغییر وضعیت کلید منبع ضروری است، نوار را بالای کلید برق بگذارید. توجه کنید که آیا وضعیت کلید، پیش از ضربه دیدن یا جابه‌جایی، به طور مناسبی مستند شده است.

۳-۱-۲-۱-۷ فعالیت‌های افزوده: جمع‌آوری افزاری رقمی روشن

موارد زیر فعالیت‌های افزوده‌ی مرتبطی هستند که وابسته به پیکربندی افزاری رقمی خاص می‌باشند.

- اگر رایانه کتابی باشد، مطمئن شوید که داده‌های فرآر قبل از حذف باتری، اکتساب می‌شوند. توصیه می‌شود DEFR به‌جای فشار دادن دکمه‌ی روشن کردن رایانه کتابی، برای خاموش کردن آن، ابتدا باتری منبع تغذیه اصلی را بردارد. توصیه می‌شود DEFR همچنین توجه کند که آیا یک تعدیل دهنده‌ی قدرت

حاضر است و در صورت وجود، تعدیل دهنده‌ی قدرت را بعد از جداساختن باتری، بردارد.

یادآوری ۱- فشردن دکمه‌ی روشن کردن ممکن است روی یک افزاره‌ی رقمی پیکربندی شود برای تعویض اطلاعات یا حذف اطلاعات از سامانه، قبل از خاموش کردن یا برای هشدار دادن به سامانه‌های متصل درمورد این‌که یک اتفاق غیر مترقبه اتفاق افتاده است که ممکن است داده‌های ارزش استنادی را قبل از این‌که شناسایی شوند، پاک کنند. همچنین ممکن است برای راه‌اندازی یک افزاره‌ی مورد نظر برای ایجاد خسارت فیزیکی برای DEFR یا دیگر افراد حاضر، راه‌اندازی شود.

- در صورت حاضر بودن، نوار را بالای شکاف لوح نرم قرار دهید.

- مطمئن شوید که راه‌انداز دو کاره‌ی لوح فشرده یا لوح همه‌کاره در محل حاضر هستند. توجه کنید که آیا این راه‌اندازهای دو کاره خالی هستند، حاوی لوح‌ها هستند یا چک نشده‌اند؛ و شکاف راه‌انداز با نوار، برای جلوگیری از باز شدن آن، بسته شده است.

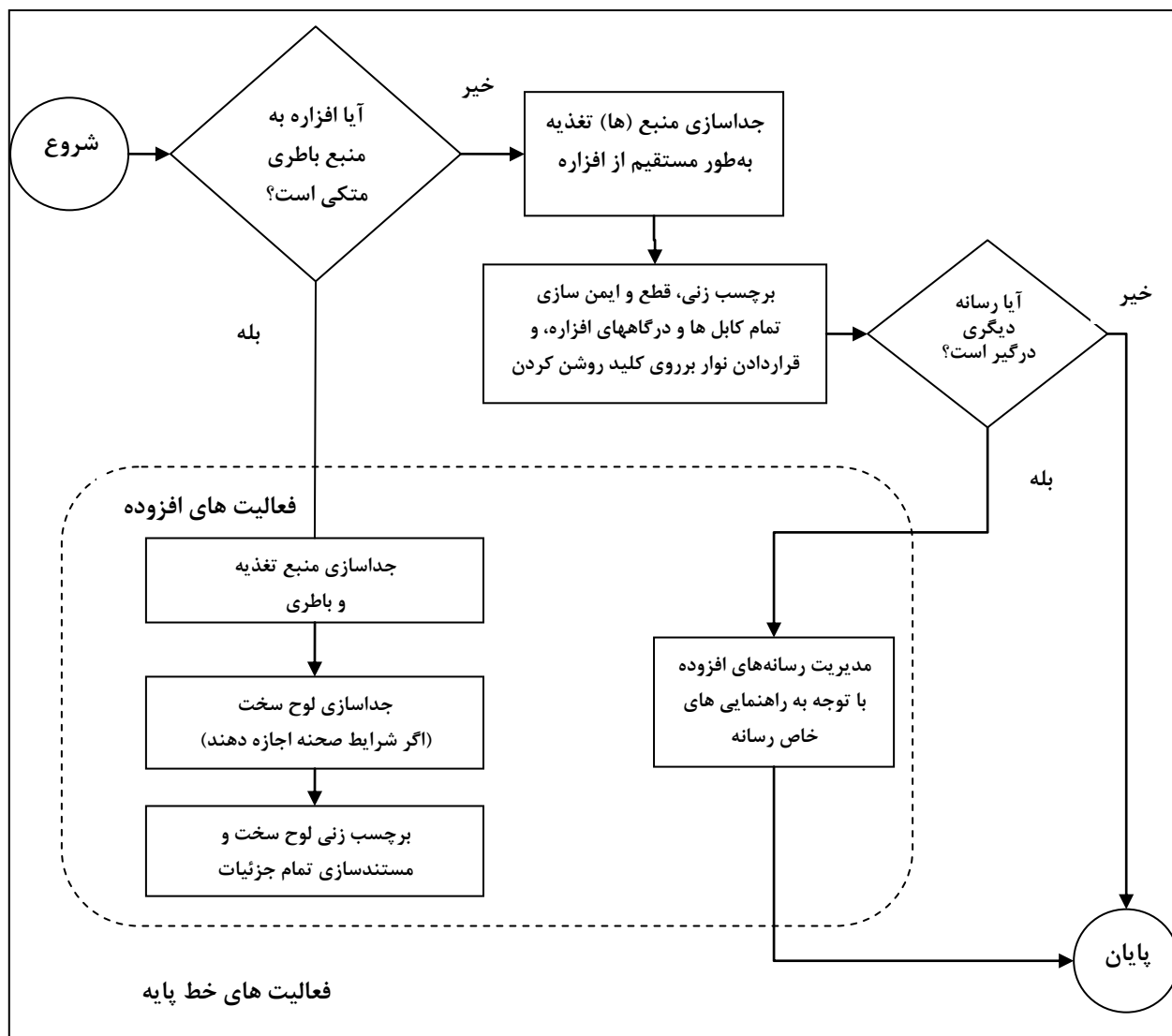
یادآوری ۲- اگر هر رسانه قابل راه‌اندازی زمانی رها شود که بعد از آن دستگاه روشن می‌شود، رسانه مذکور می‌تواند بسته به تنظیمات BIOS رایانه‌ها از چیزی به جز لوح سخت (یا فلش راه‌اندازهای دادگاهی) راه‌اندازی شود.

توصیه می‌شود DEFR جمع‌آوری شواهد غیر رقمی را با توجه به قوانین روبه‌ای هدایت کند تا قابل قبول بودن شواهد را تضمین کند.

۲-۲-۱-۷ افزاره‌های رقمی خاموش

۱-۲-۲-۱-۷ مرور کلی

یک DEFR می‌تواند از برخی راهنمایی‌ها برای جمع‌آوری در هنگامی که افزاره‌ی رقمی خاموش است، پیروی کند. همه‌ی فعالیت‌های شامل در این راهنمایی‌ها، به همه‌ی شرایط مرتبط نمی‌شوند. بنابراین بهتر است تمایز بین فعالیت‌هایی که در همه‌ی نمونه‌ها استفاده می‌شوند (فعالیت‌های خط پایه) و فعالیت‌هایی که ممکن است فقط در برخی از نمونه‌ها استفاده شوند (فعالیت‌های افزوده)، بوجود آید. شکل ۳، فعالیت‌های خط پایه و افزوده‌ی کاربرد پذیر برای جمع‌آوری افزاره‌ی رقمی خاموش را نشان می‌دهد.



شکل ۳- راهنمایی هایی برای جمع آوری افزاره ی رقمی خاموش

این مسئولیت DEFR است که فناوری جاری را بشناسد و با راهنمایی های کردن رسانه ذخیره سازی آشنا شود.

۲-۲-۲-۱-۷ فعالیت های خط پایه

در ادامه فعالیت های خط پایه ی توصیه شده برای جمع آوری هنگامی که افزاره ی رقمی خاموش می شود، آمده است:

- ابتدا کابل منبع تغذیه را جدا کنید، در واقع انتهای متصل شده به افزاره ی رقمی را جدا کنید نه انتهای متصل به سوکت را.
- همه ی کابل های افزاره های رقمی را قطع و امن کنید و درگاه ها را برچسب گذاری کنید تا سامانه بتواند در مرحله ی بعد بازسازی شود.

- اگر جلوگیری از تغییر وضعیت کلید ضروری است، نوار را بالای کلید برق بگذارید. توجه کنید که آیا وضعیت کلید، پیش از ضربه دیدن یا جابه‌جایی، به طور مناسبی مستند شده است.

یادآوری - در بیشتر موارد، رسانه‌ی ذخیره‌سازی، تا زمانی که اکتساب شود، توصیه نمی‌شود از افزاره‌ی رقمی برداشته شود، زیرا برداشتن آن مخاطره‌ی آسیب یا اشتباه شدن آن با رسانه‌های ذخیره‌سازی دیگر، را بالا می‌برد. رویه‌های محلی معطوف به احتیاج به برداشتن رسانه‌ی ذخیره‌سازی از افزاره‌های رقمی، توصیه می‌شود ارتقا داده شوند و پیروی شوند.

۳-۲-۱-۷ فعالیت‌های افزوده: جمع‌آوری افزاره‌ی رقمی خاموش

موارد زیر فعالیت‌های افزوده‌ی مرتبط به جمع‌آوری افزاره‌ی رقمی خاموش هستند که وابسته به پیکربندی افزاره‌ی رقمی خاص می‌باشند:

- در ابتدا، مطمئن شوید که رایانه کتابی به طور کامل خاموش است، زیرا برخی ممکن است در حالت آماده به‌کار باشند. آگاه باشید که برخی از رایانه‌های کتابی می‌توانند از طریق باز کردن دریچه، روشن شوند. بنابراین برای برداشتن باتری منبع تغذیه اصلی از روی رایانه کتابی، پیشی بگیرید.

