اینترپل

رهنمودهای جهانی برای آزمایشگاه های جرمیابی دیجیتالی

این راهنما توسط آزمایشگاه جرمیابی دیجیتال در مرکز نوآوری اینترپل آماده شده است.

سؤالات خود را مستقیماً مطرح کنید:

مرکز نوآوری اینترپل

18 Napier Road

Singapore 258510

رایانامه: dfl@interpol.int

تلفن: 6565503462+

مقدمه دبیر کل

رهنمودهای جهانی اینترپل برای آزمایشگاه های جرمیابی دیجیتالی

در محیط امنیتی بین المللی پیچیده کنونی، تحقیقات به افراد بسیار حرفه ایی و متخصص نیاز دارد.

برای درک بهتر این مشکلات، یکی از توانایی های پلیسی که اینترپل بروی آن متمرکز شده است جرمیابی دیجیتالی می باشد. شیوه در حال تغییری که نیاز به رویه و سیاست های قوی دارد.

تعداد در حال رشد ابزار آلات ارتباطی نظیر گوشی های هوشمند، ساعت ها، جی پی اس می توانند اطلاعات معنی داری را بصورت بالقوه که خود قسمتی از مدارک دیجیتالی در نظر گرفته شوند در خود نگاه دارند.

برای مواجه با این مشکلات در حال رشد، اینترپل بوسیله ابداع مرکز آزمایشگاه جرمیابی دیجیتال، به دیگر کشورهای عضو کمک می کند تا ظرفیت جرمیابی دیجیتال ملی و پروسه های مدیریتی شواهد الکترونیکی را برای پشتیبانی بازجویی ها و تحقیقات ایجاد کنند.

به عنوان طرح جهانی بی طرف برای مشارکت در اجرای قانون، اینترپل در حال کار کردن بروی تشویق و افزایش ارتباط و اشتغال در فرآیندهای توسعه در بین کشورهای عضو می باشد.

این مهم یکی از نیروهای محرک در بطن ایجاد رهنمود های جهانی اینترپل برای آزمایشگاه های جرمیابی دیجیتالی می باشد که اصول و روندهای اصلی را خلاصه می کند که برای کارورزان ضروری به نظر می رسد.

این رهنمود ها همچنین قسمتی از مسئولیت های بعدی ما برای ایجاد دنیا به عنوان محلی با بستر مجازی و فیزیکی امن می باشد و مایل هستم از هر کسی که برای پیشرفت خود همکاری می کند تشکر کنم.

یورگن استاک

سردبیر اینترپل

نامه ایی از مدیر مرکز نوآوری اینترپل

پیشینه متغیر جرمیابی دیجیتالی ارتباط تنگا تنگش را با نوآوری نشان می دهد. افزایش سریع ماهیت فضای دیجیتالی و تکنولوژی ها بدین مفهوم است که مقدار زیادی از علائم دیجیتالی و داده ها می تواند در یک چشم به هم زدن بوجود آیند. نوآوری مستمر در حوزه جرمیابی دیجیتال اگر برای اجرای قانون الزام به حساب نیاید حتما ضروری به نظر می رسد.

در سطح جهانی بسیاری از جرائم پیشتر موجود با برخورداری از پیشرفت در تکنولوژی و ماهیت فرامرزی جهان به هم تنیده ما، در حال گسترش به سمت تهدید جهانی چشمگیری هستند. بعلاوه، ما شاهد پدیدار شدن انواع بی سابقه ایی از فعالیتهای جنایی در گستره اجرای قانون هستیم. این پیشرفت ها در حال افزودن لایه های دیگری از پیچیدگی به مشکلات می باشد.

در برابر این درورنما، اینترپل مرکز نوآوری خود را در سال۲۰۱۷ در کشور سنگاپور با هدف کمک رسانی از راه نوآوری در جهت اجرای جهانی قوانین، تاسیس کرد. آزمایشگاه جرمیابی دیجیتالی در این مرکز منجر به تلاشهایی برای بالابردن توانایی های جرمیابی دیجیتالی در کشورهای عضو شده است. من واقعا معتقدم که وظیفه آزمایشگاه های جرمیابی دیجیتال بخش حیاتی در کنترل و مبارزه با بزه های دیجیتال ایفا می کند. در واقع، متخصصین جرمیابی دیجیتال ناگزیر در یادگیری پی در پی و گسترش دانش خود در زمینه ظهور خانه ها/ شهرهای دیجیتال، ماشین های متصل، پهبادها، شبکه های موبایل و طرح های کلود می باشند.

بدین منظور، آزمایشگاه جرمیابی دیجیتال جلسات گروه متخصصین جرمیابی دیجیتال را سالانه در سالهای اخیر برگزار کرده است که متخصصین جرمیابی را برای اجرا قانون، صنعت و دانشگاه به دور هم گرد آورده است تا اطلاعات، دانش و بهترین عملیات ممکنه را به اشتراک بگذارند. فراهم آوردن شبکه جهانی متخصصین در جرمیابی دیجیتال به صورت عظیمی در خدمت رسانی موثر به کشورهای عضو با ارزش و مفید می باشد.

رهنمود ها سعی در ایجاد بستری جهانی برای ایجاد و مدیریت کردن یک آزمایشگاه جرمیابی دیجیتالی است که در هر قسمت از جهان کاربرد دارد. این موضوع بصورت امیدوارانه کننده شکاف بین اعضا در خصوص عملیات جرمیابی دیجیتال و ظرفیت آنها را از بین می برد. در سایه امیدواری ایجاد جنبش در حوزه جرمیابی دیجیتال به جهت مستحکم شدن بخش کنترل و نظارت، مرکز نوآوری اینترپل پیش قراول ایجاد روح نوآوری در فعالیتهای آزمایشگاههای جرمیابی دیجیتال در کشورهای عضو با هدف مشارکت در چالشهای پیچیده آتی در امنیت جهانی می باشد.

آنیتا هزنبرگ

مدیر مرکز نوآوری اینترپل

عنوان مقاله: رهنمودهای جهانی برای آزمایشگاه های جرمیابی دیجیتالی

تاریخ انتشار: 2019 می 13

زبان اصلی: انگلیسی

دیگر زبانها: انگلیسی، فارسی

فهرست

منابع و مآخذ

1. A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory, Council of Europe (COE), Version 1.1, June 2017

2. Scientific Working Group on Digital Evidence (SWGDE), https://swgde.org

3. ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers, version 5, 2012, https://digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

تعاریف و اختصارها

AFF	Advanced Forensic Format	قالب جرمیابی پیشرفته
DCO	Device Configuration Overlay	پوشش پیکربندی دستگاه
DF	Digital Forensic	جرمیابی دیجیتال
DFL	Digital Forensics Laboratory	آزمایشگاه جرمیابی دیجیتال
EWF	Expert Witness Format	قالب تخصصی شواهد
HPA	Host Protected Area	محدوده محافظت شده
IDEN	Integrated Digital Enhanced Network	شبکه یکپارچه دیجیتال پیشرفته
IMEI	International Mobile Equipment Identity Number	شماره شناسایی تجهیزات موبایل بین المللی
MEID	Mobile Equipment Identity Number	شماره شناسایی تجهیزات موبایل
PDP	Personal Development Portfolio (PDP)	پروتفولیوی پیشرفت کارمندان
RAM	Random Access Memory	حافظه ی دسترسی تصادفی
SIM	Subscriber Identity Module	واحد شناسایی مشترک
SWGDE	Scientific Working Group on Electronic evidence	کارگروه علمی شواهد الکترونیکی

۱- مقدمه

۱.۱- هدف سند

رهنمود های اینترپل در آزمایشگاههای جرمیابی دیجیتال، در روند بنا کردن و مدیریت این آزمایشگاهها و ایجاد رهنمود های تکنیکی برای مدیریت و پردازش کردن مدارک الکترونیکی خلاصه میشود.

به هنگام در نظر گرفتن گسترش توانایی جرمیابی دیجیتال آنها، این رهنمود ها می بایست به عنوان یک سند الگو دیده شوند که بتوسط کشورهای عضو مورد استفاده قرار گیرد. در خصوص وضع قانون بین المللی، به اجرا در آوردن و رویه های آن، راهنمایی های ارائه شده قصد دارد که در هر سطح استراتژیک و تاکتیکی مورد استفاده قرار گیرد.

۱.۲- مخاطبین هدف

این مدارک برای استفاده به توسط کشورهای عضو اینترپل طراحی شده. اهداف این رهنمود ها این گونه است که اطمینان به عمل آورد که مدارک دیجیتالی تولید شده توسط آزمایشگاه جرمیابی دیجیتال در دادگاه های کشورهای عضو در روند سیستم های قضایی جنایی بین المللی قابل قبول می باشد.

رهنمود ها قصد دارند عمدتا بروی دو گروه مجزا متمرکز شوند: اول استراتژیست های جرمیابی دیجیتال و مدیرانی که برای آزمایشگاه های جرمیابی دیجیتال تصمیم سازی می کنند; و دومی کارمندان تکنیکی که با شواهد الکترونیک بصورت روزانه سروکار دارند.

بعلاوه، بازپرس ها، قاضی ها و وکلا از این مدرک در فهم روند جرمیابی دیجیتال که در مشاغلشان ضرورت دارد بهره می برند.

۱.۳- استفاده از مدارک

رهنمود ها قصد در ایجاد محدودیت در آزمایشگاههای جرمیابی دیجیتال ندارند که می بایست از الزامات بسترهای حقوقی بین المللی آنها پیروی کند. توصیه ارائه شده در این رهنمود ها قصد تضاد با هیچ یک از قوانین بین المللی در کشورهای عضو را ندارد.

۲- مقدمه ایی بر جرمیابی دیجیتال

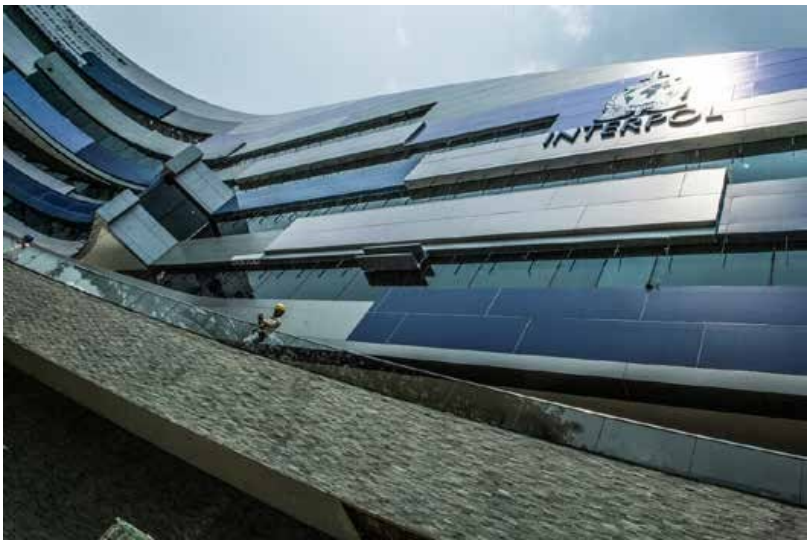
۲.۱- جرمیابی دیجیتال

جرمیابی دیجیتال شاخه ایی است از علم جرمیابی که بروی شناسایی، بدست آوری، پردازش، آنالیز و گزارش داده ها بروی یک کامپیوتر، لوازم دیجیتالی یا دیگر وسایلی که قابلیت نگهداری رسانه را دارد متمرکز میشود.

کامپیوتر، وسایل الکترونیک یا دیگر سیستم های نگهداری اطلاعات دیجیتالی که داده های ارزشمند را برای تفتیش و بازجویی نگاه میدارد به عنوان سند الکترونیک می شناسند. به عنوان مثال لپ تاپ ها، گوشی های هوشمند، سرورها، ضبط کننده های ویدویی دیجیتال، سیستم های CCTV، پهبادها، سیستم های جی پی اس و کنسول های بازی از انواع آن می باشند.

هدف اصلی جرمیابی دیجیتال استخراج داده ها از شواهد الکترونیکی، پروسه داده ها به اطلاعات مفید و ارائه داده ها برای پیگرد قانونی می باشد. همه رویه ها موجود در آن می بایست از تکنیک های صدا شناسی جرائم بهره ببرد تا یافته ها در دادگاه قابل استناد باشد.

ماهیت مواردیکه اسناد دیجیتال را شامل میشود عمدتا بدون مرز می باشد و جرم در کسری از زمان رخ می دهد.
بنابراین یافته های بدست آمده از شواهد الکترونیک می بایست از یک سری از استانداردهای رهنمود ها پیروی کنند که نه تنها مورد پذیرش فقط یک دادگاه در یک کشور باشد بلکه در سیستم های بین المللی جهانی مورد قبول باشد.
رهنمود های اینترپل برای جرمیابی دیجیتال یک خط مبنا و مرجع برای مدیریت جرائم این دست فراهم می سازد.



۲.۲- مفهوم شواهد الکترونیکی

شواهد الکترونیکی، برخلاف دیگر شواهد، از قبیل فیبر، و بقایای مو و شلیک گلوله بدلیل واقعیتهای ذیل چالش برانگیز هستند:

الف- داده ها می توانند در چندین موقعیت فیزیکی، در بعضی اوقات در کشورها پخش شوند،

ب- داده ها می توانند بدون دردسر درون قلمرو یک کشور در کسری از ثانیه منتقل شوند.

ج- آن داده ها بسیار فرار- تغییر سریع بوده و بوسیله ضرب یک دکمه رونویسی، خراب یا از بین می روند.