- اگر شرایط میدانی ایجاب می‌کند که لوح سخت برداشته شود، توصیه می‌شود DEFR مراقب باشد که افزاره‌ی رقمی را به زمین متصل کند تا از آسیب الکتریسیته‌ی ساکن به لوح سخت، جلوگیری کند. در غیر این صورت، توصیه نمی‌شود سخت‌افزار در میدان حذف شود. لوح سخت را به‌عنوان لوح مظنون، برچسب‌گذاری کنید و همه‌ی جزییات را مستند کنید مانند ساختن نام مدل، شماره ردیف و اندازه‌ی لوح سخت.

- نوار را بالای شکاف لوح نرم قرار دهید، اگر وجود دارد.

- مطمئن شوید که راه‌انداز دوکاره‌ی لوح فشرده یا لوح همه کاره در محل جمع شده‌اند. توجه کنید که آیا این راه‌اندازهای دو کاره خالی هستند، حاوی لوح‌ها هستند یا چک نشده‌اند؛ و شکاف راه‌انداز با نوار، برای جلوگیری از باز شدن آن، بسته شده است.

یادآوری - اگر هر رسانه قابل راه‌اندازی زمانی رها شود که بعد از آن دستگاه روشن می‌شود، رسانه مذکور می‌تواند بسته به تنظیم‌های BIOS رایانه‌ها از چیزی به جز لوح سخت (یا فلش راه‌اندازهای دادگاهی) راه‌اندازی شود.

۳-۱-۷ اکتساب

۱-۳-۱-۷ افزاره‌های رقمی روشن

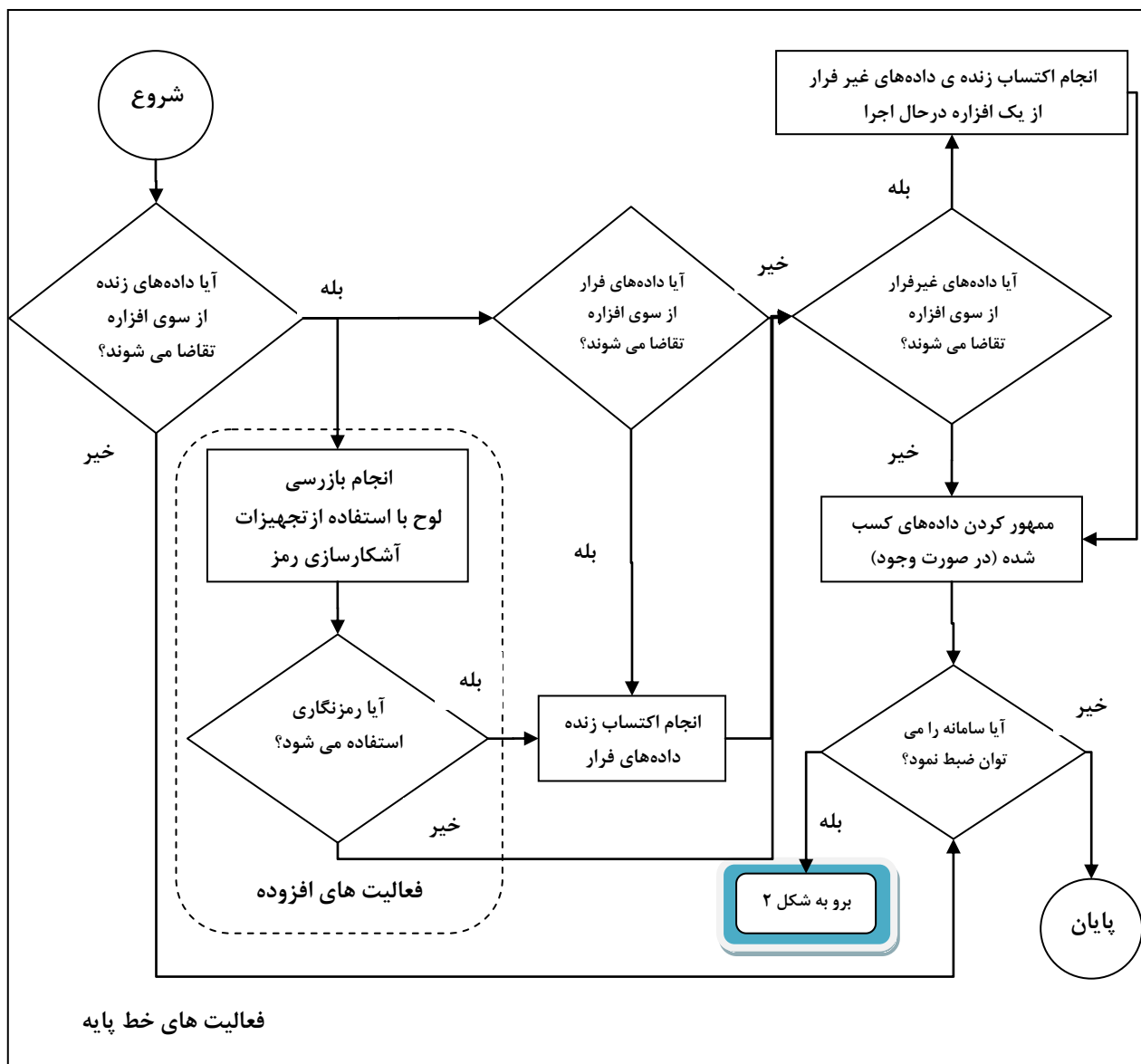
۱-۱-۳-۱-۷ مرور کلی

سه فرآیند وجود دارد برای این که کدام اکتساب ممکن است هدایت شود: هنگامی که افزاره‌های رقمی روشن می‌شوند، هنگامی که افزاره‌های رقمی خاموش می‌شوند و هنگامی که افزاره‌های رقمی روشن می‌شوند ولی نمی‌توانند خاموش شوند (مانند افزاره‌های رقمی ماموریت-بحران). در همه‌ی این فرآیندها، DEFR لازم است که یک رونوشت شواهد رقمی دقیق از رسانه‌ی ذخیره‌سازی افزاره‌های رقمی که مورد شک قرار گرفته-

اند که حاوی شواهد رقمی بالقوه باشند، تهیه کند.

اگر یک تصویر نتواند اکتساب شود، ممکن است رونوشت‌های دقیق از پوشه‌های خاص که به داشتن شواهد رقمی بالقوه مظنونند، اکتساب شوند. در حالت ایده آل، هر دوی رونوشت ارباب^۱ شناسایی شده و توصیه می‌شود رونوشت‌های در حال کار تولید شوند. توصیه نمی‌شود رونوشت ارباب دوباره استفاده شود مگر این که نیاز شود که محتواهای رونوشت در حال کار را شناسایی کند و یا یک رونوشت در حال کار جایگزین که از آسیب بر اولین رونوشت در حال کار پیروی می‌کند، تولید کند.

یک DEFR می‌تواند از تعدادی از راهنمایی‌ها برای اکتساب در هنگامی که افزاره‌ی رقمی برای روشن بودن پایه‌ریزی می‌شود، پیروی کند. همه‌ی راهنمایی‌ها برای همه‌ی نمونه‌ها مناسب و ایده‌آل نیستند، بعضی راهنمایی‌ها تنها به نمونه‌های خاصی مربوط هستند. بنابراین، راهنمایی‌ها می‌توانند به خط پایه یا افزوده دسته‌بندی شوند. توصیه می‌شود این احتمال ملاحظه شود که یک سامانه روشن ممکن است وارد حالت محافظ صفحه نمایش یا قفل خودکار شود و در این صورت دلالت‌هایی برای اتخاذ هرگونه تلاشی برای جلوگیری از آن‌ها وجود دارد. برای مثال، استفاده از نرم‌افزار mouse-jiggler مستلزم وارد کردن یک کلید همه‌گذر در داخل ثبات می‌باشد که به طور احتمالی برای هر رویداد مشابهی رخ خواهد داد. توصیه می‌شود استفاده از روش‌های مطمئن دلالت‌های این‌گونه فعالیت‌ها را کمینه کند. شکل ۴، فعالیت‌های خط پایه و افزوده که برای اکتساب افزاره‌ی رقمی روشن کاربرپذیر هستند را نشان می‌دهد.



شکل ۴- راهنمایی هایی برای اکتساب افزاره ی رقمی روشن

۲-۱-۳-۱-۷ فعالیتهای خط پایه: اکتساب افزاره ی رقمی روشن

فعالیت های خط پایه ای که توصیه می شود توسط DEFR در همه ی نمونه های حاوی اکتساب شواهد رقمی بالقوه در افزاره های روشن، پیروی شوند، در زیر آمده است:

- در وهله اول به اکتساب شواهد رقمی بالقوه توجه کنید که در غیر این صورت ممکن است اگر افزاره ی رقمی خاموش شود، شواهد مفقود شوند. این شواهد به عنوان داده ی فرار نیز شناخته می شود مانند داده-ای که روی RAM ذخیره شده است، فرآیندهای در حال اجرا، اتصالات شبکه و تنظیمات زمان/تاریخ. در شرایطی که ضرورت دارد داده های غیر فرار از افزاره هایی که همچنان در حال اجرا هستند، اکتساب شوند، اجرای یک اکتساب در سامانه ی روشن، توصیه می شود مورد توجه قرار گیرد.

- اجرای اکتساب زنده برای به دست آوردن داده‌های زنده از افزاره‌هایی که در حال اجرا هستند، ضروری است. اکتساب زنده‌ی داده‌های فرار در RAM ممکن است بازیابی اطلاعات با ارزش مانند وضعیت شبکه، اسم‌رمزها و برنامه کاربردی رمزگشایی شده، را فعال کند. اکتساب زنده می‌تواند در کنسول یا از راه دور از طریق شبکه، هدایت شوند. فرآیندها متفاوت هستند و به استفاده از مجموعه‌ی متفاوت ابزارها احتیاج دارند.

- توصیه می‌شود DEFR هرگز به برنامه‌های روی سامانه‌ها اعتماد نکند. به این علت، ابزارهای مورد اعتماد به دست آمده به وسیله‌ی DEFR (دودویی‌های ایستا) هرگاه که ممکن باشد، توصیه می‌شوند. توصیه می‌شود DEFR صلاحیت استفاده از ابزارهای معتبر را داشته باشد و برای حساب کردن اثراتی که این‌گونه ابزارها ممکن است بر سامانه داشته باشند، صلاحیت داشته باشد (برای مثال جایگزینی شواهد رقمی بالقوه، محتوای حافظه‌ای که هنگامی که نرم‌افزار بارگذاری می‌شود پاک می‌شود و غیره). همه‌ی فعالیت‌هایی که انجام شدند و تغییرات حاصل شده در شواهد رقمی بالقوه، توصیه می‌شود مستند شوند و درک شوند. اگر تشخیص اثر احتمالی معرفی ابزارها به سامانه ممکن نیست یا تغییرات نتیجه، با قطعیت قابل تشخیص نیست، توصیه می‌شود این نیز مستند شود.

- هنگام اکتساب داده‌ی فرار، توصیه می‌شود DEFR استفاده از یک محفظه‌ی پوشه منطقی که ممکن است را قبول کند و یکبار که حاوی پوشه‌های داده‌ی فرار است، مقدار درهم آن را مستند کند. در جایی که این امر امکان‌پذیر نیست، توصیه می‌شود یک محفظه از قبیل یک پوشه فشرده استفاده کند و سپس توصیه می‌شود درهم شود و مقدار آن مستند شود. توصیه می‌شود محفظه پوشه‌های نتیجه، در یک محیط ذخیره‌ساز دیجیتال رقمی که برای این منظور مهیا شده ذخیره شود، برای مثال قالب‌بندی شده است.

- با استفاده از یک ابزار تصویربرداری معتبر، فرآیند تصویربرداری را بر روی ذخیره‌ساز زنده غیرفرار اجرا کنید. توصیه می‌شود رونوشت شواهد رقمی منتج بر روی یک رسانه ذخیره‌سازی رقمی ذخیره شود که برای این منظور آماده شده است. در حالی که استفاده از یک رسانه ذخیره‌سازی جدید ترجیح داده می‌شود، استفاده از رونوشت‌های شواهد رقمی از فرآیندهای مجاز باعث تضمین یکپارچگی داده‌ها در زمان نوسازی می‌گردد. بنابراین، یک رسانه ذخیره‌سازی رقمی که مطابق با اصول می‌باشد، کفایت می‌کند. اگر تصویر را باید بر روی یک نگهدارنده پوشه منطقی ذخیره نمود، توصیه می‌شود DEFR مراقب باشد که تصویر خسارت نیابد یا از بین نرود.

یادآوری - در موقعیت‌هایی که افزاره قفل می‌باشد، دسترسی فیزیکی از طریق ابزار دیگری که دسترسی مستقیم به حافظه را ممکن ساخته‌اند (برای مثال، واسطه فایروایر)، قابل هدایت می‌باشد.

۳-۱-۳-۱-۷ فعالیت‌های افزوده: اکتساب افزاره رقمی روشن

موارد زیر بسته به پیکربندی افزاره رقمی خاص فعالیت‌های افزوده‌ای هستند که به اکتساب افزاره رقمی روشن مربوط می‌گردند:

- اکتساب داده‌های فرار را در حافظه RAM برای زمانی در نظر بگیرید که استفاده از رمزبندی مورد شک است. در وهله اول، بررسی کنید آیا این مورد به نظارت بر لوح خام یا استفاده از برخی ابزار شناسایی علائم رمز مربوط است. در این صورت، این نکته را به خاطر بسپارید که سامانه عامل میزبان زنده ممکن است غیرقابل اعتماد باشد و استفاده از ابزار مطمئن و مجاز را مورد توجه قرار دهید.

- از یک منبع زمانی مطمئن بهره برده و زمان هر کار انجام شده را مستند کنید.

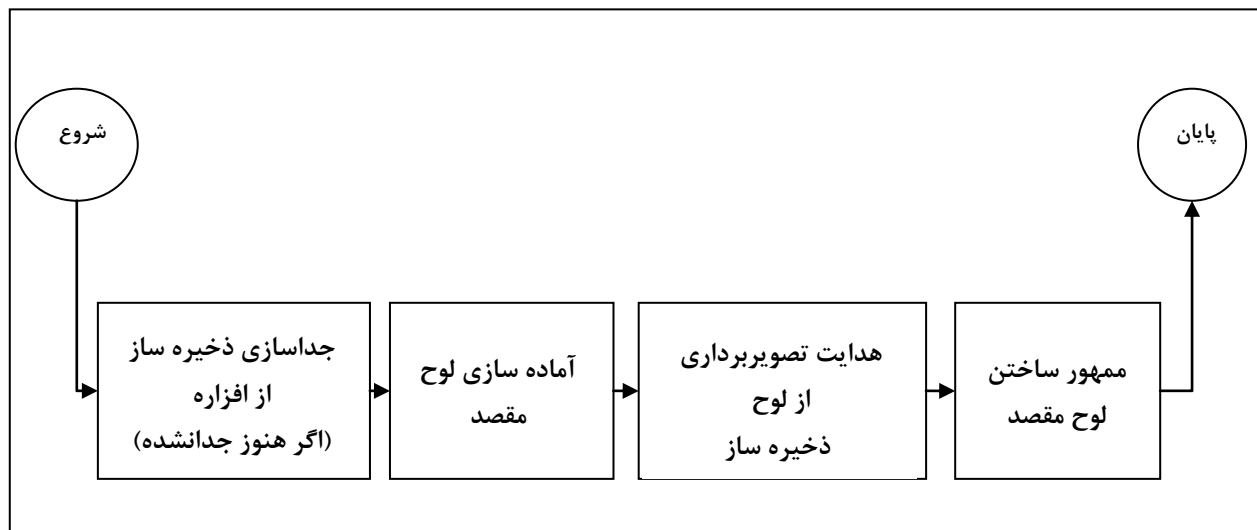
- مرتبط ساختن DEFR با شواهد دیجیتالی بالقوه کسب شده (با استفاده از امضاهای رقمی، زیست سنجش‌ها و عکس) ممکن است امری مناسب باشد.

یادآوری- عمل فشردن دکمه روشن کردن بر روی یک افزاره رقمی را می‌توان برای آماده‌سازی یک پوشه آغازگر پیکربندی نمود که ممکن است اطلاعات را تغییر داده و/یا آن‌ها را از سامانه قبل از خاموش کردن حذف کند یا سامانه‌های متصل را تغییر دهد به‌طوری‌که یک رویداد غیرمنتظره رخ داده است و داده‌های دارای ارزش استنادی قبل از شناسایی شدن، ممکن است پاک شوند. عمل مذکور را می‌تواند برای راه‌اندازی یک افزاره‌ای نیز پیکربندی نمود که به منظور ایجاد خسارت فیزیکی برای DEFR و دیگر افراد حاضر طراحی شده است.

۲-۳-۱-۷ افزاره‌های رقمی خاموش

۱-۲-۳-۱-۷ مرور کلی

مدیریت یک افزاره خاموش در مقایسه با یک افزاره روشن آسانتر است، چرا که نیازی به اکتساب داده‌های فرار وجود ندارد. شکل ۵ فعالیت‌هایی را نشان می‌دهد که برای اکتساب افزاره رقمی خاموش، کاربرپذیر هستند.



شکل ۵- راهنمایی‌هایی برای اکتساب افزاره‌ی رقمی خاموش

۲-۲-۳-۱-۷ اکتساب افزاره رقمی خاموش

فعالیت‌های زیر زمانی برای اکتساب منظور می‌گردند که افزاره دیجیتالی خاموش یافت شود:

- اطمینان حاصل کنید که افزاره واقعا خاموش است
- در صورت مناسب بودن شرایط، ذخیره‌ساز را از افزاره رقمی خاموش خارج کنید البته اگر از قبل خارج نشده باشد. ذخیره‌ساز را به‌عنوان حافظه مشکوک برچسب‌گذاری کرده و تمام جزییات را مستند سازید، از قبیل سازنده، نام مدل، شماره ردیف و حجم ذخیره‌ساز.
- فرآیند پردازش تصویر را با استفاده از ابزار تصویر برداری مجاز اجرا کنید تا یک رونوشت از شواهد رقمی لوح مشکوک ایجاد نمائید.

یادآوری- در بیشتر موارد، توصیه می‌شود رسانه ذخیره‌ساز از افزاره رقمی جدا نشود تا زمانی که اکتساب آن در غیر این صورت قابل انجام نمی‌باشد چرا که جداکردن ذخیره ساز باعث افزایش مخاطره خسارت یا اشتباه گرفتن آن با رسانه ذخیره‌ساز دیگر می‌گردد. توصیه می‌شود رویه‌های محلی مرتبط با جداسازی لوح‌های سخت، توسعه داده و پیروی شود.

۳-۳-۱-۷ افزاره‌های رقمی حیاتی

در برخی موارد، افزاره‌های رقمی را نمی‌توان به‌دلیل ماهیت حیاتی سامانه‌ها خاموش نمود. این سامانه‌ها هم‌چون خدمت‌گذارها در مراکز داده‌ها نیز می‌توانند به سرویس گیرنده‌های بی‌زیان، سامانه‌های نظارت، سامانه‌های پزشکی و چندین مورد دیگر خدمت ارائه دهند که ممکن است در حالت بحرانی تحت تاثیر قرار گیرند اگر متوقف گشته یا خاموش شوند. توصیه می‌شود توجه خاصی را در زمان کار با این چنین سامانه‌هایی مبذول داشت.