د- از آن داده ها بدون اینکه از بین روند میشود کپی تهیه کرد.

ه- گسترده زمانی شواهد الکترونیکی، برخلاف هیچ یک از گروه اسناد جرائمی، پیش از آنکه بصورت بلااستفاده درآیند کوتاه است. یک نمونه از آن گوشی های هوشمند است که بعد از پنج سال ممکن است که روشن نشود یا از نظر کارکردی درست عمل نکند.

بنابراین بر پایه این واقعیت ها شواهد الکترونیکی می بایست پردازش شده و با احتیاط لازم و کافی به کار برده شوند.

۲.۳- اصول شواهد الکترونیکی

هنگامیکه با شواهد الکترونیکی سروکار داریم اصول زیر را می بایست مد نظر قرار داد:

الف- شواهد الکترونیکی می بایست بر اساس رفتار حقوقی بدست آید.

ب- کارمندان آن می بایست دوره های آموزشی مناسب را پیش از اشتغال به شواهد الکترونیکی به پایان رسانده باشند.

ج- هر اقدام بکارگرفته در شواهد الکترونیک نمی بایست باعث تغییر داده های آن شود. در صورت نیاز برای دسترسی به اصل داده ها یا تغییر زمینه سیستم ها، توصیه میشود که تنها کارمندان مجاز می توانند چنین کاری انجام دهند، و خود آن کارمند است که قادر به توجیه آن فعالیت ها است.

د-هر فعالیتی که برای دسترسی یا تغییر نیاز به داده های اصلی دارد باید ضبط شود و یک فرد متخصص در صورت لزوم شاهد آن باشد.

ه- ضبط همه فعالیتهای گرفته شده هنگام اشتغال به شواهد الکترونیک می بایست انجام شود و محافظت شود به گونه ای که بشود به آن رسیدگی کرد. یک شخص غیر وابسته می بایست قادر باشد آن فعالیتها را تکرار کرده و به همان نتایج دست یابد.

۳- مدیریت آزمایشگاه جرمیابی دیجیتالی

این بخش درباره پروسه تاسیس یک آزمایشگاه جرمیابی دیجیتال صحبت می کند که برنامه آن را ایجاد کرده، منابع مورد نیاز و فعالیت های مرتبط با حفظ آن را ارائه می دهد.

۳.۱- اعمال برنامه

تحقیق اولیه می بایست به منظور فراهم کردن آمار جدید بروی تصرف شواهد الکترونیک، انواع جرائم، مکان، تخصصی کردن مامور ثبت و ضبط و کدامیک از آنالیز جرمیابی دیجیتال صورت گرفته انجام شود.

اطلاعات می بایست راهنمایی نسبتا خوبی را بمنظور رشد تحقیق دیجیتال فراهم کند و از آن به عنوان نشانه ایی برای شروع آن تحقیق استفاده شود. این اطلاعات همچنین میبایست به آژانس برای شناسایی الزامات سرمایه گذاری بعلاوه سایز آزمایشگاه جرمیابی دیجیتال کمک کند.

هر آژانسی می بایست به دنبال فهم الزامات رویه ایی یا حقوقی در استقرار آزمایشگاه جرمیابی دیجیتال در سیستم قضایی جنایی کشور خود باشد. که می تواند از طریق مقایسه با کشورهای دارای جغرافیای یکسان و همان اندازه جمعیت که قبلا آن آزمایشگاه را بنا کرده اند صورت پذیرد که به فهم دقیق الزامات استقرار آن کمک می کند.

یافتن جواب برای سوالات آورده شده در زیر به تصمیم گیرندگان برای فهم و شناخت حوزه آزمایشگاههای جرمیابی دیجیتال کمک خواهد کرد:

الف- چه میزان تحقیق با استفاده از داده های دیجیتال در ۳، ۲ و ۱ سال گذشته در جرائم گزارش شده، تسهیل شده اند؟

ب- آیا رشد مستند و واضحی از بررسی ها در این نوع وجود دارد؟

پ- اگر تحقیق دیجیتالی نیاز بود:

- چه کسی آنالیز را انجام داده است؟
- از کدام رویه پیروی شده؟
- نتیجه چه شد؟
- هزینه بررسی ها چه بود؟
- امکان نبود که بعضی از کارکردها را به علت فقدان منابع حذف کرد؟

ج- آیا آژانس های دیگر اجرا کننده قانون در آن کشور که یک الزام مشابه دارند وجود دارد، که با آن امکان شروع یک مشارکت برای تسریع پذیرش طرح آزمایشگاه جرمیابی دیجیتال بوجود آید؟

۳.۲- محوطه

هنگام انتخاب محل برای ساخت آزمایشگاه، نیاز به رعایت چندین فاکتور است تا موفقیت تضمین شود. در هنگام بنا کردن آزمایشگاه بخش ذیل به صورت مفصل فاکتورهای ممکن در موفقیت را شرح می دهد.

۳.۲.۱- مکان

چندین فاکتور مورد نیاز برای انتخاب مکان اجرا آزمایشگاه نیاز است. چندمورد که نیاز به توجه است در زیر آمده است:

ملاحضات انتخاب محل آزمایشگاه جرائم دیجیتال	
۱	آیا منبع برق کافی به جهت راه اندازی تجهیزات مورد نیاز در اختیار هست، آیا تجهیزات اضافی برای مکمل برق مانند ژنراتور یا یو پی اس وجود دارد؟
۲	اگر آزمایشگاه در بالای زمین است آسانسور به جهت انتقال مقادیر بزرگ اسناد الکترونیک موجود است؟
۳	آیا ساختمان یا دفتر به اندازه ایی قوی است که امنیت داده ها و افراد موجود در آن حفظ شود؟
۴	آیا دیوار، طبقات و سقف به اندازه ایی قوی هست که در برابر خسارت های محیطی و فیزیکی مقاومت کند؟
۵	خطرات ناشی از سیل،آتش سوزی، آسیب طبیعی و ناآرامی های مدنی چیست؟
۶	آیا مراقبت کافی برای کاهش حملات تروریستی یا سازمان های جنایی برای خلل در تحقیقات انجام گرفته است؟

۷	آیا تجهیزات تهویه مناسب مورد نیاز در ساختمان موجود است یا باید چیزی به آن افزود

۳.۲.۲- امنیت فیزیکی

آزمایشگاه فقط نیاز به تامین امنیت اسناد الکترونیک نداشته بلکه نیاز به تامین امنیت کارمندان و نرم افزار و سخت افزار ارزشمند خود نیز دارد.

چک لیست امنیت فیزیکی	
۱	سیستم نظارت این سیستم برای نمایش محوطه هایی است که ممکن است مورد دسترسی غیر مجاز و غیر قانونی قرار گیرد. به کار گماردن حرفه ایی ها باعث نظارت بر استراتژیک ترین محل و همچنین بهترین تصمیم گیری برای اطمینان از حداکثر امنیت میشود.
۲	کنترل دسترسی کنترل دسترسی می تواند به شکل قفل های فیزیکی و کلید، کلیدهای دیجیتال، کارتهای مغناطیسی و/ یا بیومتری ها می باشد که بستگی به بودجه دارد.
۳	سیستم اطفا حریق یک آزمایشگاه می بایست مجهز به سیستم کاهش و کنترل آتش در محوطه باشد. مواد مورد استفاده برای کنترل و سرکوب آتش نمی بایست به پرسنل و تجهیزات صدمه وارد کند.
۴	محافظت از دیوار، در و پنجره در زمان نیاز پنجره با میله و قفل می بایست جهت ممانعت از ورود غیرمجاز تقویت شود. اگر آزمایشگاه پنجره و دیوار شیشه ایی دارد اقدامات احتیاطی برای محافظت از داده های حساس انجام شده و خارج از دید نگاه داشته شود. در ضد آتش در محل راهروها و نردبان جهت جلوگیری از ورود آتش به محوطه نصب شود.

۵	نصب کافی سوکت برق، فیوز و تابلوهای جریان برق این تجهیزات از پر باری که منجر به آتش سوزی و به خطر افتادن امنیت کارکنان و آزمایشگاه میشود جلوگیری می کند
۶	طبقه ضد ساکن(ایستا) به کاهش تخلیه الکترواستاتیک ممکن در طبقه که به کارمندان و تجهیزات و اسناد صدمه می زند.
۷	سیستم پارازیت ماهواره ایی توصیه میشود که آزمایشگاه یک سیستم برای انسداد سیگنال های شبکه به عنوان مثال قفس فارادی یا وسیله پارازیتی داشته باشد. سیستم پارازیت ماهواره ایی هر سیگنالی را مسدود کرده و هرگونه ورود سرزده را به محل جلوگیری می کند. با تکنولوژی وایرلس کنونی امکان اتصال به شبکه به صورت اتوماتیک برای گوشی های هوشمند و لپ تاپ وجود دارد از اینرو داده های آنها را اصلاح می کنند. قانون گذاری ملی می بایست بررسی شود که امکان استفاده از چنین سیستم هایی تایید شود و با دیگر سیستم ها تداخلی نداشته باشند.
۸	سیستم خنک کننده برای یک آزمایشگاه با داشتن کامپیوتر برای انجام کار تولید حجم زیادی از گرما درون آن اجتناب ناپذیر است. گرما بیش از حد منجر به از بین رفتن داده ها و آسیب به سخت افزار میشود. درآزمایشگاه یک سیستم خنک کننده می بایست نصب شود تا دمای اتاق و اتاق سرور و نگهداری اسناد را کنترل کند.
۹	بک آپ از دیتا در خارج از محل تعداد زیادی از داده ها در آزمایشگاه نگهداری میشود هنگامیکه بصورت قابل استفاده در آمد و ذاتا حساس هستند. داده ها معمولا در سرور نگهداری میشوند. بهترین عمل برای داده ها این است که جهت بک آپ گیری در خارج از محل سرور ذخیره شود. در مواقع بلایای طبیعی که آزمایشگاه درگیر همچین موضوعی میشود. نگهداری در اینگونه محل ها برای دسترسی به داده های با اهمیت کاربرد دارد. داشتن یک محل ذخیره داده در خارج از محل قسمتی از برنامه بازیابی در زمان بلای طبیعی است که تضمین می کند که عملیات در زمان کوتاهی انجام میشود.
۱۰	ذخیره داده های آرشیوی/ ذخیره بلند مدت داده ها پس از آنالیز، داده ها می بایست در محلی که بعدا به عنوان رویه قضایی مورد استفاده قرار بگیرد ذخیره میشود. ذخیره زمانی می بایست مطابق با الزامات حقوقی کشور باشد.

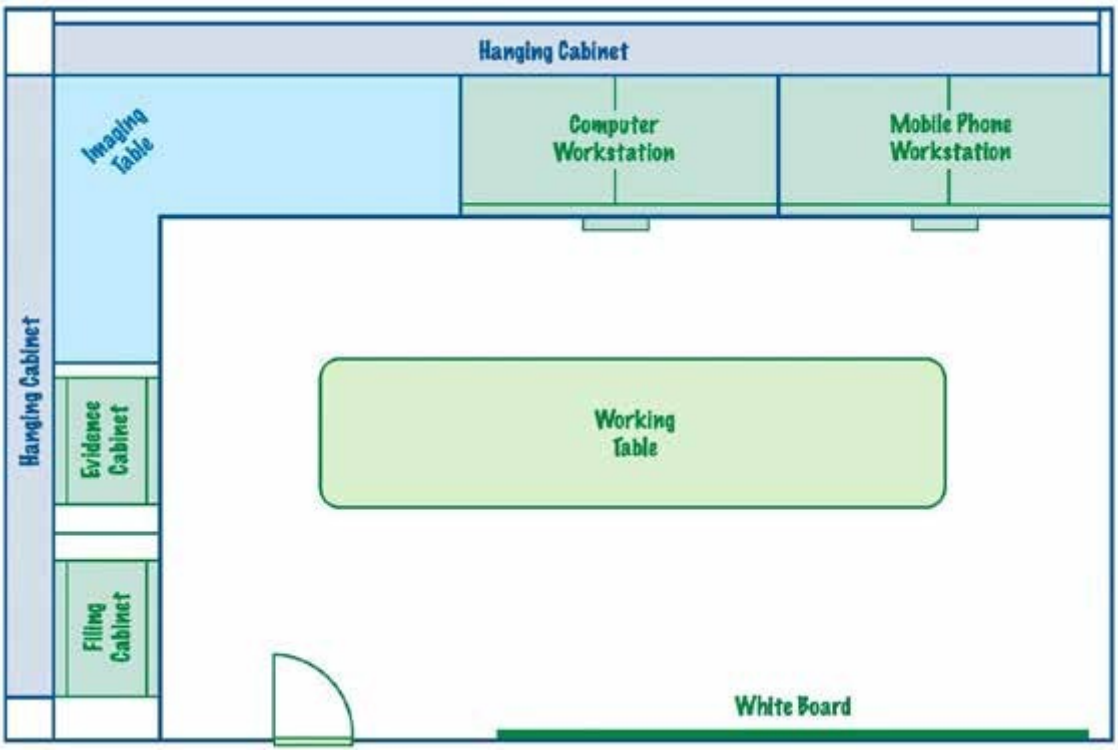
۳.۲.۳- سایز و طرح بندی

حداقل یک آزمایشگاه می بایست تبلت های رومیزی برای آزمایش کنندگان جهت انجام آنالیز نیاز دارد. یک تبلت بزرگ برای ثبت اسناد، برچسب گذاری، عکسبرداری و مهرو موم کردن یک کابینت ضد حریق برای نگهداری اسناد الکترونیکی و یک کابینت بایگانی. این مقدار حداقلی برای آزمایشگاه با مقیاس کوچک که با مقدار کمی اسناد سروکار دارد مناسب است

اگرچه برای یک آژانس که با مقدار زیادی از اسناد الکترونیکی سروکار دارد این مقدار حداقل ناکافی به نظر می رسد. توصیه میشود که در آزمایشگاه انواع مخصوصی از فعالیتها را در محل های جدا از هم به جهت جلوگیری از آلودگی های متقابل انجام داد.

به عنوان مثال محلی باید برای اسناد دریافتی باشد. این موضوع در مخل پذیرش انجام میشود که آزمایش کننده درخواست را شرح دهد و درخواست کننده و تکنسین سند دریافتی را ثبت می کند.

به عنوان مثال آزمایشگاه، آزمایشگاه گوشی همراه یا آزمایشگاه کامپیوتر فقط برای کارمندان آزمایشگاه قابل دسترسی باشد. هر آزمایش کننده به میز بزرگی برای تجهیزات IT کابینت بایگانی برای نگهداری فایلها و صندلی های راحتی نیاز دارد. بعلاوه صفحه کلید ارگونومیک و تشک های راحتی جهت سهولت کار آزمایش کننده نیاز است.

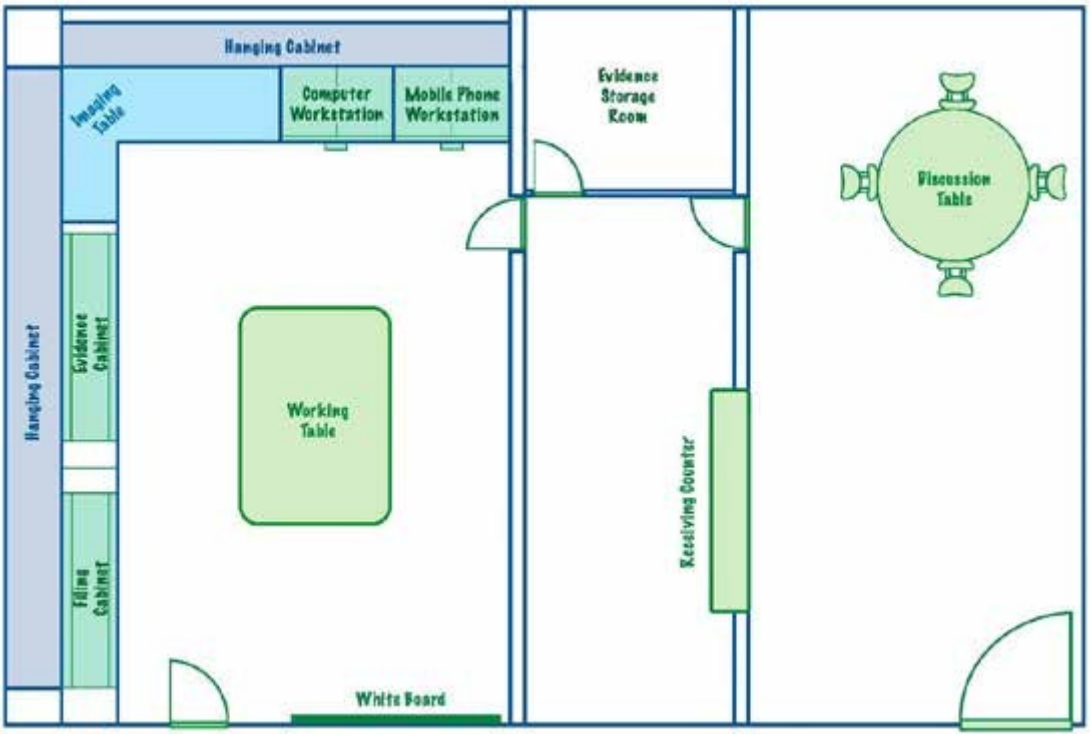


اگر آزمایشگاه به سرور نیاز داشته باشد می بایست درون آزمایشگاه و در صورت امکان خارج از آن اتاق نگهداری شود.

یک محیط متمایز برای عکسبرداری و پردازش نیاز است که می بایست از محل کار آزمایش کننده جدا باشد و در صورت امکان نزدیک به اتاق اسناد باشد تا برخورد های تصادفی را تا حد امکان کاهش دهد

آزمایشگاه ممکن است نیاز به داشتن مکانی برای انجام جلسات و محلی برای اتاق مدیر داشته باشد.

بعلاوه موارد بالا، محل مختص به انبار تجهیزات غیر سندی از قبیل کپی کننده های ویدئو ها، تجهیزات تولید ویدئو، پرینتر، اسکنر، پرونده ها، کیسه های دارایی، برچسب ها، لیبل های اسناد، انبار ویدئوها، تجهیزات دفتری و خصوصی کارمندان از مواردی هستند که هنگام انتخاب محل مناسب برای آزمایشگاه به آن باید توجه کرد.



۳.۲.۴- امکانات

زمانی که محل ها انتخاب شدند و ویژگی های امنیتی نصب شدند، مدیر آزمایشگاه نیاز به فکر کردن در این مورد دارد که امکانات باید در آزمایشگاه نصب شوند.

جدول ۳- امکانات مرسوم نصب شده در یک آزمایشگاه

۱	**بخش پذیرش** بخش ای برای ارائه و جمع آوری شواهد الکترونیک. بهتر است این بخش از آزمایشگاه ها با یک درب جدا شود. این کار برای پیش گیری از دسترسی غیر مجاز به آزمایشگاه ها است.
۲	**اتاق ذخیره شواهد** این اتاق برای ذخیره شواهد الکترونیک است. در بعضی آزمایشگاه ها، این اتاق همچنین برای نگه داشتن سرور استفاده می شود. دسترسی به این اتاق باید تنها محدود به بعضی کارکنان آزمایشگاه باشد. از سویی، اگر تنها یک تعداد بخش وجود دارند، در این صورت یک راه حل به صرفه داشتن یک بخش ایمن یا کابین ضد آتش برای ذخیره تمام بخش های الکترونیک است به جای داشتن یک اتاق ذخیره اختصاصی.
۳	**بخش پردازش شواهد** یک بخش طراحی شده برای جدا کردن، سر هم کردن، عنوان گذاری و تصویربرداری شواهد الکترونیک. این بخش باید ازمحل کاری بررسی کننده جدا شود و باید نزدیک اتاق ذخیره شواهد باشد تا میزان کار دستی کاهش یابد.
۴	**آزمایشگاه** بسته به انواع موارد دریافت شده، یک آزمایشگاه می تواند دارای چندین آزمایشگاه برای جدا سازی کار بر اساس انواع شواهد باشد. مثال ها در این زمینه عبارتند از یک آزمایشگاه جرم شناسی کامپیوتری، آزمایشگاه تلفن همراه، آزمایشگاه صوتی یا ویدیویی.
۵	**فضای شخصی** در بعضی آزمایشگاه ها، کارکنان باید میز خودشان را داشته باشند تا کارهای مدیریتی را انجام دهند، گزارش ها را بنویسند و اسلایدها را ایجاد کنند. آزمایشگاه ها تنها برای کار تحلیلی به کار برده می شوند، در حالی که این فضای شخصی توسط کارکنان برای کارهای ضروری به کار برده می شود.
۶	**فضای تبادل دیدگاه ها** یک فضای تبادل دیدگاه ها محلی است که بازرسان می توانند در مورد یک حالت بحث کنند و محلی است که مدیر آزمایشگاه می تواند یک جلسه تبادل نظر در مورد یک موضوع برگزار کند. این اتاق می تواند یک فضایباز یا بسته باشد. بهتر است این اتاق دارای یک صفحه نمایش باشد و یک وایت برد داشته باشد تا کار ارائه مطالب راحت تر انجام شود.

۷	**دسترسی به اینترنت مستقل و غیر فیلتر شده** آزمایشگاه ها عموما دارای شبکه مجزای خودشان از شبکه سازمان هستند. این کار برای پیش گیری از بد افزار و ویروس ها است تا اینکه وارد بقیه شبکه نشوند. به علاوه، آزمایشگاه باید دارای دسترسی به اینترنت غیر محدود و بدون فیلتر داشته باشد. بعضی موارد نیازمند این هستند تا بازرسان به وب سایت ها دسترسی داشته باشند که در نتیجه آنها نیازمند اینترنتی هستند که اجازه این کار را می دهد. این شبکه باید دارای ویژگی های امنیتی باشد و ورود به آن تشخیص داده شود و سیستم ردیابی داشته باشد که به صورت دوره ای بررسی می شود.

۳.۲.۵- بازدیدکننده ها

دسترسی بازدید کننده به آزمایشگاه باید محدود باشد تا از درز اطلاعات پیش گیری شود یا هیچ گونه آسیبی به شواهد الکترونیک وارد نیاید. بازدیدکنندگان می توانند شامل این موارد بشوند: کارکنان نگهداری، کارکنان دیگر نهادها، مشاوران یا افراد ارائه کننده شواهد الکترونیک.

جدول ۴- چک لیست برای بازدیدکنندگان

۱	**ثبت** بازدیدکنندگان باید با استفاده از یک فرم یا از طریق سیستم آنلاین قبل از ورود آزمایشگاه ثبت نام شوند. برای گروه بزرگی از بازدیدکنندگان، کارکنان آزمایشگاه همراهی کننده باید روندهای ثبت مناسب را سازمان دهی کنند و به نهاد اطلاع داده شود و اندازه گروه و هدف بازدید بیان شود.
۲	**شناسه عبور ID** یک شناسه عبور ID می تواند برای بازدیدکننده صادر شود مخصوصا برای بازدیدهای طولانی. این شناسه

	باید به وضوح بازدید کننده را از کارکنان آزمایشگاه متمایز کند.
۳	**اسکورت** بازدیدکنندگان باید با کارکنان آزمایشگاه در تمام زمان حضور همراه باشند که در محل های آزمایشگاه هستند.
۴	**رویه بازدید کننده** امضاهای واضح یا یک دیاگرام در رویه بازدید کننده باید در بخش مرسوم آزمایشگاه نمایش داده شوند تا بازدید کنندگان آنها را بخوانند. رویه هایی همانند عکس برداری، خوردن و نوشیدن، لمس تجهیزات جرم شناسی و شواهد الکترونیک و غیره باید برای بازدید کنندگان به وضوح توضیح داده شوند. دستورالعمل ها باید ساده باشند و به آسانی برای افراد غیر انگلیسی قابل خواندن باشند.
۵	**بررسی پیش گیری از قاچاق** علایم واضح باید نشان دهند که تصاویر غیر قانونی و نا مناسب تجزیه و تحلیل و در آزمایشگاه دیده می شوند.

۳.۳- کارکنان

بسته به اندازه آزمایشگاه و تعداد کارکنان مورد نیاز، عملکردهای متفاوتی که مورد نیاز هستند باید مد نظر قرار گیرند. نقش ها و مسئولیت های کارکنان باید مستند شوند. توصیف جزییات کار باید آماده شود تا اینکه هر عضو تیم درک واضحی از کار خودش داشته باشد. تا حد ممکن، ساختار یک آزمایشگاه باید اجازه دهد تا کارکنان کار خودشان را در سازمان به پیش ببرند.

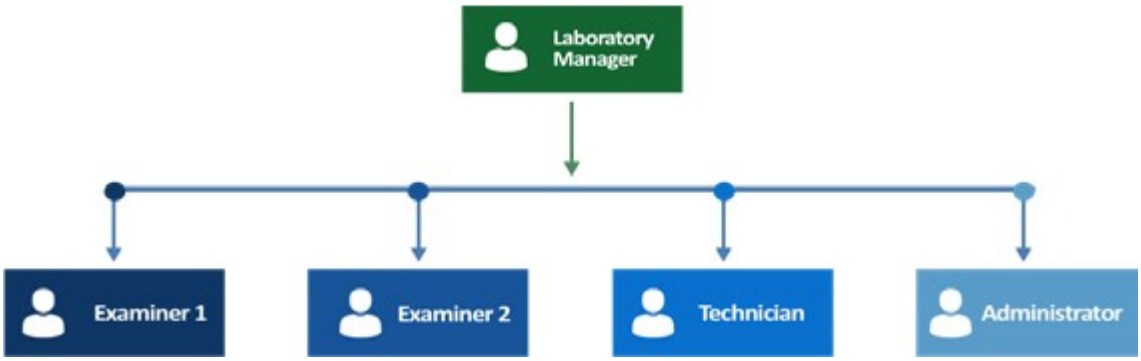
تجربه نشان داده است که کارکنان بسیار متبحر بیشتر وقت خود را صرف انجام کارهای اولیه زیر سطح تخصصشان می کنند. یک پروفایل کاری و یک توضیح واضح از کار در مرحله اولیه توسعه آزمایشگاه راهنمایی خواهد بود برای برنامه ریزی سازمان و پیش بینی بودجه.

۳.۳.۱- استخدام

کارکنان به کار گرفته شده توسط سازمان برای کار جرمیابی دیجیتال اغلب وابسته به نوع حالت جرمیابی دیجیتال و میزان کلی شواهد الکترونیک ارائه شده به آزمایشگاه هستند. این کارکنان ممکن است سطوح تحصیلی متفاوتی داشته باشند اما باید پایه قوی داشته باشند و علاقه زیادی به محاسبات و پیشرفت های جدید در زمینه تکنولوژی داشته باشند.