وقتی افزاره رقمی را نتوان خاموش نمود، اکتساب زنده و/یا جزیی را هدایت کنید، همان‌طور که در زیربندهای ۳-۱-۷ و ۴-۳-۱-۷ مورد بحث قرار گرفت.

۴-۳-۱-۷ اکتساب جزیی

- اکتساب جزیی بنا به دلایل متعددی ممکن است انجام شود، از قبیل:
- ذخیره‌ساز سامانه برای انجام اکتساب بسیار بزرگ است (برای مثال کارسازهای پایگاه داده)؛
- روشن بودن یک سامانه بسیار حیاتی است؛
- وقتی تنها داده‌های منتخب برای اکتساب شامل داده‌های نامرتبط در داخل همان سامانه می‌باشد؛ یا
- وقتی به‌وسیله مقام ذی‌صلاح قانونی ضبط شده است از قبیل اجازه تفتیش که حوزه اکتساب را محدود می‌سازد.
- وقتی تصمیمی برای انجام اکتساب جزیی اخذ شده است، توصیه می‌شود فعالیت‌های اکتساب شامل موارد زیر گردند، اما محدود به این موارد نمی‌شوند:
- شناسایی پوشه (ها)، پرونده (ها) یا هر سامانه مرتبط دیگری جهت اکتساب داده‌های مورد نظر،

- هدایت اکتساب منطقی بر روی آن دسته از داده‌های شناسایی شده.

۵-۳-۱-۷ رسانه ذخیره‌ساز رقمی

انواع متعددی از رسانه‌های ذخیره‌ساز رقمی را می‌توان در یک صحنه وقوع یافت. به طور معمول این رسانه‌ها پائین‌ترین نوع داده‌های فرار بوده و طی جمع‌آوری و اکتساب می‌توانند کمترین اولویت را داشته باشند. این نکته بدان معنا نیست که موارد مذکور مهم نیستند چرا که در بیشتر موارد، رسانه‌های ذخیره‌ساز بیرونی شامل رویدادهایی هستند که تحلیلگران به دنبال آن‌ها می‌باشند. یک DEFR باید از بابت موارد زیر اطمینان حاصل نماید:

- بررسی و مستندسازی محل (برای مثال قفسه راه‌انداز، کابل و متصل کننده، شکاف همه‌گذر و غیره)، سازنده، مدل و شماره ردیف (اگر موجود بود) هر رسانه ذخیره‌سازی رقمی یافت شده.

- تصمیم‌گیری در مورد جمع‌آوری رسانه ذخیره‌سازی رقمی شناسایی شده یا هدایت اکتساب در محل، توصیه می‌شود تصمیم مبتنی بر ماهیت رویداد و منابع در دسترس باشد. در راستای هدایت اکتساب در محل رسانه ذخیره‌ساز رقمی (در اصل لوح سخت)، به شکل ۴ مراجعه شود.

- اگر DEFR تصمیم به این کار گرفت و مجاز به جمع‌آوری رسانه ذخیره‌ساز رقمی بود، توصیه می‌شود رسانه‌های جمع‌آوری شده پوشانیده شده یا در یک بسته‌بندی مناسب قرار گیرند.

- تمام رسانه‌های ذخیره‌سازی رقمی و بخش‌های مرتبط با آن‌ها را برچسب‌زنی کنید. توصیه می‌شود برچسب‌های رویداد به طور مستقیم بر روی بخش‌های مکانیکی رسانه رقمی قرار نگیرند و اطلاعات مهم را نپوشانند از قبیل شماره ترتیب، نام مدل و شماره قطعه. توصیه می‌شود تمام رسانه‌های جمع‌آوری شده به نحوی اکتساب و ذخیره‌سازی یابند که از یکپارچگی رسانه‌های جمع‌آوری شده اطمینان حاصل شود. وقتی توصیه می‌شود رویدادهای احتمالی را با مهرهای مربوطه مهور نمود، توصیه می‌شود DEFR یا کارکنان دخیل در این امر بر روی برچسب امضا بزنند.

- توصیه می‌شود رسانه ذخیره‌ساز رقمی جمع‌آوری شده در محیطی مناسب برای حفاظت از داده‌ها ذخیره‌سازی یابد.

- رسانه‌های ذخیره‌سازی رقمی مختلف دارای قابلیت‌های مختلف برای نگهداری داده‌های هستند. توصیه می‌شود DEFR از بیشینه دوره زمانی قابل قبول آگاه باشد که از سوی مقام ذی‌صلاح مربوطه تعیین می‌گردد، باتوجه به قابلیت‌های نگهداری داده‌ها در رسانه ذخیره‌ساز رقمی.

۴-۱-۷ حفاظت

پس از تکمیل فرآیند اکتساب، توصیه می‌شود DEFR داده‌های کسب شده را با استفاده از توابع درستی - سنجی یا امضاهای رقمی مهور نماید تا تعیین کند رونوشت‌های شواهد رقمی معادل یا اصل هستند. علاوه

بر این، ابعاد امنیتی نیازمند کنترل گرهایی هستند که اصول حفظ محرمانگی، یکپارچگی و در دسترس پذیری شواهد رقمی بالقوه را اعمال می کنند. در راستای حفاظت در برابر تباہ سازی، جنبه های محیطی توصیه می شود با شاخص های مناسب بیان شوند. یک DEFR باید از موارد زیر اطمینان حاصل نماید:

- استفاده از تابع مناسب برای درستی سنجی در جهت فراهم ساختن شواهدی که پرونده های رونوشت شده معادل با اصل هستند.

- مرتبط ساختن DEFR با شواهد رقمی بالقوه کسب شده (با استفاده از امضاهای رقمی، زیست سنج ها و عکس) ممکن است مناسب عمل کند.

- از تمام افزاره های رقمی که جمع آوری شدند باید به طور مناسبی محافظت بعمل آید. انواع مختلف افزاره های رقمی ممکن است نیازمند روشهای مختلف حفاظت و نگهداری باشند. شواهد رقمی بالقوه باید در کل دوره استفاده مورد محافظت قرار گیرند که ممکن است با توجه به حوزه های قضایی و خط مشی های سازمانی متغیر باشد.

یادآوری - به عنوان جایگزینی برای ممهور ساختن داده های کسب شده با توابع درستی سنجی یا امضاهای رقمی، DEFR می تواند از ویژگی های زیست سنجی بهره ببرد. زیست سنجی از مشخصه های فیزیکی و رفتاری برای تعیین هویت یک فرد استفاده می کند. با پیوست یک افزار زیست سنج به شواهد کسب شده، می توان اطمینان حاصل کرد که شواهد بدون تشخیص ویژگی زیست سنج قابل دست کاری نیست.

۲-۷ افزاره های شبکه شده

۱-۲-۷ شناسایی

۱-۱-۲-۷ مرور کلی

در این بند، افزاره های شبکه به عنوان رایانه یا دیگر افزاره های ملاحظه شده اند که در حالت سیمی یا بی سیم به شبکه متصل هستند. این افزاره های شبکه شده ممکن است شامل بزرگ رایانه ها، کارسازها، رایانه های رومیزی، راه گزین های بی سیم، سوده ها، هاب ها، مسیریاب ها، افزاره های سیار، دستیاران رقمی شخصی، PED ها، افزاره های بلوتوث، سامانه های دوربین مدار بسته و غیره باشند. توجه داشته باشید که اگر افزاره های رقمی شبکه شوند، تعیین محل ذخیره سازی نتیجه جستجوی شواهد رقمی بالقوه دشوار می گردد. داده ها را می توان در هر جایی بر روی شبکه قرار داد.

شناسایی یک افزاره رقمی شامل مولفه هایی چون نشان واره های تولید کننده، شماره ردیف ها، کلاف ها و تطبیق دهنده های برق. یک DEFR می تواند ابعاد زیر را به عنوان شاخصه های شناسایی منظور گرداند:

- مشخصه های افزاره: تولید کننده یک افزاره رقمی را می توان بعضی اوقات با مشخصه های قابل مشاهده آن شناسایی نمود، به خصوص اگر عناصر طراحی خاصی به کار گرفته شده باشند.

- واسطه افزاره: متصل کننده برق اغلب خاص تولید کننده بوده و یک کمک قابل اعتنا برای شناسایی است.

- برچسب افزاره: برای افزاره‌های سیار خاموش، اطلاعات به‌دست آمده از داخل حفره باطری را می‌توان نشان داد، به خصوص وقتی با یک پایگاه داده مناسب پیوسته باشد. برای مثال، IMEI یک عدد ۱۵ رقمی است که تولیدکننده، نوع مدل و کشور تایید کننده افزاره‌های GSM را نشان می‌دهد؛ ESN یک شناسه ۳۲ رقمی منحصر به فرد می‌باشد که بر روی یک تراشه ایمن در یک تلفن همراه به‌وسیله تولید کننده مستند می‌گردد- ۸ تا ۱۴ رقم اول تولید کننده را نشان داده و بیت‌های مابقی شماره ردیف تخصیص یافته را شناسایی می‌کنند.

- جستجوی معکوس: در مورد تلفن‌های همراه، اگر شماره تلفن مشخص باشد، یک جستجوی معکوس را می‌توان برای شناسایی متصدی شبکه مورد استفاده قرار داد.

به‌دلیل حجم به نسبت کوچک افزاره‌های سیار، DEFR باید توجه بیشتری را برای شناسایی تمام انواع افزاره‌های سیاری مبذول دارد که ممکن است به مورد تحت تجسس مرتبط باشد. یک DEFR باید صحنه وقوع جرم مشکوک را حفاظت کرده و اطمینان حاصل نماید که هیچ فردی افزاره‌های سیار یا هر افزاره رقمی دیگری را از صحنه جدا نمی‌کند. افزاره‌های رقمی که ممکن است شامل شواهد رقمی باشند باید از دسترسی غیرمجاز حفاظت شوند.