یک آزمایشگاه عموما در بر گیرنده دست کم یک مدیر آزمایشگاه و دو بررسی کننده می باشد. بررسی کننده در آزمایشگاه کار می کند، شواهد الکترونیک را بررسی می کند و گاهی اوقات ممکن است نیاز باشد که به سایت برود تا شواهد را بررسی کند. اگر افزایشی در حالت ها مشاهده شود و تجهیزات جرم شناسی بیشتری به دست آیند، اغلب برای آزمایشگاه بهتر است تا یک تکنسین را به کار گیرد. یک مدیر ممکن است همچنین در آزمایشگاه به کار گرفته شود تا چند وظیفه مدیریتی را انجام دهد همانند مدیریت اسناد متفاوت، آموزش، بازدیدها و گفت و گو.

یک چارت سازمانی پیشنهادی در سطح حداقل به صورت زیر است:



۳.۳.۲- امور امنیتی

قبل از اینکه کارکنان آزمایشگاه به کار گرفته شوند، پیشنهاد می شود که داوطلبان مورد بررسی اولیه قرار گیرند یا بررسی امنیتی انجام شود. حداقل، آزمایشگاه یا بخش منابع انسانی باید مطمئن شوند که یک داوطلب دارای هیچ سابقه جنایی نیست و مسئولان از لحاظ امور امنیتی او را تایید کرده اند. اگر چه این کارها همیشه ایده آل نخواهند بود، اما این کارها دست کم شواهدی را فراهم می آورند در مورد موارد جنایی جدی در گذشته. عموما مدیر بخش منابع انسانی یا آزمایشگاه دسترسی به سوابق فردی داوطلبان دارد قبل از اینکه مصاحبه انجام شود.

۳.۳.۳- توصیف کار

تمام کارکنان باید توصیف واضحی از کار داشته باشند زمانی که آنها توسط آزمایشگاه به کار گرفته می شوند. نقش ها و مسئولیت های هر فرد در آزمایشگاه باید در توصیف کاری توضیح داده شود. دست کم، نقش ها و مسئولیت های هر فرد در آزمایشگاه باید به صورت زیر توصیف شود:

مدیر آزمایشگاه

مدیر آزمایشگاه باید دارای دانش فنی و درکی قوی از نیازهای قانونی برای شواهد الکترونیک و رویه ها و روندها باشد. یک مدیر آزمایشگاه باید درکی از اصول توصیف شده در این راهنما داشته باشد. او باید کنترلی بر ساختار اصلی داشته باشد و دیدگاهی در مورد خرید سخت افزار و نرم افزار یا رویه ها و عملکردهای آزمایشگاه داشته باشد.

او مسئول استخدام، آموزش، مشاوره و راهنمایی هر فرد استخدام شده در این واحد است. مدیر آزمایشگاه همچنین مسئول تصمیم گیری مرتبط با افراد است از جمله پذیرش یا رد یک حالت و نیز اولویت بندی آنها.

بررسی کننده

بررسی کننده باید دارای دانش فنی مرتبط و توانایی کافی باشد. عموما او باید دارای آموزشی در زمینه استفاده از نرم افزار جرمیابی دیجیتال باشد. زمانی که او به کار گرفته می شود، لازم است آموزش خاصی را بگذراند تا حداقل مهارت ها را به دست آورد. بررسی کننده باید دارای دانش و آگاهی کافی در مورد عناصر هر جرم باشد تا اینکه این حقایق را در زمانی درک کند که انواع متفاوت جرم ها را بررسی می کند. این نقش ها نیازمند یک تحلیل و بررسی هستند. بررسی کننده باید همچنین قادر باشد یافته های خود را به طریقی قابل درک ارائه دهد و در نتیجه مهارت های ارتباطی شفاهی و کتبی بسیار ضروری هستند.

تکنسین

تکنسین پردازش شواهد را انجام می دهد همانند ثبت، به دست آوردن و ذخیره کردن. بسته به اندازه آزمایشگاه، چند تکنسین ممکن است مورد نیاز باشند. تکنسین باید مهارت های فنی قوی در زمینه محاسبات داشته باشد و دانش فنی در زمینه روش های متفاوت به دست آوردن داده های دیجیتال جرم شناسی داشته باشد. یک مهارت مهم توجه به جزییات و توانایی مستند کردن تمام کارهای انجام شده در مورد هر کدام از شواهد است.

تکنسین همچنین مسئول نگهداری تجهیزات جرم شناسی است. او نیازمند اطمینان از این مورد است که سخت افزار به روز شده است و نرم افزارها هنگام به روز رسانی نصب شده اند.

تکنسین همچنین مسئول مدیریت شواهد در اتاق ذخیره شواهد است. او نیازمند نگهداری سوابق مرتبط است و نیز بررسی شواهد در اتاق ذخیره.

مدیر

یک آزمایشگاه همچنین ممکن است یک مدیر را برای انجام کارهای مدیریتی آزمایشگاه استخدام کند. او مسئول مدیریت اسناد آزمایشگاه است. او همچنین می تواند به عنوان یک افسر رابط با بخش های داخلی و بیرونی کار کند. مدیر همچنین می تواند مسئول مدیریت خرید تجهیزات برای آزمایشگاه باشد.

۳.۳.۴- توسعه کارکنان

مدیریت آزمایشگاه باید مطمئن شود که کارکنان در حال کار در جرمیابی دیجیتال کاملا مجهز هستند و دارای مهارت های مناسب هستند.

دلیل این امر این است که داده های موجود در شواهد الکترونیک می توانند به سادگی تغییر کنند یا آسیب ببینند که در نتیجه کارکنان باید بدانند که چگونه داده ها را مدیریت کنند بدون اینکه به آنها آسیب برسد. دلیل دیگر این است که پیچیدگی جرم امروزه می تواند باعث مشکل شدن کشف داده های صحیح شود. در نتیجه کارکنان آزمایشگاه باید بدانند که چگونه آنها را بیابند و استخراج کنند.

الف. آموزش

زمانی که کارکنان استخدام شدند، بسیار مهم است که توانایی های خود را ارتقا دهند و برنامه پیوسته ای برای پشتیبانی از این امر داشته باشند. این کار می تواند شامل ایجاد انگیزه برای محل کار جدید آنها شود. توصیف کار باید به وضوح نقش و مسئولیت آنها را شامل شود و به مدیر گزارش شود. مدیر باید نیازهای آموزشی کارکنان را مشخص کرده و برنامه ریزی کند و مقدمات مناسب را فراهم آورد. آزمایشگاه ممکن است کارکنان را برای دوره های آموزشی بفرستد یا جلسه ای را ترتیب دهد برای کارکنان تا آموزش های لازم را طی کنند که بر طبق یک جدول زمانی برنامه ریزی شده خواهد بود. برای مثال، بررسی کننده ها نیازمند آموزش بیرونی مناسب هستند تا اینکه بتوانند از ابزارهای جرم شناسی استفاده کنند و به درستی شواهد قابل اعتمادی را در دادگاه ارائه دهند. یک لیست مهارت های پیشنهادی می تواند برای کمک به تعیین نیازهای آموزشی به کار برده شود که در پیوست ارائه شده است.

ب. نگهداری مهارت

پیشرفت ها در فناوری نیازمند این است که کارکنان دانش و مهارت خود را دائم به روز کنند. علاوه بر برنامه آموزشی، آزمایشگاه باید یک برنامه نگهداری مهارت را به کار گیرد که به عنوان بخشی از نیاز کارکنان است که باید مهارت خود را

ارتقا دهند و در جلسات فنی مرتبط حضور یابند و تحلیل شواهد الکترونیک دائم انجام شود و در برنامه های نگهداری مشارکت کنند. این برنامه برای اطمینان از این مورد لازم است که مهارت های بررسی کنندگان به روز هستند و بر اساس فناوری جدید هستند و آنها همیشه قادر به اجرای عملکردهای جرمیابی دیجیتال هستند.

ج. پورتفیلو توسعه فردی (PDP)

برای مدیریت موثر توسعه کارکنان، آزمایشگاه ممکن است برای هر عضو یک پورتفیلو توسعه فردی (PDP) را به کار گیرد. این پورتفیلو باید شامل یک برنامه آموزشی، گواهی آموزشی و رکورد شود. مدیران ممکن است از PDP ها برای تعیین اهداف برای افراد استفاده کنند و به بررسی عملکرد آنها از زمانی به زمان دیگر اقدام کنند.

د. فعالیت های تحقیق و توسعه

جدای از آموزش و نگهداری، مدیریت باید همچنین زمانی را به کارکنان اختصاص دهد برای انجام فعالیت های تحقیق و توسعه. کارکنان باید ابزارهای جدید را ارزیابی کنند و تصمیم بگیرند که کجا آزمایشگاه نیاز دارد تا از آنها استفاده کند.

و. نگهداری کارکنان

آزمایشگاه باید دقت کند که برنامه آموزشی گسترده باعث می شود که کارکنان ارزش بسیاری برای سازمان به همراه آورند و با این حال میزان گردش زیاد در آزمایشگاه حاصل می آید. زمان و پول زیادی صرف آموزش کارکنان می شود و بسیار ضروری است که آنها نگه داشته شوند مخصوصا زمانی که آنها تجربه بیشتری به دست می آورند. برای کاهش ریسک از دست دادن کارکنان، سازمان باید برنامه خوبی برای نگهداری کارکنان داشته باشد. داشتن برنامه های قوی برای هر کدام از کارکنان برای هر کدام از کارکنان اهدافی فردی را فراهم می آورد و درک بهتری از مسیر حرفه ای خواهند داشت و اینکه چه فرصت هایی در سازمان خواهند داشت. عواملی که باعث وفاداری کارکنان می شوند همیشه محدود به حقوق نیستند و اغلب یک محیط کاری خوب و سالم عامل مهمی است.

۳.۳.۵- مشاوره

برای کارکنان تازه استخدام شده توصیه می شود یک جلسه مشاوره در مدت مراحل اولیه شروع به کار آنها برگزار شود. مشاوره روندی است که بر اساس آن کارکنان با تجربه کار افراد تازه کار را بررسی می کنند. نقش مشاور راهنمایی و پشتیبانی و نیز اشتراک اطلاعات در یک محیط دوستانه است. نیاز به جلسات مشاوره برای کارکنان تازه زمانی برطرف می شود که آنها نقش های جدید خود را یاد بگیرند.

مشاوره معمولا به صورت تمرین است و شامل ارزیابی عملکرد در رابطه با مراحل اولیه می شود.

۳.۳.۶- سلامتی و ایمنی

مدیر آزمایشگاه مسئول اطمینان از سلامتی و ایمنی تمام کارکنان و بازدیدکنندگان آزمایشگاه است. یک ارزیابی ریسک باید با بررسی شرایط کنونی در مواردی انجام شود که می تواند تاثیر گذار بر سلامت یا ایمنی باشد. هر گونه موارد مخاطره آمیز باید در نظر گرفته شوند. اغلب کارکنان یا تیم تخصصی در یک سازمان باید به موضوعات تخصصی بپردازند اما وقتی آنها نیستند این مسئولیت مدیر آزمایشگاه است که آگاهی در مورد موارد قانونی و نیازهای ایمنی داشته باشد. ارزیابی هایی باید انجام شوند تا این اطمینان به وجود آید که بازدیدکنندگان و و کارکنان از دیگر بخش ها با موارد غیر قانونی مواجه نیستند. این احتمال با پیروی از پیشنهادات فراهم آمده قبلی با توجه به ساختار آزمایشگاه کاهش خواهد یافت.

چند ویژگی ایمنی مرسوم در یک آزمایشگاه معمولا یافت می شوند که به صورت زیر است:

* تشک های ضد استاتیک و مچ بند – برای کاهش ریسک آسیب استاتیک به تجهیزات.
* کد لباس – لباس مناسبی که پا را کاملا می پوشاند باید پوشیده شود و موی بلند باید بسته شود و جواهر آلات و لباس های گشاد باید ایمن شوند. در صورت نیاز، دستکش های جراحی باید پوشیده شوند تا از تماس با مواد آلوده پیش گیری شود.
* آسانسور – این اطمینان به وجود می آید که کارکنان آگاه از راه درست بلند کردن آیتم های سنگین هستند تا از آسیب پیش گیری شود.
* تشک های لاستیکی – برای کاهش ریسک شوک الکتریکی.
* کاهش دهنده های مدار – برای کاهش ریسک شوک الکتریکی یا آسیب به تجهیزات و شواهد.

۳.۴- تجهیزات

یک آزمایشگاه باید دسترسی به تجهیزات جرم شناسی داشته باشد که نیاز هستند تا نتایج جرم شناسی مناسبی به دست آیند. تجهیزات می توانند از نوع سخت افزاری باشند و یا نرم افزاری و با منبع باز باشند یا ابزارهای تجاری باشند. قبل از استفاده از تجهیزات، آنها باید تست شوند تا این اطمینان به وجود آید که قادر به تولید نتایج درست هستند. تجهیزات اصلی توصیه شده برای یک آزمایشگاه در **پیوست ب** ارائه شده اند.

۳.۴.۱- نرم افزار

زمان خرید یک نرم افزار، آزمایشگاه باید قیمت، هزینه های سالانه، هزینه های نگهداری و آموزش را در نظر بگیرد. هزینه مجوزها می توانند بسیار مهم باشند، در نتیجه آزمایشگاه باید بررسی گسترده ای انجام دهد و آن را در برنامه ریزی بودجه برای سال های آینده مورد توجه قرار دهد. باید این اطمینان به وجود آید که نرم افزار کاملا مطابق با نیازهای آزمایشگاهاست.

بعضی از نرم افزارهای با منبع باز ویژگی های گسترده ای را ارائه می دهند و می توانند توسط بررسی کننده ها به کار برده شوند اما این نرم افزار ممکن است شامل پشتیبانی و فرصت های آموزشی نشود.

بعضی استانداردها نیازمند بررسی ابزار دوگانه هستند و لازم است نرم افزار بیشتری خریداری شود تا اینکه مقایسه و بررسی نتایج اجرا شود.

آزمایشگاه باید همچنین یک سیستم مدیریت حالت را برای عملکرد خود مد نظر قرار دهد. این سیستم شامل یک پایگاه داده در مورد نام بررسی کننده و نتایج جرم شناسی می شود. حداقل موارد ورودی به یک سیستم به صورت زیر هستند:

* تاریخ، زمان و فرد ارسال کننده و دریافت کننده در آزمایشگاه.
* شماره مرجع خاص.
* شماره مرجع خاص یک حالت.
* نام درخواست کننده و جزییات شماره تماس.
* نوع جرم و عمل مرتبط.
* نام کارکنان آزمایشگاه که با بقیه در ارتباط هستند.
* توصیف حالت مورد درخواست.
* عوامل زمانی – همانند تاریخ عرضه و تاریخ مورد انتظار دادگاه.

* روند تحلیل – تصویر برداری، بررسی، استخراج، محاسبه و غیره.
* تاریخ دقیق و زمان تحلیل انجام شده و نیز نام بررسی کننده.
* جزییات کیفی توسط مدیران و کارکنان.
* نتایج تحلیل.
* ثبت ارتباط با درخواست کننده.

تمام این اطلاعات بسیار مهم هستند تا اینکه تداوم و قابلیت اطمینان کارها و شواهد را نشان دهند. آزمایشگاه می تواند این سیستم را به صورت درونی ایجاد کند، راه حل مناسبی را خریداری کند یا یک برنامه نویس را به کار گیرد تا سیستم را توسعه دهد.

۳.۴.۲- سخت افزار

سخت افزار باید همچنین به صورت دوره ای نگهداری شود که برای این منظور توصیه می شود یک برنامه مدون و یک لیست تجهیزات داشته باشد.

یک عنصر مهم برای آزمایشگاه که باید مد نظر قرار دهد جدای از ذخیره و پشتیبانی داده های کاربردی ذخیره شواهد الکترونیک است. سه نوع داده که آزمایشگاه ممکن است برای بررسی نیاز داشته باشد عبارتند از شواهد اصلی، کپی های جنایی و داده های ایجاد شده در مدت تحلیل. برای آزمایشگاه بسیار ضروری است که یک سرور بزرگ و نیرومند به علت حجم بالای داده ها و شواهد الکترونیک داشته باشد. باید به این مورد توجه شود که چگونه آن ذخیره می شود، آرشیو می شود و پشتیبانی از آن گرفته می شود. یک پشتیبانی و آرشیو مناسب باید اجرا شود.

لیستی از تجهیزات اصلی آزمایشگاه در **پیوست ب** ارائه شده است.

۳.۴.۳- ابزارها و لوازم

ابزارها و لوازمی همانند کابل ها، درایورها و سیم های برق همانند سخت افزارها و نرم افزارها در یک آزمایشگاه مهم هستند. بعضی از کارهای جرمیابی دیجیتال نیازمند ابزارهای الکترونیک هستند تا اینکه جدا شده و سر هم شوند، که در نتیجه آزمایشگاه نیازمند دسترسی به ابزارها و لوازم با کیفیت است. در زیر لیستی از آیتم های ممکن که یک آزمایشگاه ممکن است برای انجام کارهای روزمره نیاز داشته باشد ارائه شده است:

* سیم برق
* رابط ها و آداپتورها
* پیچ گوشتی

* جعبه ابزار
* دوربین، ظبط ویدیویی
* نوارهای مغناطیسی
* ابزارهای ارتباطی
* جعبه ذخیره یا محفظه برای حمل تجهیزات
* چراغ قوه
* ذره بین
* جعبه شواهد
* استیکرها
* مارکرهای دائمی
* کیسه فارادی

۴- مدیریت روال جرمیابی دیجیتال

آزمایشگاه باید یک رویه مدیریتی را قبل از شروع دریافت موضوعات به کار گیرد. عموما هفت مرحله در مدیریت یک موضوع وجود دارند که در شکل زیر نشان داده شده است و در بخش های بعدی هم بیشتر توضیح داده شده است. قبل از اجرای یک موضوع، آزمایشگاه باید اطمینان یابد که مطابق با قوانین مرتبط است. مدیر یا بررسی کننده باید اطمینان یابد که اجازه قانونی برای پردازش شواهد وجود دارد. هدف از اجرای کار جرمیابی دیجیتال استفاده از شواهد برای اثبات یا عدم اثبات حقایق مورد مناقشه است، با این حال شواهد الکترونیک باید در انطباق با موارد قانونی به دست آیند. در انتهای کار DF، باید این اطمینان حاصل آید که شواهد الکترونیک قابل پذیرش هستند و گزارش جنایی در دادگاه قابل پذیرش است.

روال مدیریت موضوع

دریافت درخواست > ثبت موضوع > نمایش ثبت > نمایش عکس > انجام تحلیل > بازگشت > بستن موضوع

۴.۱- دریافت یک درخواست

کار آزمایشگاه با دریافت یک درخواست رسمی از یک درخواست کننده شروع می شود. این درخواست رسمی می تواند به صورت یک نامه باشد یا ای میل یا فاکس. اطلاعات فراهم آمده در درخواست رسمی باید شامل توصیفی از جرم، عمل مرتبط، جزییات شواهد الکترونیک، هدف موضوع و احتمالا اخطار بشود.

مدیر آزمایشگاه یا کارکنان مرتبط سپس مروری بر درخواست خواهند داشت و تعیین می کنند که آیا موضوع بر اساس معیارهای زیر قابل انجام است یا خیر:

الف. موضوع در حیطه جرم شناسی دیجیتال قابل بررسی است، برای مثال شواهد الکترونیک هستند و نه چیز دیگری همانند DNA یا اثر انگشت

ب. روش ها و ابزارهایی که موجود هستند.

ج. کارکنانی که برای اجرای این موضوع وجود دارند.

د. نیازهای قانونی مد نظر قرار داده می شوند.

آزمایشگاه سپس به درخواست پذیرش یا عدم پذیرش پاسخ می دهد. اگر تصمیم به پذیرش باشد، آزمایشگاه تاریخی را برای ارائه شواهد الکترونیک از درخواست کننده فراهم خواهد آورد.

۴.۲- ثبت یک موضوع

زمانی که آزمایشگاه تصمیم می گیرد که یک موضوع را بپذیرد، درخواست کننده با شواهد الکترونیک به آزمایشگاه خواهد آمد. آزمایشگاه یک تعداد زمینه های خاص را برای آن موضوع ایجاد می کند و یک فرم ثبت موضوع را پر می کند. یک نمونه از فرم ثبت موضوع در **پیوست ج** ارائه شده است.

برای بررسی موثر شواهد الکترونیک، بررسی کننده ها نیاز دارند تا یک درخواست واضح و خاص از سوی درخواست کننده ارائه شود. به علت میزان بالا و انواع متفاوت داده ها در یک ابزار، همانند اسناد، ویدیوها، ارتباطات، داده های بررسی سلامت، محل ها و غیره در نتیجه یک بررسی کننده نمی تواند داده ها را بدون درخواست واضح و خاص بررسی کند.

بر اساس این اطلاعات بررسی کننده می تواند روش ها و ابزارهایی را برنامه ریز کند که می توانند برای پردازش شواهد به کار برده شوند.

هر دوی طرفین، درخواست کننده و کارکنان آزمایشگاه، باید فرم را امضا کنند. این کار حالا باید به صورت رسمی شروع شود. سپس آزمایشگاه یک پوشه در یک واسط ذخیره ایجاد خواهد کرد که برای ذخیره تمام داده های منطقی مرتبط با موضوع به کار برده می شود.

۴.۳- ثبت شواهد (شواهد الکترونیک)

زمانی که شواهد الکترونیک (شاهدها) دریافت می شوند، بسیار مهم است که شاهد مهر و موم شود قبل از اینکه محافظت بتواند به آزمایشگاه منتقل شود. برای حذف هر گونه شک معقول در مورد اتحاد شواهد، هر دوی درخواست کننده و بررسی کننده باید قادر باشند اثبات کنند که هیچ کس دیگری دسترسی به شواهد در مدت روند انتقال از یکی از طرفین به دیگری نداشته است. این مورد برای بعضی سازمان ها جدید و هزینه بر است ولی برای آزمایشگاه در هر صورت آگاهی سریع را فراهم می آورد و یک برنامه زمانی را برای شروع این روال برای سازمان ها فراهم می آورد.

هر بخش از شواهد الکترونیک که ارائه می شوند باید ثبت شوند و یک عنوان به آنها اختصاص داده شود که شامل جزییات آنها در فرم ثبت نام می شود. یک نمونه از فرم ثبت شاهد در **پیوست د** ارائه شده است.

این ثبت شامل هر زیر آیتم شاهد می شود، همانند سیم کارت ها و کارت های حافظه. عناوین باید قادر باشند هر زیر آیتم را تا آیتم اصلی آن ردیابی کنند. برای مثال، اگر یک موبایل دارای عنوان ۲۰۱۹۰۱۰۵(۲)-MP۰۱ باشد، در این صورت سیم کارت ممکن است دارای عنوان ۲۰۱۹۰۱۰۵(۲)-MP۰۱-SIM۰۱ باشد.

لازم به ذکر است که هر گونه نقص در شاهد باید در فرم ثبت شاهد مستند شود. این کار برای محافظت از آزمایشگاه در برابر هر گونه اظهار نظر منفی در آینده است. هر فرم از اسناد کپی مرتبط با شاهد باید در فولدر مرتبط با موضوع بارگذاری شود.

حالا زنجیره شواهد شروع شده است و این فرم باید توسط کارکنان دریافت کننده شاهد پر شود. اگر چه شاهد مورد استفاده نیست اما باید در یک اتاق ذخیره شاهد ذخیره شود به صورتی که در بخش ۳.۲.۴ توضیح داده شده است.

۴.۴- عکس برداری از شواهد

یک عکس شاهد به دلایل زیر گرفته می شود: برای ثبت حالت شاهد و مشخص کردن موثر شاهد در آینده. عکس برداری از دیدگاه کلی شاهد و نیز دیدگاه نزدیک لازم است. اگر صفحه فعال باشد، عکس برداری از صفحه نمایش نیز باید انجام شود. این تصاویر سپس باید در فولدر مرتبط با موضوع بارگذاری شوند. پیشنهاد می شود از شاهد قبل از بازگشت آن به درخواست کننده برای ارجاع در آینده عکس برداری شود.

۴.۵- انجام تجزیه و تحلیل

تجزیه و تحلیل باید مطابق با مدل آنالیز DFL انجام شود. برای جزئیات در مورد نحوه انجام تجزیه و تحلیل به بخش ۵ مراجعه کنید. در طی این فرایند، بررسی کنندگان باید ارتباط با درخواست کننده را حفظ کرده و هرگونه انحراف یا محدودیتی را که ممکن است در طول امتحان ایجاد شود را اطلاع دهند. برخی از بررسی کنندگان سالها دانش در زمینه جرمیابی دیجیتال دارند و به همین دلیل در صورت وجود ارتباطات مؤثر بین بررسی کنندگان و درخواست کننده می توانند داده های صحیح را به شما اارائه دهند.

۴.۶- بازگرداندن شواهد

پس از اتمام تجزیه و تحلیل، DFL برای تهیه مدارک با درخواست کننده تماس می گیرد. روش معمول در DFL بازگشت این شاهد به همراه گزارش جرمیابی به درخواست کننده است تا در زمان رفت و آمد صرفه جویی شود. قبل از بازگشت شاهد، DFL باید آن را مهر و موم کند. مهر و موم باید دارای مشخصات اولیه کارکنان، عنوان شاهد و تاریخ و زمان پلمپ آن باشد. نمونه ای از مهر و موم شاهد در پیوست E: نمونه ای از مهر و موم شاهد موجود است.

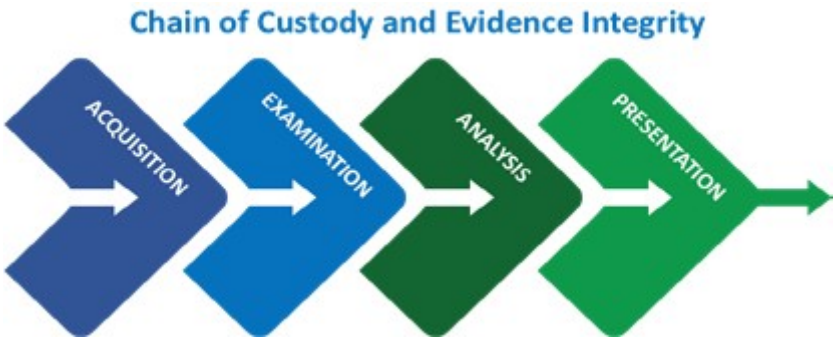
۴.۷- بسته شدن پرونده

این روند کامل شده و DFL می تواند فایل را ببندد. برای بستن فایل، هر دو طرف باید توافق کنند که کار کامل است و گزارش به درخواست کننده تحویل داده شده است. این کار را با امضای فرم می توانید انجام دهید. نمونه ای در **پیوست د** وجود دارد: نمونه فرم ثبت نام شاهد، که در آن با امضای بخش بازگشت به شاهد، هر دو طرف موافق هستند که هم اکنون کار کامل است.