یادآوری- در برخی موارد، توصیه می‌شود ارتباط را قطع نکرد. در مورد مسایل احتمالی افراد مجاز را مطلع سازید (برای مثال، به افراد ناشناخته در مورد افزاره خاموش کردن هشدار ندهیم).

۲-۱-۲-۷ جستجو و مستندسازی صحنه وقوع فیزیکی

قبل از آنکه هرگونه اکتساب یا جمع‌آوری قابل انجام باشد، توصیه می‌شود صحنه وقوع به یک شیوه بصری به‌وسیله عکسبرداری، فیلم برداری یا ترسیم صحنه از همان ورودی، مستند گردد. انتخاب روش مستندسازی باید مطابق با شرایط، هزینه، زمان، منابع دردسترس و اولویت‌ها صورت پذیرد. توصیه می‌شود DEFR تمام اقلام دیگر در صحنه را مستندسازی نماید، مواردی که ممکن است شامل موارد مرتبط هم‌چون نوشته‌های ناخوانا، یادآوری‌های روزانه، خاطرات روزانه و غیره، گردد.

- توصیه می‌شود DEFR نوع، نامان، مدل و شماره ردیف‌های هر افزاره رقمی مورد استفاده را مستند ساخته و آن دسته از افزاره‌های رقمی را شناسایی کند که طی این مرحله اولیه باید اکتساب یا جمع‌آوری گردند. تمام افزاره‌های سیار و اقلام مرتبط با آن‌ها از قبیل کارت‌های حافظه، سیم کارتها، شارژکننده‌ها و کلاف‌های یافت‌شده در صحنه و همین‌طور شماره ردیف‌های مربوطه آن‌ها و هرگونه ویژگی شناسایی کننده‌ای، در صورت لزوم توصیه می‌شود مستند و جمع‌آوری شوند. همچنین برای یافتن بسته‌بندی اصلی تلفن‌های همراه نیز تلاش کنید؛ این تلفن‌ها ممکن است حاوی کدهای PIN یا PUK باشند.

- اگر افزاره به شبکه متصل باشد، توصیه می‌شود DEFR خدمات قابل عرضه توسط افزاره‌ها را شناسایی کند تا قبل از تصمیم‌گیری در مورد قطع افزاره از شبکه وابستگی‌ها و فوریت افزاره‌های در داخل شبکه را شناخته و تعیین کند. این امر در صورتی مهم است که افزاره‌ها آن دسته از توابع بحرانی را اجرا کنند که

هیچ گونه زمان خاموشی را نمی‌توانند تحمل کنند و مانع از بین رفتن شواهد رقمی بالقوه می‌گردند. با این حال، اگر به نظر تهدیدات مبتنی بر شبکه برای افزارها وجود دارند، DEFR ممکن است درمورد قطع دستگاه از شبکه جهت حفاظت از شواهد رقمی بالقوه تصمیم‌گیری کند.

- اگر افزار شبکه‌بندی شده یک سامانه تلویزیون مدار بسته است، توصیه می‌شود DEFR به تعداد دوربین‌های متصل به سامانه توجه کند و همین‌طور به دوربین‌هایی که فعال هستند. توصیه می‌شود DEFR به سازنده، مدل و تنظیمات اصلی سامانه از قبیل تنظیمات صفحه نمایش، تنظیمات ضبط جاری و محل ذخیره‌سازی به‌طوری‌که اگر قرار است تغییراتی برای تسهیل فرآیند جمع‌آوری و اکتساب انجام داد، توجه کند. بنابراین امکان بازگرداندن سامانه به وضعیت اصلی خود وجود داشته باشد.

- تا جایی که امکان دارد، توصیه می‌شود وضعیت افزارهای رقمی همان‌طور که هست باقی بماند. در کل، اگر افزارهای رقمی خاموش باشند، توصیه نمی‌شود DEFR آن‌ها را روشن کند و اگر روشن هستند، توصیه نمی‌شود DEFR آن‌ها را خاموش کند. این امر می‌تواند مانع از تباہ‌سازی غیرضروری از شواهد رقمی بالقوه گردد. افزارهای که دارای باتری‌هایی است که ممکن است تمام شوند، باید جهت حصول اطمینان از بین نرفتن اطلاعات، همیشه در شارژ باشند. یک DEFR باید رسانه‌ها و کابل شارژکننده بالقوه را طی این مرحله شناسایی کند. اگر قرار است افزارهای در آینده نزدیک منتقل شود یا مورد آزمایش قرار گیرد، بهتر است آن را خاموش کنیم تا پتانسیل خسارت برای داده‌های موجود در افزار را تا حد کمینه کاهش دهیم.

- توصیه می‌شود DEFR استفاده از یک آشکارساز سیگنال بی‌سیم را نیز برای شناسایی و آشکارسازی یک سیگنال بی‌سیم از افزارهای بی‌سیم مخفی، در نظر بگیرد. ممکن است نمونه‌هایی وجود داشته باشند که در آن‌ها آشکارساز سیگنال بی‌سیم به دلیل محدودیت‌های هزینه و زمان مورد استفاده قرار نمی‌گیرند و توصیه می‌شود DEFR آن را مستند نماید.

۲-۲-۷ جمع‌آوری، اکتساب و حفاظت

۱-۲-۲-۷ مرور کلی

یک DEFR باید تصمیم بگیرد که شواهد رقمی بالقوه را از افزارهای رقمی جمع‌آوری یا اکتساب نماید. این انتخاب باید مطابق با شرایط، هزینه، زمان، منابع در دسترس و اولویت‌ها باشد.

اگر DEFR تصمیم به قطع افزارها نمود، فرآیند جمع‌آوری یا اکتساب شواهد رقمی بالقوه از موارد مشروحه در زیربند ۴-۵ پیروی خواهد کرد. در صورتیکه نتوان افزارها را از شبکه قطع نمود، به دلیل فوریت استفاده از آن یا احتمال از بین رفتن شواهد رقمی بالقوه، توصیه می‌شود DEFR اکتساب زنده را هدایت کند درحالی‌که افزارها به شبکه به صورت متصل باقی می‌مانند.

یادآوری - داشتن رویه‌های استاندارد ضروری است که از ابزار معتبر بهره می‌برند، البته همراه با مستندسازی مطلوب و یک

اکتساب و جمع‌آوری شواهد رقمی بالقوه از افزاره‌های سیار شبکه شده پیچیده می‌باشند، چرا که آن‌ها می‌توانند در حالات و وضعیت‌های متعدد تعامل قرار داشته باشند از قبیل بلوتوث، بسامد رادیویی، صفحه لمسی و مادون قرمز. علاوه بر این، تولید کنندگان مختلف افزاره‌های بی‌سیم از انواع مختلف سامانه‌های عامل بهره می‌برند و نیازمند روشهای مختلفی برای اکتساب شواهد هستند. همچنین گستره وسیعی از کارت‌های حافظه وجود دارد که با افزاره‌های بی‌سیم مورد استفاده قرار می‌گیرند و جداکردن این کارت‌های حافظه از افزاره‌های بی‌سیم روشن ممکن است باعث اختلال در اجرای فرآیندها گردد.

در کل، افزاره‌های بی‌سیم مانند دستیاران رقمی شخصی و تلفن‌های همراه نیز باید روشن شوند تا شواهد رقمی بالقوه را کسب کنند. این افزاره‌ها به طور پیوسته محیط اجرایی خود را در حالی که روشن هستند تغییر می‌دهند، برای مثال زمان ساعت قابل بروزرسانی است. مشکل اینجاست که دو رونوشت شواهد رقمی بالقوه نمی‌توانند استانداردهای درستی‌سنجی از قبیل درهم سازی را بگذرانند. در این موقعیت، دیگر توابع درهم‌ساز که وجوه اشتراک و/یا تفاوت را شناسایی می‌کنند، ممکن است بهتر باشد.

این نکته حایز اهمیت است که توصیه نمی‌شود DEFR افزاره‌های Wi-Fi یا بلوتوث را وارد صحنه‌هایی کند که می‌توانند اطلاعات مشترک بروی افزاره‌های رقمی بالقوه را تغییر دهند. این امر در صورتی بسیار مهم است که مامور تجسس بخواهد بداند چه افزاره‌هایی متصل هستند.

اگر DEFR تصمیم گرفت که از یک فرآیند اکتساب پیروی کند، توصیه می‌شود افزاره‌های شبکه به اجرای امور خود جهت تحلیل بیشتر ادامه دهند تا دیگر افزاره‌های متصل به شبکه تعیین شوند. توصیه می‌شود DEFR احتمال خرابه‌کاری عمدی از سوی فرد مظنون از طریق اتصال شبکه فعال در نظر بگیرد و تصمیم بگیرد که سامانه را مورد نظارت قرار دهد یا آن را قطع کند.

۲-۲-۲-۷ راهنمایی‌هایی برای جمع‌آوری افزاره‌های شبکه شده

در برخی شرایط، متصل نگه داشتن افزاره‌های شبکه شده بهتر است به‌طوری‌که فعالیت را بتوان از سوی DEFR و/یا DES با مقام ذی‌صلاح مورد نظارت و مستندسازی قرار داد. در صورت عدم لزوم، توصیه می‌شود افزاره‌ها به شرح زیر جمع‌آوری شوند:

- توصیه می‌شود DEFR افزاره را از شبکه جدا کند، وقتی قطعی شد که هیچ داده مرتبطی با این کار مجدد نوشته نخواهد شد و هیچ خرابه‌کاری در سامانه‌های مهم رخ نخواهد داد (از قبیل سامانه‌های مدیریت تجهیزات در بیمارستان‌ها). این کار را می‌توان با جداسازی اتصالات شبکه سیمی از سامانه تلفن یا درگاه شبکه یا همین‌طور غیرفعال‌سازی اتصال با نقطه دسترسی بی‌سیم انجام داد.

- قبل از جداسازی شبکه‌های سیمی، توصیه می‌شود DEFR اتصالات به افزاره‌های رقمی را پیگیری کرده و درگاه‌های لازم برای اتصالات آتی در کل شبکه را برچسب‌گذاری نماید. یک افزاره ممکن است دارای

بیش از یک روش ارتباطی باشد. برای مثال، یک رایانه ممکن است دارای شبکه‌های محلی سیمی، یک مودم بی‌سیم و کارت‌های تلفن همراه باشد. PEDها نیز ممکن است به شبکه از طریق وای فای، بلوتوث یا اتصالات شبکه تلفن همراه متصل گردند. توصیه می‌شود DEFR سعی در شناسایی تمام روش‌های ارتباطی داشته و فعالیت‌های مناسب برای حفاظت در برابر تخریب شواهد رقمی بالقوه انجام دهد.

- آگاه باشید که جداسازی منبع تغذیه از افزاره‌های شبکه‌بندی شده در این نقطه ممکن است باعث از بین رفتن داده‌های فرآر. از قبیل فرآیندهای در حال اجرا، اتصالات شبکه و داده‌های ذخیره شده در حافظه گردد. سامانه‌عامل میزبان ممکن است نامطمئن بوده و اطلاعات اشتباه را گزارش دهد. توصیه می‌شود DEFR این اطلاعات را با استفاده از روش‌های معتبر ضبط کند و منبع تغذیه را از این افزاره‌ها جدا نماید. وقتی DEFR از بابت عدم از بین رفتن شواهد رقمی بالقوه مطمئن شد، اتصالات را می‌توان از افزاره‌های رقمی جدا نمود.

- اگر جمع‌آوری نسبت به اکتساب اولویت داشته باشد و مشخص باشد که افزاره شامل حافظه فرآر است، توصیه می‌شود افزاره به طور پیوسته به یک منبع تغذیه متصل باشد.

- اگر افزاره سیار خاموش باشد، به دقت آن را بسته‌بندی کرده، ممه‌ور نمایید و افزاره را برچسب‌زنی کنید. این کار برای جلوگیری از هر گونه عملیات تصادفی یا خرابه‌کارانهٔ کلیدها یا دکمه‌ها صورت می‌پذیرد. در نتیجه و به‌عنوان یک پیش‌هشدار، توصیه می‌شود DEFR استفاده از جعبه‌های فارادی یا پوشش‌دار را نیز مورد توجه قرار دهد.

- تحت برخی شرایط، توصیه می‌شود افزاره‌های سیار در حین جمع‌آوری خاموش باشند تا از تغییر داده‌ها جلوگیری شود. این امر ممکن است به وسیله‌ی ارتباط خروجی و ورودی یا دستوراتی که می‌توانند شواهد رقمی بالقوه را نابود کنند، اتفاق افتد.

- در نتیجه، هر افزاره رقمی را می‌توان به‌عنوان یک افزاره مستقل در نظر گرفت (به بند ۷-۱ مراجعه شود) تا زمانی که مورد آزمایش قرار گیرد. طی آزمایش، توصیه می‌شود این افزاره به‌عنوان یک افزاره شبکه شده ملاحظه گردد.

یادآوری - پیاده‌سازی یک شکل از شبکه با استفاده از افزاره‌های ذخیره‌ساز قابل جداسازی به‌عنوان نشانه‌های انتقال ممکن می‌باشد. توصیه می‌شود DEFR ملاحظه نماید که آیا این افزاره‌ها که در حال جمع‌آوری به این روش مورد استفاده قرار خواهند گرفت و در این صورت به دنبال اطلاعاتی در مورد دیگر افزاره‌ها در چنین شبکه‌ای بگردد.

۳-۲-۲-۷ راهنمایی‌های برای اکتساب افزاره شبکه شده

در موقعیتی که افزاره‌ها به یک شبکه متصل هستند، این احتمال وجود دارد که افزاره‌ها به بیش از یک شبکه فیزیکی و / یا شبکه مجازی متصل باشند. برای مثال، افزاره‌ای که به نظر دارای یک اتصال شبکه فیزیکی قابل مشاهده می‌باشد شاید در واقع بر روی یک شبکه مجازی شخصی (VPN) و دستگاه مجازی دارای بیش

از یک آدرس IP در حال اجرا می‌باشد. در چنین حالتی، قبل از قطع کردن افزاره از شبکه، توصیه می‌شود DEFR اکتساب منطقی داده‌های مربوط به اتصال شبکه منطقی را هدایت نماید. (برای مثال اتصال به شبکه اینترنت). داده‌های مرتبط به پیکربندی IP و جداول مسیریابی مربوط می‌شوند اما به آن‌ها محدود نمی‌گردند.

برای یک افزاره شبکه که لازم است به طور پیوسته روشن باشد، توصیه می‌شود افزاره را از تعامل با شبکه رادیویی بی‌سیم (برای مثال افزاره‌های دارای سامانه موقعیت‌یابی جهانی) بر حذر داشت. توصیه می‌شود DEFR روش‌های مجاز اعلام شده از سوی قوانین محلی را برای جداسازی سیگنال‌های رادیویی به کار گیرد. با این حال، توصیه می‌شود احتیاط لازم جهت کسب اطمینان از این‌که افزاره دارای منبع تغذیه کافی می‌باشد، صورت پذیرد، همان‌طور که روش‌های جداسازی ممکن است منجر به استفاده از نیروی اضافی در تلاشی برای اتصال به یک شبکه گردند. روش‌های جداسازی می‌توانند مربوط به موارد زیر گردند اما نه محدود به آن‌ها:

- استفاده از یک افزاره پخش اغتشاش که دارای توانایی مسدود ساختن انتقال می‌باشد، این کار از طریق ایجاد تداخل قوی در زمان پخش سیگنال‌های افزاره در گستره بسامدی یکسان با افزاره‌های سیار صورت می‌پذیرد.

یادآوری ۱- استفاده از افزاره‌های پخش پارازیت ممکن است با الزامات قانونی عنوان شده در برخی آیین‌نامه‌های قانونی در تضاد باشند.

یادآوری ۲- استفاده از افزاره‌های پخش پارازیت ممکن است دارای تأثیر منفی بر رفتار افزاره‌های الکترونیکی هم‌چون تجهیزات پزشکی باشد.

- استفاده از یک محیط کاری دارای پوشش برای هدایت آزمایشات ایمن در یک محل ثابت توصیه می‌شود. ایجاد پوشش را می‌توان برای کل محیط کاری یا از طریق راه‌اندازی تجهیزات فارادی^۱ هدایت نمود که امکان جابه‌جایی را فراهم می‌سازند. تغذیه کابل‌ها به داخل این محفظه مشکل‌ساز می‌باشد، با این حال از آن‌جایی که بدون تفکیک مناسب آن‌ها می‌توانند رفتاری هم‌چون یک آنتن داشته باشند، باعث ضعف در رسیدن به هدف آن محفظه می‌گردند. فضای کاری را نیز می‌توان بسیار محدود ساخت.

- استفاده از یک فضای کاری دارای پوشش جهت هدایت آزمایشات ایمن در یک محل ثابت توصیه می‌شود. یک فضای کاری دارای پوشش بسامد رادیویی یا نگهدارنده (یک قفسه فارادی) را می‌توان برای جلوگیری از اتصالات به شبکه مورد استفاده قرار دهد.

یادآوری ۳- توصیه می‌شود تمام روش‌های مسدود ساختن دسترسی بی‌سیم به شبکه‌ها را برای استفاده بر روی بسامدهای مناسب بررسی نمود. توصیه می‌شود این عمل بررسی و اعتبارسنجی، به آن دسته از کابل‌هایی که از میان پوشش ایجاد شده عبور می‌کنند، گسترش یابد.

1- Faraday

- استفاده از یک جایگزین (U)SIM که از شناسایی افزاره اصلی تقلید کرده و مانع از دسترسی شبکه به وسیله افزاره می‌گردد. این کارت‌ها دارای توانایی تغییر هویت افزاره جهت قبول نمودن آن‌ها به‌عنوان (U)SIM اصلی فراهم کردن امکان هدایت آزمایشات ایمن در هر محلی می‌باشند. توصیه می‌شود (U)SIM را برای افزاره و شبکه قبل از استفاده مورد بررسی و درستی‌سنجی قرار داد.

- خدمات شبکه را با فراهم کردن حامل خدمت سیار و شناسایی جزییات بر روی خدمات مورد نظر برای غیرفعال‌سازی (برای نمونه شناسایی‌کننده تجهیزات، شناسایی‌کننده مشترک، یا شماره تلفن) غیرفعال نماید. با این حال، چنین اطلاعاتی را همیشه نمی‌توان به راحتی دسترسی‌پذیر نمود چرا که فرآیند هماهنگی و تأیید با تأخیر همراه است.

یک DEFR می‌تواند اکتساب زنده افزاره بی‌سیم را قبل از جداسازی باتری هدایت کند (برای مثال، برای دسترسی به سیم کارت). این کار را می‌توان در راستای جلوگیری از بین رفتن اطلاعات مهم بالقوه در حافظه جانبی تلفن همراه یا تسهیل فرآیند آزمایش انجام داد (برای مثال در جایی که باور بر این است که افزاره را می‌توان به وسیله یک PIN یا PUK محافظت نمود که بخش قابل توجهی از زمان را برای دسترسی به خود اختصاص می‌دهد).

یادآوری ۴- توصیه می‌شود DEFR اطمینان حاصل نماید که جمع‌آوری و اکتساب شواهد رقمی بالقوه در ارتباط با قوانین و آیین‌نامه‌های محلی می‌باشند، همان‌طور که براساس شرایط خاص مورد نیاز می‌باشند.