پس از تکمیل فایل، راه پیش رو شامل این مورد می شود که بررسی کننده در دادگاه حاضر شود تا در صورت لزوم شهادت کارشناسی را در مورد نتایج جرمیابی فایل ارائه دهد. درخواست کننده در صورت نیاز در دادگاه به بررسی کننده اطلاع می دهد.

۵- اصول تجزیه و تحلیل آزمایشگاهی

در این فصل روش انجام تجزیه و تحلیل بر روی شواهد الکترونیکی در DFL ارائه شده است. به طور کلی، یک مدل فرایند بر پایه زمان ارائه شده است تا یک مرور کلی بهتر از فرآیندهای اصلی ارائه شود. به طور معمول چهار مرحله در تجزیه و تحلیل شواهد الکترونیکی در DFL وجود دارند: اکتساب، بررسی، تجزیه و تحلیل و ارائه. در طی این فرایند، زنجیره بررسی مدارک و شواهد همیشه باید در صورت تغییر افراد به روز شود و هماهنگی آن باید در هر زمان تأمین شود. مراحل آزمایش و تجزیه و تحلیل ممکن است تکرار شود تا زمانی که کار بررسی فایل آسان شود.
معمولاً درک می شود که انجام کار جرمیابی دیجیتال در DFL به این چهار مرحله نیاز دارد، با این وجود همه موارد به همه این مراحل نیاز ندارند. در موارد خاص، مرحله اکتساب را می توان کنار گذاشت و به صورت مستقیم سه مرحله بعدی را دنبال کرد. نمونه ای از چنین مواردی وقتی وجود دارد که مجموعه های بزرگی از داده ها وجود دارند، که به کار گیری مرحله اکتساب در هر مورد ممکن است عملی نباشد.
شکل زیر مدل آنالیز آزمایشگاهی را نشان می دهد:



شکل ۵. مدل تجزیه و تحلیل آزمایشگاهی جرمیابی دیجیتال

بخش بعدی در این سند به تفصیل هر مرحله شامل در مدل تحلیل DFL را توصیف می کند.

۵.۱- اکتساب

۵.۱.۱- بررسی اجمالی

اکتساب یا همانطور که مشهورتر است، جمع آوری داده ها، فرآیند ایجاد نسخه جرمیابی از شواهد الکترونیکی (شاهد) مانند هارد دیسک، فلش یا سرور در قالب یک فایل یا فایل های تصویری است. سپس از فایل تصویری یا فایل ها برای مرحله بعدی روند تجزیه و تحلیل شواهد استفاده می شود. اکتساب به منظور حفظ هماهنگی شواهد الکترونیکی انجام شده است. این کار برای تولید یک نسخه یکسان از داده ها بدون تغییر محتوای مدارک الکترونیکی به هر طریقی است.

شواهد الکترونیکی باید به روشی کاملاً قانونی به دست آیند. داده ها معمولاً با جمع آوری داده های ناپایدار از رایانه در حال کار هنگام جستجو به دست می آیند یا با دستیابی به یک وسیله ذخیره سازی از یک کامپیوتر یا در هر مرحله دیگر در طی تحقیقات بدست می آیند. ماهیت نامشهود داده ها و اطلاعات ذخیره شده به صورت الکترونیکی امکان دستکاری را فراهم می آورد و بیشتر مستعد تغییر نسبت به انواع سنتی شواهد خواهد بود. بنابراین داشتن یک روند تعریف شده و آزمایش شده برای اکتساب حائز اهمیت است.

پس از ایجاد یک فایل تصویری، باید ارزش ذاتی شاهد و فایل تصویر ثبت شود. از هاشینگ (ارزش گذاری) برای اثبات این موضوع استفاده می شود که فایل تصویری دقیقاً مشابه محتوای شاهد است یا خیر. بسیاری از الگوریتم های ارزش گذاری در جرمیابی دیجیتال مانند SHA-256 استفاده می شوند. بیشتر نرم افزارها و سخت افزارهای جرمیابی ویژگی ایجاد هش را ارائه می دهند.

بررسی و تجزیه و تحلیل فقط باید بر روی یک نسخه قانونی از شواهد اصلی انجام شود، مگر اینکه شرایط باعث شوند بررسی کنندگان نتوانند این کار را انجام دهند. این امر به منظور حفظ هماهنگی شواهد مهم است. نسخه جرمیابی مدارک الکترونیکی باید در سایر رسانه های ذخیره سازی ذخیره شود و هرگز بر روی خود شواهد قرار نگیرد. نسخه جرمیابی باید به طور واضح عنوان گذاری شود تا اطمینان حاصل شود که با شواهد اصلی یا نسخه های جرمیابی از موارد دیگر درآمیخته نیست. بنابراین DFL قبل از دریافت موارد باید برخی از رسانه های ذخیره سازی را آماده کند.

این سند روند انجام آزمایش و تحلیل جرمیابی دیجیتال را در دو نوع دستگاه توضیح می دهد:

(۱) رایانه (۲) دستگاه های تلفن همراه

۵.۱.۲- رایانه

اکتساب رایانه ها به شرح زیر است:

۵.۱.۲.۱- انواع اکتساب داده ها

دو سطح کسب داده وجود دارد: کسب داده های فیزیکی و دستیابی به اطلاعات منطقی. در حالی که کسب داده های فیزیکی شامل کلیه داده های خام است، یک نسخه منطقی معمولاً فقط شامل یک زیر مجموعه اختصاصی از این داده ها می شود.
اکتساب داده های فیزیکی، در کل در سطح دیسک، تمام داده های موجود در دیسک، از جمله طرح پارتیشن، منطقه پارتیشن، و منطقه بدون پارتیشن را کپی می کند. کسب داده های منطقی در سطح دیسک فقط یک منطقه دارای پارتیشن بندی منطقی را کپی می کند.
بررسی کننده معمولاً بدست آوردن داده های فیزیکی کل دیسک را انتخاب می کند زیرا شامل فایل های حذف شده و دسته های اختصاص داده نشده است. با این حال، هنگام رمزگذاری، جمع آوری داده های منطقی از داده های قفل شده به دستیابی فیزیکی از داده های رمزگذاری شده ترجیح داده می شود. در این موارد اگر نرم افزار جرمیابی از نصب تصویربرداری رمزگذاری شده پشتیبانی کند، اکتساب فیزیکی همچنان توصیه می شود.
برای ایجاد یک نسخه، ابتدا باید بررسی کننده وضعیت شاهد را انتخاب کند. اگر سیستم در حال اجرا و کار باشد، ممکن است بررسی کننده نیاز به انتخاب مستقیم (زنده) داشته باشد.
اما اگر سیستم خاموش باشد، ممکن است بررسی کننده اکتساب مرده را انتخاب کند. تفاوت این روش های اکتساب در جدول زیر توضیح داده شده است.

جدول ۶. روش انجام اکتساب - اکتساب مرده و اکتساب زنده

	اکتساب مرده	اکتساب زنده
چه چیز؟	اکتساب مرده در یک سیستم مرده اجرا می شود. یک سیستم مرده سیستمی است که در حال اجرا نیست و خاموش است. زمانی که سیستم مرده است، داده های فرار در مناطق ذخیره سازی موقت همانند حافظه ram، حافظه کش یا گفت و گوهای فعال در یک کامپیوتر دیگر موجود نخواهند بود.	اکتساب زنده در یک سیستم زنده اجرا می شود. یک سیستم زنده سیستمی است که زمانی در حال کار است که اطلاعات ممکن است تغییر کنند اگر دائم پردازش شوند. به علت ارزش بالای شواهدی که می توانند در یک سیستم زنده کشف شوند، خاموش کردن آن ممکن است باعث آسیب به داده های فرار شود همانند داده های ذخیره شده در ابر، داده های رمز گذاری شده، اتصال به شبکه و فایل نصب شده در سیستم.
چگونه؟	روند اجرای اکتساب مرده سر راست است زیرا عموما به صورت خودکار با استفاده از ابزارهای جنایی انجام می شود. در صورت امکان هارد دیسک باید ابتدا از کامپیوتر در آورده شود قبل از اتصال آن به ابزار. در بعضی موارد نت بوک ها یا ابزارهای با درایو حالت جامد نمی توانند در اکتساب مرده به کار برده شوند. دیگر روش ها برای اجرای استخراج در چنین مواردی، همانند بوت کردن سیستم با یک cd/usb زنده باید	داده ها در یک سیستم دارای سطوح متفاوت فراریت هستند. این داده ها از دست خواهند رفت اگر سیستم خاموش شود یا دوباره راه اندازی شود. هر وقت بررسی کننده داده های زنده را به دست آورد، آن حساس به جمع آوری از بیشتر داده های فرار است. سطح مرسوم فراریت، از بیشترین به کمترین فراریت به صورت زیر است: * حافظه * فایل سواپ * پردازش های شبکه * پردازش های سیستم

	در نظر گرفته شوند.	* اطلاعات سیستم فایل
چه زمانی؟	اکتساب مرده زمانی اجرا می شود که: * سیستم خاموش است * داده های حذف شده مهم تر از داده های فرار هستند.	اکتساب زنده زمانی استفاده می شود که: * سیستم به لحاظ کاری دارای اهمیت است و نمی تواند خاموش شود. * داده های فرار مهم تر از داده های حذف شده هستند.

سپس بررسی کننده باید انتخاب کند که آیا می تواند شاهد را کلون کند یا یک تصویر را ایجاد کند. کلون داده ها را بیت به بیت از یک رسانه ذخیره سازی به دیگری کپی می کند. از طرف دیگر، داده را بیت به بیت از یک رسانه ذخیره سازی در یک فایل تصویری کپی می کند. سپس این فایل می تواند در یک رسانه دیگر ذخیره شود. روش دوم معمولاً مورد استفاده قرار می گیرد زیرا متعاقباً فایل تصویری توسط بیشتر نرم افزار جرمیابی برای پردازش تجزیه و تحلیل جرمیابی خوانده می شود. کلونینگ معمولاً برای اهداف شبیه سازی استفاده می شود. قبل از انجام این کار، بررسی کننده باید اطمینان حاصل کند که این شاهد برای نوشتن مسدود شده است (چیزی نمی توان روی آن نوشت). روشی که فقط خواندن را قادر می سازد و از هرگونه نوشتن در شاهد جلوگیری می کند.

۵.۱.۲.۲- بلوک کردن نوشتن (مسدود کردن)

مسدود کننده نوشتن وسیله ای است که می تواند داده ها را از یک هارد دیسک بدون تغییر داده های دیسک بدست آورد. این دستگاه اجازه می دهد تا یک دستور خوانده شود، اما اجازه نمی دهد دستورات نوشتن بر روی هارد دیسک اجرا شود. بیشتر ابزارهای تصویربرداری دارای مسدود کننده نوشتن داخلی هستند که بررسی کننده می تواند هنگام تصویربرداری از یک هارد دیسک از آن استفاده کند. در حالی که مسدود کردن نوشتن همچنین توسط ابزارهای نرم افزاری یا تغییراتی در رجیستری ویندوز حاصل می شود، اما راه حل های سخت افزاری در DFL ها ترجیح داده می شوند.

۵.۱.۲.۳- ابزارهای تصویربرداری

تصویربرداری از یک فضای ذخیره سازی با استفاده از نرم افزار جرمیابی یا سخت افزار قابل انجام است. محصولات رایگان و تجاری نیز در دسترس هستند که می توانند در روند این کار کمک کنند. هنگام خرید این ابزار، مهمترین معیار برای جستجوی آن، سرعت انجام تصویر برداری و قابلیت اطمینان است. نرم افزار تصویربرداری می تواند شامل ویژگی هایی از این قبیل باشد:

* شناخت مناطق پنهان
* تصویربرداری از چندین دستگاه به طور همزمان
* تصویربرداری همزمان از چندین مقصد
* صف های تصویربرداری
* تأیید هش با الگوریتم های هش مرسوم
* تأیید هش در مراحل مختلف فرایند تصویربرداری

* رایج ترین قالب های تصاویر جرمیابی را پشتیبانی کند
* تولید تصاویر رمزگذاری شده و فشرده شده
* به کار گیری یک روند اکتساب بدون وقفه
* تحمل خطاهای سخت افزاری

بررسی کننده همیشه باید نسبت به احتمال وجود تکنیک های ضد جرمیابی هوشیار باشد. مناطق پنهان مانند مناطق محافظت شده از میزبان (HPA) یا روکش پیکربندی دستگاه (DCO)، که فقط از طریق دستورات ویژه ATA قابل دسترسی هستند، فقط توسط برخی راه حل های نرم افزاری تصویربرداری موجود قابل شناسایی هستند.

۵.۱.۲.۴- قالب تصویربرداری

چندین فرمت فایل متداول وجود دارند، که عبارتند از خام یا dd. این قالب ها کلیه داده ها را از رسانه اصلی در یک فایل خام ذخیره می کنند. قالب های دیگر شامل فرمت شاهد (EWF) و قالب جرمیابی پیشرفته (AFF) هستند. اینها شامل ویژگی هایی از این قبیل هستند:

* فشرده سازی داده ها
* رمزگذاری داده ها
* بررسی خطا
* فرا داده ها
* مقادیر هش
* تقسیم بندی تصویر به چند بخش

علاوه بر این، راه حل های مختلف نرم افزار جرمیابی با قالب های اختصاصی تصویر با ویژگی های مشابه ارائه می شوند. هنگام انتخاب قالب تصویر برداری، همیشه گزینه ای را انتخاب کنید که توسط اکثر راه حل های نرم افزار جرمیابی پشتیبانی می شود. برخی از DFL ها از نرم افزار جرمیابی متفاوتی استفاده می کنند و در نتیجه این امکان وجود دارد که اگر بررسی کننده یک فرمت فایل تصویری منحصر به فرد را انتخاب کند، ممکن است فایل تصویر باز نشود.