۴-۲-۷ راهنمایی‌هایی برای حفاظت از افزاره شبکه شده

بنابر ماهیت افزاره‌های رقمی و شواهد رقمی بالقوه، راهنمایی‌ها برای حفاظت از افزاره‌های شبکه شده هم‌چون راهنمایی‌های مربوط به حفاظت از رایانه‌ها، افزاره‌های جانبی و رسانه‌های ذخیره‌ساز رقمی می‌باشد. جهت کسب جزییات مربوط به حفاظت از افزاره به زیربند ۷-۱-۴ مراجعه شود.

۳-۷ حفاظت، اکتساب و جمع‌آوری دوربین‌های مدار بسته

توصیه می‌شود DEFR درک کند که رویکرد استخراج دنباله‌های ویدیویی از یک سامانه مبتنی بر رایانه یا تلویزیون مدار بسته با استخراج شواهد رقمی متداول از یک رایانه متفاوت می‌باشد. در زیر برخی راهنمایی‌های خاص برای اکتساب شواهد رقمی بالقوه از سامانه‌های تلویزیون مدار بسته ارائه شده‌اند:

- قبل از شروع فرآیند اکتساب، توصیه می‌شود DEFR در وهله اول تعیین کند که آیا سامانه دنباله ویدیویی مورد نظر را مستند ساخته است یا خیر. در نتیجه، توصیه می‌شود DEFR قاب زمانی ویدیوی مورد نیاز را تعیین کرده و زمان سامانه را با زمان صحیح مورد توجه قرار دهد و هرگونه نکته خاص را مورد توجه قرار دهد. همچنین توصیه می‌شود DEFR تعیین کند که چه دوربین‌هایی مورد نیاز هستند و این که آیا آن‌ها را می‌توان به طور مجزا اکتساب نمود. توصیه می‌شود DEFR به سازنده و مدل سامانه توجه کند. این اطلاعات می‌تواند جهت عرضه نرم‌افزار صحیح برای بازپخش مورد نیاز باشند.

- توصیه می‌شود DEFR تمام ضبط‌های دوربینی مرتبط را طی زمان مورد نظر برای حفاظت از اطلاعات افزوده‌ی تجسس اکتساب نماید، این اطلاعات می‌توانند در مراحل بعدی توسعه یابند. توصیه می‌شود DEFR به تمام دوربین‌های متصل به یک سامانه تلویزیون مدار بسته توجه نموده و تعیین کند که آیا آن‌ها به طور فعال در حال ضبط باشند یا خیر.

توصیه می‌شود DEFR این موارد را تعیین کند: حجم ذخیره‌ساز سامانه تلویزیون مدار بسته و همین‌طور زمان جای نوشت اطلاعات ویدیویی. این اطلاعات به DEFR اجازه خواهد داد تا بداند چه مدتی دنباله ویدیویی بر روی سامانه قبل از، از بین رفتن باقی خواهد ماند. توصیه می‌شود برخی اقدامات جهت کسب اطمینان از عدم تغییر شواهد انجام پذیرد. برای شواهد ویدیویی رقمی، حفاظت در برابر نوشتن را باید در محل انجام داد.

- چند گزینه وجود دارند که DEFR می‌تواند آن‌ها را جهت اکتساب شواهد رقمی بالقوه از سامانه‌های تلویزیون مدار بسته انتخاب نماید :

۱- اکتساب پوشه‌های ویدیویی با نوشتن آن‌ها بر روی لوح فشرده / لوح همه کاره / Blu-ray اما این کار در صورتی که پوشه ویدیویی بسیار حجیم باشد عملی نخواهد بود.

۲- اکتساب پوشه‌های ویدیویی با نوشتن آن‌ها بر روی رسانه ذخیره‌سازی بیرونی.

۳- اکتساب پوشه‌های ویدیویی از طریق یک اتصال شبکه. این کار در صورتی ممکن خواهد بود که سامانه تلویزیون مدار بسته به تجهیزات شبکه مجهز باشد.

۴- استفاده از ویژگی تبدیل سامانه تلویزیون مدار بسته به قالب‌های پوشه‌ای دیگر (به طور معمول MPEG یا AVI) که یک نسخه فشرده از پوشه ویدیویی است. توصیه می‌شود این کار به‌عنوان آخرین راه حل مورد استفاده قرار گیرد چرا که فشرده‌سازی مجدد باعث تغییر داده‌ها شده و همیشه جزئیات تصویر را از بین می‌برد. تکیه بر داده‌های دوباره فشرده شده برای آزمایش توصیه نمی‌شود در صورتی که داده‌های اصلی وجود داشته و برای تحلیل در دسترس می‌باشند.

یادآوری ۱- کیفیت پوشه ویدیویی تبدیل شده نمی‌تواند به خوبی پوشه اصلی باشد.

۵- وقتی که امکان اکتساب مستقیم به یک رونوشت شواهد رقمی از پوشه‌ها بر روی افزاره ضبط وجود ندارد، توصیه می‌شود DEFR یا DES سعی در اکتساب یک نسخه قیاسی از خروجی قیاسی موجود بر افزاره ضبط کننده اصلی با استفاده از یک افزاره ضبط قیاسی مناسب داشته باشند.

- به محض تکمیل اکتساب، توصیه می‌شود پوشه کسب شده در راستای تأیید صحیح بودن پوشه یا این که بخش درست پوشه اکتساب شده است، مورد بررسی قرار گیرد. توصیه می‌شود این پوشه با نرم‌افزار پخش

کننده نیز مورد بررسی قرار گیرد (برای قالب‌های پوشه افزاره رقمی) تا امکان پخش آن بر روی سامانه‌های دیگر مورد آزمون قرار گیرد- بیشتر سامانه‌های تلویزیون مدار بسته اختصاصی بوده و پوشه‌ها ضرورتاً با استفاده از نرم‌افزار پخش دیگری قابل استفاده نمی‌باشند. از طریق نرم‌افزار مربوطه می‌توان هم‌زمان با ضبط به پخش و مشاهده پوشه ویدیویی نیز پرداخت.

- توصیه می‌شود رسانه ذخیره‌ساز رقمی که شامل پوشه کسب شده است به‌عنوان رونوشت شواهد رقمی اصلی منظور گردد. اگر پوشه بر روی یک رایانه کتابی یا یک افزاره کارت حافظه / همه‌گذر ریخته شود، پس توصیه می‌شود یک رونوشت دائم اصلی را از این موارد به سرعت تهیه نمود.

- در نتیجه، توصیه می‌شود DEFR در صورتی سامانه تلویزیون مدار بسته را مجدد راه‌اندازی کند که خاموش باشد. توصیه می‌شود این کار در حضور فرد ذی‌صلاح صورت پذیرد.

در شرایطی که هدایت اکتساب در صحنه عملی نیست، توصیه می‌شود DEFR تصمیم به جمع‌آوری رسانه ذخیره‌سازی رقمی بگیرد. یک روش سریع همان جایگزینی لوح سخت سامانه تلویزیون مدار بسته با یک لوح سخت خالی می‌باشد. با این حال، توصیه می‌شود DEFR مخاطرات متعددی را قبل از استفاده از این روش مورد ارزیابی قرار دهد، از قبیل انطباق لوح سخت جدید با سامانه و انطباق لوح سخت جدا شده با دیگر سامانه‌های مورد نظر برای آزمایش.

یادآوری ۲- برخی سامانه‌ها دارای یک لوح سخت قابل جداسازی در یک قفسه می‌باشند، اما این لوح سخت ممکن است برای بازپخش نیازمند سخت‌افزار سامانه باشد.

اگر هیچ کدام از روش‌های فوق عملی نشد، پس توصیه می‌شود کل سامانه تلویزیون مدار بسته از صحنه جدا شده و توصیه می‌شود فرآیند اکتساب مجدد در یک آزمایشگاه قانونی صورت پذیرد. این کار راه حل پایانی DEFR می‌باشد با فرض این‌که انجام این کار به صورت فیزیکی ممکن می‌باشد چرا که برخی سامانه‌های تلویزیون مدار بسته به شدت بزرگ و پیچیده می‌باشند. مجدد، توصیه می‌شود DEFR مخاطراتی را در رابطه با الزامات قانونی و بیمه قبل از جداسازی در نظر بگیرد.

بنابر ماهیت افزاره‌های رقمی و شواهد رقمی بالقوه، راهنمایی‌ها برای حفاظت از سامانه‌های تلویزیون مدار بسته هم‌چون راهنمایی‌های مربوط به حفاظت از رایانه‌ها، افزاره‌های جانبی و سامانه‌های ذخیره‌ساز رقمی می‌باشند. جهت کسب جزییات بیشتر در مورد حفاظت از سامانه تلویزیون مدار بسته به زیربند ۷-۱-۴ مراجعه شود.