۵.۱.۲.۵- جریان روند

فرآیند متداول برای دستیابی به جمع آوری داده ها در شکل زیر نشان داده شده است:

شکل ۶. فرآیند دستیابی به اطلاعات در رایانه

روش دستیابی به اطلاعات در بخش زیر توضیح داده شده است. یک جریان روند تفصیلی در **پیوست ج**: نمودار جریان فرآیند دستیابی موجود است.

الف) رسانه ذخیره سازی را مشخص کنید

بررسی کننده باید قبل از تحویل، یک رسانه ذخیره سازگار با اندازه کافی از داده ها را تهیه کند. اگر این شاهد بزرگ باشد، ممکن است بررسی کننده برای ذخیره فایل تصویری نیاز به تهیه چندین رسانه ذخیره سازی داشته باشد.

ب) از شاهد تصویر بگیرید

برای تصویربرداری از شاهد، ابتدا آن را به یك مسدود کننده نوشتن متصل کنید تا مطمئن شوید این شاهد قابل نوشتن نیست، بنابراین از هماهنگی آن محافظت می کنید. بیشتر ابزارهای جرمیابی این ویژگی را ارائه می دهند. سپس فایل تصویری در رسانه ذخیره سازی آماده ذخیره می شود. برای محافظت از رسانه های ذخیره سازی و فایل تصویر، با استفاده از شواهد و مدارک به دست آمده از SHA۲۵۶، از یک قالب استاندارد عنوان گذاری استفاده کنید.

بررسی کننده باید توجه داشته باشد که استفاده از یك روش مسدود کننده نوشتن موجود، مانع از تغییر اطلاعات در درایو حالت جامد یا فلش نمی شود، که شامل تراشه کنترلر است. به محض وصل شدن کنترلر به منبع تغذیه، سازماندهی مجدد داده ها روی تراشه های فلش آغاز خواهد شد. کارهایی مانند تقویت نوشتن و جمع آوری ضایعات توسط کنترل کننده انجام می شوند حتی در هنگام اتصال به دستگاه مسدود کننده نوشتن. در این مقطع زمانی، فقط

یک روش فشرده بر منابع برای ایجاد یک نسخه جرمیابی از رسانه های فلش وجود دارد. این کار با عدم ارسال مجدد تراشه از صفحه مدار و سپس تجدید مجدد داده ها به روش صحیح در صورت امکان انجام می شود.
ج - بررسی شاهد و فایل تصویری
پس از ایجاد فایل تصویر، بررسی کننده باید بررسی کند که با استفاده از نرم افزار جرمیابی قادر به اجرای آن است و مقادیر هش در شاهد و فایل تصویر همسان هستند یا خیر.
د. مستند کردن کلیه اقدامات
آخرین مرحله برای بررسی و تجزیه و تحلیل رایانه، مستند سازی فرآیند، ابزارهای مورد استفاده، مقادیر هش، تاریخ و زمان و همچنین کارهای اولیه بررسی کننده در یادداشت های فایل است. نمونه ای از یادداشت ها یا کاربرگ در پیوست F: کاربرگ اکتساب داده ها موجود است.

۵.۱.۳- دستگاه های تلفن همراه

در زیر جزئیات استخراج داده ها در دستگاه های تلفن همراه ارائه شده است.

۵.۱.۳.۱- انواع استخراج داده ها

قبل از شروع کار جرمیابی دیجیتال، بررسی کننده باید فایل های موردی را که از درخواست کننده به دست آمده است، بررسی کند تا انواع داده های مورد نیاز از شاهد را مشخص کند. این کار می تواند به بررسی کننده در تصمیم گیری در مورد بهترین روش استخراج فایل کمک کند. قبل از انجام کار باید تلاش شود همه گذرواژه‌ها یا الگوهای شاهد را جمع کنید. برای مثال با استفاده از روش دستی، قفل گوشی باید باز شود. تقریباً تمام روشهای استخراج نیاز به باز کردن قفل تلفن ها دارند. بنابراین همیشه خوب است که سعی کنید کد باز کردن قفل را بدست آورید.
پنج سطح مختلف استخراج داده ها برای دستگاه های تلفن همراه وجود دارند، که از سطحی توصیف می شوند که در آن اکثر داده ها می توانند به صورتی استخراج شوند که کمترین میزان ممکن باشد. صرف نظر از روش استفاده شده، پس از استخراج اطلاعات از دستگاه (با وارد کردن سیم کارت و MicroSD) سیم کارت و Micro SD باید جداگانه مورد تجزیه و تحلیل قرار گیرند.

الف) استخراج فیزیکی

استخراج فیزیکی کسب داده های باینری خام از ذخیره سازی رسانه دستگاه است. سپس این داده های خام باید در مرحله بعدی توسط نرم افزار جرمیابی تجزیه و تحلیل و پردازش شوند. این روش به طور معمول به بررسی کننده اجازه می دهد تا به داده های زنده و حذف شده، فایل های سیستم عامل و مناطقی از دستگاه که به طور معمول در دسترس کاربر نیستند دسترسی پیدا کند.

ب) استخراج فایل سیستم (FSD)

استخراج فایل سیستم (FSD) ترکیبی از استخراج فیزیکی و استخراج منطقی است. FSD سیستم فایل دستگاه را بازیابی می کند و داده ها را در مرحله پردازش تفسیر می کند. این امر اجازه می دهد تا به عنوان مثال، بانک اطلاعاتی که پیام های حذف شده را که ممکن است در یک استخراج منطقی در دسترس نباشند، بازیابی کند. با این حال، محدودیت FSD این است که تمام داده های حذف شده را به روشی که یک استخراج فیزیکی قادر به انجام آن است، بازیابی نمی کند.

ج) استخراج منطقی

استخراج منطقی شامل دریافت اطلاعات از دستگاه تلفن همراه است و به دستگاه اجازه می دهد داده ها را برای تجزیه و تحلیل ارائه دهد. این امر اغلب معادل دستیابی به داده های خود دستگاه است. این روش فقط داده های زنده را در اختیار بررسی کننده قرار می دهد. بیشتر نرم افزار های جرمیابی دستگاه تلفن همراه این نوع ویژگی را ارائه می دهد.

د) روش دستی

محدودیت نرم افزار جرمیابی این است که گاهی اوقات از مدل برخی از دستگاه های موبایل منحصر به فرد یا مدل های اخیراً راه اندازی شده پشتیبانی نمی کند. در این حالت معمولاً استفاده از روش دستی برای بررسی کننده قابل قبول است. این روش به عکس و داده های نمایش داده شده روی صفحه با عکس یا فیلم یا رونویسی از داده های آن دسترسی می یابد. برای دستگاه های اندروید، بررسی کننده ممکن است انجام اقدامات ضبط با استفاده از ابزارهای نرم افزاری را در نظر بگیرد. این روش ممکن است نیاز به اتصال تلفن از طریق دستور ADB داشته باشد و حالت مربوط به توسعه دهنده فعال باشد.

و) JTAG / برداشتن چیپ / ریشه یابی / Jail Breaking

برای دستگاه های تلفن همراه که با یک رمز عبور آسیب دیده یا قفل شده اند، می توان از روش های JTAG و برداشتن چیپ برای استخراج داده ها استفاده کرد. استخراج JTAG نیاز به بازیابی دستگاه و صفحه منطقی آن و اتصال کابل خاص به یک اتصال خاص روی برد دارد. این امر نیاز به مهارت فنی بالایی دارد. با استفاده از این روش، بررسی کننده می تواند داده های باینری خام را از حافظه رسانه ای دستگاه بازیابی کند.

برداشتن چیپ همچنین امکان استخراج داده های باینری خام از حافظه دستگاه را می دهد، اما به حذف دائمی تراشه حافظه دستگاه از صفحه حافظه نیاز دارد. هنگامی که متخصص برداشتن چیپ را انجام داد، دستگاه آسیب می بیند و دیگر نمی توان از آن استفاده کرد. علاوه بر این، انتظارات در مورد استفاده از برداشتن چیپ برای دستگاه های تلفن همراه باید تعدیل شوند. دستگاه های اخیر داده های رمزگذاری شده را روی تراشه حافظه خود ذخیره می کنند. دستگاه هایی که بر روی نسخه اندروید ۷.۰ به بعد کار می کنند به صورت پیش فرض رمزگذاری می شوند. برداشتن چیپ برای سایر دستگاه های IoT که معمولاً داده ها را با متن روشن ذخیره می کنند، همچنان قابل استفاده خواهد بود.

روش دیگر، که کمتر مخرب است و می تواند با برخی از دستگاه های تلفن همراه استفاده شود "Root" یا "**Jail Breaking**" است. این فرایند شامل ویژگی های اعمال شده سیستم عامل برای افزایش مجوزها و امتیازات کاربر در حال اجرا (شبیه به روند دستیابی به "Root" در سیستم عامل لینوکس) است. این فرآیند را نمی توان به عنوان یک تکنیک جرمیابی در نظر گرفت زیرا شامل اصلاح فایل های سیستم است و به طور بالقوه می تواند به دستگاه آسیب برساند و بنابراین باید در لیست تکنیک های مورد استفاده کم باشد.

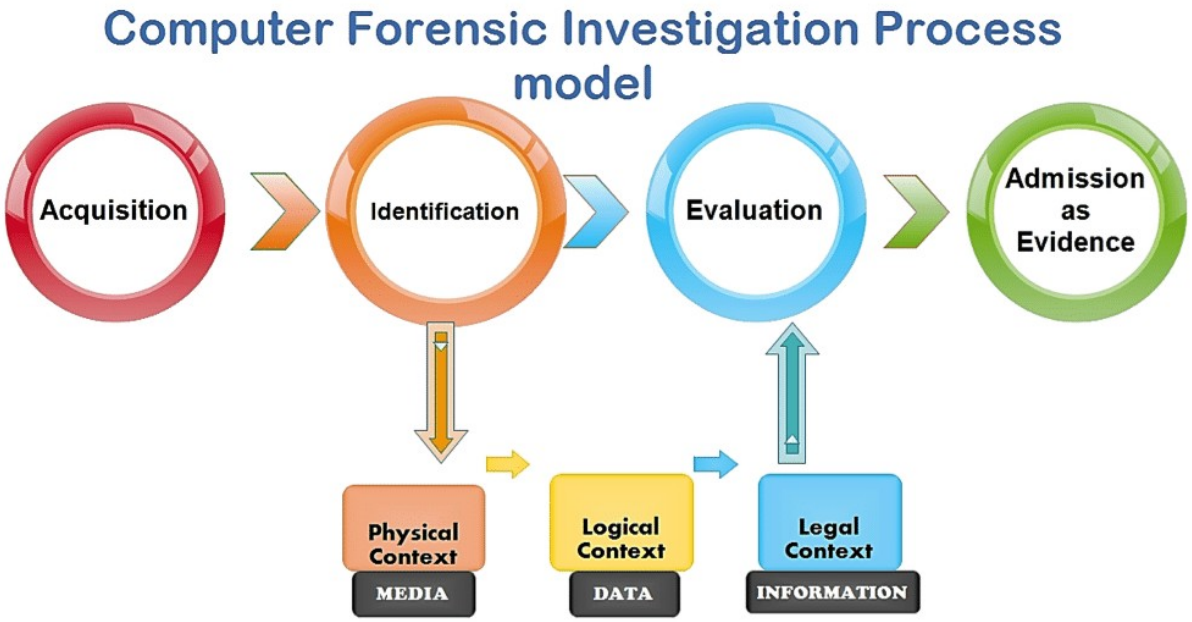
ترتیب تلاش برای استخراج مهم است. بررسی کنندگان باید تلاش کنند تا روش بررسی را انجام دهند که کمترین تخریب را داشته باشد اما بیشترین اطلاعات را به دست می آورد. این امر به بررسی کنندگان این امکان را می دهد تا مناطقی را که ممکن است در مراحل بعدی آسیب دیده یا رونویسی شوند، مشخص کنند. روش های استخراج مانند JTAG و چیپ خاموش فقط باید به عنوان آخرین راه حل در نظر گرفته می شوند، به ویژه در مورد چیپ خاموش زیرا این روند می تواند مخرب و غیرقابل بازگشت باشد.

۵.۱.۳.۲- ابزار استخراج

تجزیه و تحلیل دستگاه های تلفن همراه به طور معمول نیاز به استفاده از نرم افزار اختصاصی، کابل برق و کابل داده دارد. تکنیک های پیشرفته تر بررسی مانند JTAG یا چیپ خاموش به ابزارهای دیگری احتیاج دارند. اینها شامل تجهیزات لحیم کاری و ابزارهای تخصصی برای خواندن داده های خام از تراشه های حافظه دستگاه می شوند.

۵.۱.۳.۳- فرمت استخراج فایل

به دلیل نیاز به استفاده از ابزارهای اختصاصی برای استخراج داده ها، داده های تلفن همراه اغلب در قالب اختصاصی استخراج می شوند. این فرمت ها اغلب می توانند بین ابزارهای مختلف منتقل شوند تا نقاط قوت توانایی های مختلف رمزگشایی را به دست آورند. سایر قالب های غیر اختصاصی شامل فایل های بازیابی و فایل های خام می شوند.