پیوست الف

(اطلاعاتی)

مهارت‌های اصلی DEFR و شرح صلاحیت

جدول الف - ۱ - نمونه‌های از شرح صلاحیت

شماره	مهارت‌های اصلی	شرح مهارت‌های اصلی	شرح صلاحیت		
			آگاهی (۱)	دانش (۲)	مهارت (۳)
۱	شناسایی شواهد رقمی	مشخص نمودن افزاره رقمی، مولفه‌ها، اطلاعاتی که می‌توانند به تجسس کمک کنند و همین‌طور قوانین مرتبط برای بررسی شواهد رقمی بالقوه و جرم مرتبط با رایانه. شناسایی الزامات ابزاری برای جمع‌آوری و اکتساب داده و افزاره‌ها و همین‌طور ارزیابی مخاطره.	کاربر عمومی فناوری اطلاعات و مدیریت در چندین نوع از افزاره‌های فناوری اطلاعات و افزاره‌های شبکه؛ رویه‌های تجسس در صحنه جرم؛ تعیین وضعیت افزاره؛ ارزش اطلاعات استنادی؛ افزاره‌های مرتبط با مسایل حقوقی شبکه و اطلاعات.	پیکربندی گزارشات و سامانه/ برنامه کاربردی؛ شناسایی گزارش‌های سامانه و برنامه کاربردی شامل پست الکترونیک، گزارش‌های وب، نوشت، گزارش‌های دسترسی، گزارش‌های اسمرمز، پوشه‌های sysconfig، اطلاعات IP میزبان، کارکرد و وابستگی افزاره؛ توانایی در درک اثر برروی شواهد فرار و غیرفرار.	تحلیل خاص؛ تفسیر گزارش برای آشکار-سازی نفوذ در شناسایی دیگر سامانه‌های تحت تاثیر (برخی مراجع قضایی نیازمند تایید شواهد فعلی قبل از جمع‌آوری هستند)؛ شناسایی کلمات عبور لازم برای افزاره‌های مربوطه قبل از جمع-آوری، شناسایی نمودار شبکه و مکانیزم‌های کنترل دسترسی برای شناخت و بستگی‌ها، آدرس‌های IP پیوند و آدرس‌های MAC برای تایید افزاره
۲	جمع‌آوری شواهد رقمی	الزامات ابزاری و پیاده-سازی بسته‌بندی شواهد رقمی، حفاظت در برابر تهدیدهای زیست محیطی. زمینه‌های کاری شامل امنیت اطلاعاتی.	جمع‌آوری ایمن داده‌ها؛ اصول و طراحی ابزار اولیه؛ تعیین بهترین روش برای جمع‌آوری در راستای حفظ اطلاعات بیشینه مرتبط با رویداد.	تنظیم و اجرای فرآیند جمع‌آوری؛ جمع‌آوری شواهد؛ ایجاد اسناد شواهد؛ زنجیره وقوع؛ کیفیت کنترل فرآیند جمع‌آوری شواهد؛ مصاحبه با مظنون.	بهینه‌سازی فرآیند جمع‌آوری؛ مستند سازی شواهدی که قابل اکتساب نیستند (به دلیل محدودیت-های متعدد)؛ جمع-آوری کلمات عبور، کلیدها، قفل‌های سخت‌افزاری و دیگر اطلاعات لازم برای

شماره	مهارت‌های اصلی	شرح مهارت‌های اصلی	شرح صلاحیت		
			آگاهی (۱)	دانش (۲)	مهارت (۳)
					تحلیل در آزمایشگاه.
۳	اکتساب شواهد رقمی	اعمال الزامات اکتساب شواهد رقمی بالقوه در شکل منطقی، کسب اطمینان از تکرارپذیری، قابل سازگاری، قابلیت بازتولید و قابلیت دفاع. زمینه‌های تحت پوشش: انجام اکتساب بر روی سامانه روشن، انجام اکتساب بر روی سامانه خاموش و مسایل حقوقی شبکه.	شناخت اطلاعات موجود در افزاره‌های رقمی، اسناد تولید شده توسط سامانه، داده‌های تولیدشده توسط کاربر و داده‌ی فرار؛ پوشه‌های سامانه‌ای یونیکس و ویندوز و وسایل برقی؛ آگاهی از تاثیر بر روی داده‌های فرار.	دانستن چگونگی تعیین الزامات ذخیره سازی؛ اجرای رویه اکتساب تصویربرداری (برای مثال اکتساب رسانه‌های ذخیره سازی رقمی به صورت کامل و جزئی)؛ اجرای اکتساب بر روی یک سامانه روشن، اجرای اکتساب بر روی یک سامانه خاموش؛ ایجاد مقدار هش	توانایی برای هدایت اکتساب رسانه ذخیره سازی رقمی شامل RAID، پایگاه داده، وسایل برقی و افزاره‌های کوچک شده؛ شناخت وابستگی‌ها و تاثیر بر روی روش‌های مختلف اکتساب.
۴	حفاظت از شواهد رقمی	اعمال و ارزیابی الزامات برای حفاظت از شواهد رقمی بالقوه، شناخت عوامل و پارامترهای تاثیرگذار بر روی صحت آن. زمینه‌های تحت پوشش: روش‌شناسی، نگهداری از زنجیره توقیف، بررسی افزاره رایانه‌ای و رسانه‌های ذخیره سازی رقمی.	شناخت الزامات و رویه‌ها برای نگهداری زنجیره توقیف در برابر الزامات قانونی؛ تاثیر زیست محیطی از قبیل رطوبت، دما و ضربه به سمت افزاره رقمی؛ شناخت گزینه های بسته بندی، حمل و نقل و الزامات ذخیره سازی.	شناخت چگونگی تولید اسناد نظارت بر شواهد؛ تعریف پارامترهایی برای اسناد؛ تضمین امنیت اطلاعات، تهدیدها، آسیب پذیری و کنترل شواهد رقمی.	اعمال سنجش‌ها برای شواهد رقمی ایمن به شکل افزاره-های بزرگ تا افزاره-های دستی کوچک شده؛ رویه‌هایی برای مستندسازی جزییات شواهد.

جدول الف - ۲ - تعریف صلاحیت

۱	آگاهی - تشخیص، شناسایی - درخواست کمک در صورت لزوم
۲	دانش - کسب شده از طریق آموزش رسمی یا کار در یک گروه. شرکت کردن، دخیل بودن - انجام کار با کمک
۳	مهارت - تجربه اثبات شده از طریق کار در محیط کاری. کارهای بدون نظارت. اعمال، نشان دادن - انجام کار بدون کمک
یادآوری - صلاحیت یک DEFR می تواند از یک حوزه قضایی تا حوزه دیگر تغییر کند.	

پیوست ب

(اطلاعاتی)

کمیته الزامات مستندسازی برای انتقال شواهد

توصیه می‌شود DEFR مسؤول داده‌ی کسب شده و افزاره‌های رقمی در هر زمانی باشد، در حالی که این موارد در زنجیره توقیف و اختیارات خود هستند. در راستای حفظ این کنترل، توصیه می‌شود DEFR دارای در حد مناسب مجاز، آموزش دیده و واجد شرایط باشد. با این حال، از آنجایی که قانون محلی یک عامل تعیین کننده در توانایی DEFR برای پیروی از هر سه الزام مورد انتظار می‌باشد، شایستگی یک DEFR ممکن است از یک مرجع قضایی به مرجع دیگر متفاوت باشد. در نتیجه، این احتمال وجود دارد که الزامات مستندسازی برای انتقال شواهد رقمی قضایی در محکمه‌های مختلف یکسان نباشند.

به همین صورت، کمیته مجموعه الزامات مستندسازی باید تعیین گردند تا تبادل بین محکمه‌ای شواهد رقمی بالقوه را معین کنند. این الزامات مستندسازی باید با نکات مستندسازی مذکور در بند ۶-۶ منظور گردند. از آنجایی که این استاندارد بین‌المللی الزامات قانونی خاص هیچ حوزه قضایی را جایگزین نمی‌کند، به‌عنوان یک راهنمای عملی برای انتقال شواهد رقمی بالقوه در تمام مرزهای قانونی عمل می‌کند.

کمیته مستندسازی جهت برقراری ارتباط به شرح زیر می‌باشد:

- نام و نشانی مقام ذی‌صلاح مربوطه؛
 - سند مجوز، آموزش و شرایط لازم DEFR؛
 - هدف از آزمایش؛
 - کارهایی که انجام شده‌اند؛
 - چه کسانی کارها را انجام داند و در چه زمانی؛
 - زنجیره توقیف مربوط به تجسس؛
 - فهرست تشریحی شواهد رقمی بالقوه و رسانه‌های ذخیره‌ساز رقمی جمع‌آوری شده و اکتساب یافته؛ و
 - اطلاعات مربوط به هر آزمایش، آزمون و تجسس مورد استفاده برای ایجاد رونوشت شواهد.
- الزامات خاص مرجع قضایی ممکن است شامل موارد زیر گردند:
- اگر شواهد به‌عنوان یک نظر کارشناسی منظور می‌گردند، تایید کارشناس شاهد ذی‌صلاح؛ و
- دستور دادگاه که تعیین می‌کند کدام مستندات باید انتقال یابند و دلیل انتقال.

کتابنامه

- [۱] استاندارد ملی ایران شماره ۱۷۰۲۴ : سال ۱۳۸۶، ارزیابی انطباق - الزامات کلی برای موسسه‌های گواهی کننده اشخاص
- [۲] استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات - الزامات
- [۳] استاندارد ملی ایران شماره ۲۷۰۰۲ : سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات - آیین کار مدیریت امنیت اطلاعات
- [۴] استاندارد ملی ایران شماره ۲۷۰۳۱ : سال ۱۳۹۱، فناوری اطلاعات - فنون امنیتی - راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب و کار
- [۵] استاندارد ملی ایران شماره ۲۷۰۳۵ : سال ۱۳۹۲، فناوری اطلاعات - فنون امنیتی - مدیریت رخداد امنیت اطلاعات
- [6] ILAC-G19:2002. Guidelines for forensic science laboratories. Available from: www.ilac.org/documents/g19_2002.pdf
- [7] IOCE, G8 proposed principles for the procedures relating to digital evidence. Available from: <http://ioce.org/core.php?ID=5>
- [8] ISO/IEC 15489:2001, Information and Documentation — Records Management
- [9] ISO/IEC 17043:2010, Conformity assessment — General requirements for proficiency testing
- [10] ISO/IEC 24760-1, Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts
- [11] Forensic Science Society Academic Accreditation Standards & CPD. Available from: <http://www.forensic-science-society.org.uk>
- [12] Guidelines for evidence collection and archiving. Available from: <http://www.ietf.org/rfc/rfc3227.txt>