شکل ۷. فرآیند استخراج داده ها در دستگاه های تلفن همراه

الف) مشخص کردن شاهد و رسانه ذخیره سازی

قبل از ادامه مراحل بعدی، بررسی کننده شاهد موجود را مشاهده می کند. عنوان شاهد باید در قسمت داخلی دستگاه تلفن همراه گذاشته شود، یا در پشت آن چاپ شود. عنوان باید شامل شماره شناسه تجهیزات بین المللی موبایل (IMEI)، شناسه تجهیزات تلفن همراه (MEID) یا شماره سریال باشد. این داده های منحصر به فرد دستگاه را شناسایی کرده و برای ارسال درخواست برای صدور صورتحساب یا انجام تجزیه و تحلیل در مراحل بعدی تحقیق استفاده می شوند. ساخت، مدل و IMEI / MEID نیز می توانند برای تعیین سطح پشتیبانی از نرم افزار جرمیابی استفاده شوند. در مرحله بعد، یک رسانه ذخیره سازی باید برای ذخیره داده های استخراج شده آماده شود. در صورت نیاز به یک سیم کارت کلون شده، یک سیم کارت کار نکرده و خالی باید تهیه شود.

ب) شاهد را از شبکه جدا کنید

هنگام انجام استخراج از دستگاه تلفن همراه، دستگاه باید روشن شود. برای جلوگیری از هرگونه تلاش برای اتصال به یک شبکه و متعاقباً ریسک تغییر در هر داده، این شاهد باید از یک شبکه جدا شود. در برخی کشورها، برخی از شبکه های عمومی در همه جا در دسترس هستند و شاهد باید برای اتصال آنها به صورت پیش فرض پیکر بندی شود.

بسته به بودجه، جدا سازی را می توان از طریق اشکال مختلف حاصل کرد:

کارت SIM/IDEN کلون شده	یک کارت SIM/IDEN کلون شده در شاهد به صورت کارت اصلی ظاهر می شود اما دارای قابلیت اتصال به شبکه تلفن همراه نیست. یک کارت SIM/IDEN مشترک را تشخیص می دهد و یک اتصال به شبکه را انجام می دهد. بعضی ابزارهای جنایی دارای عملکرد کلون کردن کارت SIM/IDEN هستند. آخرین تلفن های همراه می توانند بدون سیم کارت کار کنند و هیچ تاثیری بر ذخیره داده ها در تلفن مشاهده نمی شود.
اتاق دارای پوشش شبکه	یک آزمایشگاه نصب شده با پوشش فارادی برای پیش گیری از سیگنال های شبکه. با این حال این راه حلی بسیار گران قیمت است و استفاده از باکس های فارادی کوچک تر می تواند راه جای گزین موثرتری باشد. در صورت عدم وجود آن، محفظه های مناسب همانند کیسه های فارادی می توانند استفاده شوند.
تجهیزات متراکم کردن بی سیم	این ابزار سیگنال های ورودی شبکه را بلوکه می کند. در بعضی موارد، استفاده از آن غیر قانونی است که در بخش ۳.۲.۲ به آن اشاره شده است.
روش دستی	این ارزان ترین روش است. با این حال، نیازمند این است که بررسی کننده به شاهد دسترسی داشته باشد. این کار باعث ریسک هایی برای تغییر داده ها می شود. این مورد با تنظیم دستگاه تلفن همراه در حالت پرواز و غیر فعال کردن وای فای، بلوتوث و هر گونه اتصال دیگر به شبکه عمل می کند.

ج) استخراج داده های مربوطه

با توجه به برخی از تکنیک های استخراج خاص، مانند استخراج بارگذار iOS Boot و ریشه یابی کردن دستگاه های اندرویدی، همیشه امکان پیاده سازی مسدود کردن نوشتن بر روی دستگاه تلفن همراه ممکن نیست. در صورت امکان، مسدود کردن نوشتن باید به عنوان مثال در کارت های حافظه اجرا شود. با این حال، به طور گسترده ای اذعان شده است که روش انسداد نوشتن همیشه برای دستگاه های تلفن همراه امکان پذیر یا کاربردی نیست. به همین دلیل لازم است که بررسی کننده هنگام کار با دستگاه های تلفن همراه کاملاً از عواقب اقدامات خود آگاه باشد و قادر به توضیح و توجیه این اقدامات باشد.

دستگاه های تلفن همراه با سه رسانه مجزا ارائه می شوند که به روش های جداگانه دستیابی نیاز دارند، مانند جدول زیر:

جدول ۸. رسانه ذخیره سازی دستگاه تلفن همراه

رسانه	توصیف
کارت SIM/IDEN کلون شده	نیازمند ابزارهای جنایی تلفن همراه است. روش استخراج داده استخراج منطقی است. استخراج فیزیکی برای این ابزار امکان پذیر نیست. بهتر است که کارت SIM/IDEN کلون شده از شاهد در مدت کار جرمیابی دیجیتال برداشته شود. با این حال، بعضی ابزارها نیازمند این هستند که کارت درون دستگاه ها باشد زمانی که آنها روشن می شوند. بررسی کننده ممکن است یک کارت SIM/IDEN کلون شده ایجاد کند برای غلبه بر این مشکل.
کارت های حافظه	اینها می توانند همانند یک هارد دیسک کامپیوتر بررسی شوند. هر دوی استخراج منطقی و فیزیکی می توانند در این کارت ها اجرا شوند تا زمانی که ابزارهای جنایی از این ویژگی

	پشتیبانی می کنند. بررسی کننده داده ها را استخراج می کند و سپس دوباره آن را در دستگاه قرار می دهد قبل از روشن کردن آن. بعضی ابزارها داده ها را در کارت حافظه ذخیره می کنند و اگر آن تشخیص دهد که کارت موجود نیست، می تواند باعث از دست رفتن داده ها از دستگاه تلفن همراه شود. اگر زمان و منابع اجازه دهند، یک کلون بیت به بیت از کارت حافظه باید ایجاد شود و آن کلون در دستگاه قرار گیرد.
حافظه داخلی	این مورد نیازمند ابزارهای جنایی دستگاه تلفن همراه است. بعضی دستگاه ها توسط ابزارهای جنایی برای یک استخراج فیزیکی بارگذاری بوت پشتیبانی می شوند.این مورد می تواند اغلب بدون کارت SIM/IDEN کلون شده انجام شود. ابزارهای جنایی دستگاه را به طریقی خاص راه اندازی می کنند و استخراج فیزیکی را بدون تغییرات در داده های کاربر روی دستگاه انجام می دهند. این روش می تواند به صورت بالقوه کدهای قفل شده دستگاه را بازیابی کند که به بررسی کننده امکان می دهد دسترسی کاملی به شاهد در زمان روشن کردن آن داشته باشد.

بسته به ابزار استخراج انتخاب شده فرایند استخراج متفاوت خواهد بود. بیشتر ابزارهای جرمیابی دارای راهنمایی هستند که روشی که باید برای استخراج موفقیت آمیز دنبال شود را توضیح می دهند. در برخی موارد، بررسی و تجزیه و تحلیل دستگاه تلفن همراه به منظور استخراج داده ها نیاز به تغییر در فایل های سیستم یا سیستم عامل دارد. تا حدودی لازم است اپلیکیشن ها را بر روی دستگاه تلفن همراه بارگذاری یا نصب کنید. این فرآیند می تواند باعث از بین رفتن غیرقابل برگشت برخی از داده ها شود، اما فقط روی فایل های سیستم با ارزش بدیهی تأثیر می گذارد. با داشتن گواهینامه های آموزشی مناسب، از جمله آموزش ارائه شده توسط تولید کنندگان نرم افزار جرمیابی موبایل یا تجربه عملی شامل آزمایش استخراج دستگاه های تلفن همراه، می توان دانش مربوط به هر یک از این مراحل را داشت.
منبع خوب دیگر برای شواهد جرمیابی، فایل پشتیبان دستگاه تلفن همراه است. برخی از کاربران و دستگاه ها روی دستگاه های دیگر پشتیبان ایجاد می کنند مثلا درون کامپیوتر یا در ابرها. این نسخه های پشتیبان می توانند در ساخت یک جدول زمانی از شواهد کمک کنند و همچنین می توانند برای دستیابی به یک دستگاه قفل شده از رمز عبور استفاده کنند. همچنین می توان برخی از پشتیبان ها را گویی که یک وسیله فیزیکی هستند، تجزیه و تحلیل کرد.

د) بررسی شاهد و داده های استخراج شده

پس از استخراج داده ها، بررسی کننده باید داده ها را بر اساس داده های نمایش داده شده در شاهد بررسی کند. اطلاعاتی از قبیل تاریخ و زمان باید توسط بررسی کننده بررسی شوند، زیرا بعضی اوقات در طی فرآیند استخراج به قالب تاریخ / زمان دیگری تبدیل می شوند.

و) مستند کردن کلیه اقدامات

آخرین مرحله برای بررسی و تجزیه و تحلیل یک دستگاه تلفن همراه، مستند سازی فرآیند، ابزارهای مورد استفاده، تاریخ و زمان و مدارک اولیه بررسی کننده در یادداشت های موردی است.

۵.۲- بررسی

۵.۲.۱- موارد عمومی

در صورت امکان از بررسی شواهد اولیه خودداری شود. بررسی کننده باید همیشه بر روی نسخه جرمیابی (فایل تصویر) شواهد کار کند. اگر این کار اجتناب ناپذیر باشد، دسترسی به داده ها باید با استفاده از مسدود کننده نوشتن محافظت شود.

در موارد خاص، بررسی کنندگان برای انجام بررسی باید از یک محیط جدا شده یا یک محیط از پیش تعیین شده استفاده کنند. به عنوان مثال، انجام شبیه سازی بر روی سیستم پایگاه داده یا نرم افزار بازی. برای دستیابی به این هدف، بررسی کنندگان ممکن است از فناوری مجازی سازی استفاده کرده و فایل را در یک محیط کاری محافظت کنند. پس از اتمام بررسی، بررسی کننده می تواند با استفاده از یک تصویر شناخته شده یا با استفاده از ویژگی ارائه شده توسط سیستم عامل، محل کار را به حالت قبلی خود برگرداند.

۵.۲.۲- تریاژ

تریاژ فرایند اولویت بندی موارد، شاهد ها یا داده های مربوط به فرآیندهای تجزیه و تحلیل، با توجه به اهمیت آنها در مورد موضوع است. براساس نتیجه تریاژ، فایل ها، شاهد ها یا داده ها بسته به توالی اولویت آنها از مهمترین تا کمترین اهمیت آنالیز خواهند شد. این امکان وجود دارد که برخی به دلیل بی ربط بودن به فایل مورد بررسی، اصلاً مورد تحلیل قرار نگیرند.

تریاژ به منظور رسیدگی به موقعیت هایی مانند موارد زیر انجام می شود:

* حجم عظیمی از شاهد ها یا داده های دسته جمعی باید در یک بازه زمانی کوتاه مورد تجزیه و تحلیل قرار گیرند.
* شاهد ها به دلیل مسائل حقوقی دیگر قابل ذخیره نیستند.
* این یک مورد با اولویت بالا است و نتایج باید بلافاصله به دست آیند، یعنی در موردی که آسیب فیزیکی یا مرگ فیزیکی امکان پذیر باشد.

در حالی که تریاژ مزایایی را ارائه می دهد، اما معایبی نیز وجود دارند که باید برطرف شوند. یک تریاژ نمی تواند جایگزین یک آزمایش کامل شود. تریاژ با استفاده از پردازش خودکار انجام می شود، این کار توسط نرم افزار جرمیابی یا با کدهای خود نوشته شده برای شاهد ها یا داده ها انجام می شود. این خطر وجود دارد که این پردازش خودکار فقط زیرمجموعه داده ها را بررسی کند، و برخی از داده های مهم ممکن است کنار گذاشته شوند. این خطر باید برای بررسی کننده، دادستان یا قاضی توضیح داده شود و براساس اطلاعاتی که ممکن است آنها برای تصمیم گیری به نفع یا در مقابل روند دادرسی برای آن مورد خاص نیاز داشته باشند، توضیح داده شود. با این حال، تریاژ یک روش معتبر برای کنار آمدن با وضعیتی است که به هیچ وجه قابل حل نیست.

نرم افزارهای زیادی در بازار وجود دارند که عملکردهای تریاژ را ارائه می دهند که برخی تجاری و برخی با منبع آزاد هستند. تریاژ را می توان با اجرای نرم افزار در حالی که شاهد هنوز زنده است یا با راه اندازی این شاهد با استفاده از رسانه های راه اندازی انجام داد. سپس بررسی کننده کلمات کلیدی را وارد می کند و به سیستم اجازه می دهد تا قبل از انتخاب فایل های مربوطه و ذخیره آنها در رسانه های قابل جابجایی، سیستم را اجرا کند. با این کار چندین شاهد می توانند همزمان، حتی در طول شب یا در آخر هفته نیز پردازش شوند.

پس از انجام تریاژ و زمانی که بررسی کننده تصمیم گرفت که این شاهد به تحقیقات مرتبط است، بررسی کننده می تواند سپس به مراحل بعدی که در این سند توضیح داده شده است برود و از روش های پیچیده تری برای جمع آوری داده های بیشتر از رایانه استفاده کند.

۵.۲.۳- روش های آزمایش رایانه

روش ها و تکنیک های زیادی برای بررسی یک کامپیوتر وجود دارند. برخی به مهارت های زیادی نیاز دارند در حالی که برخی دیگر مهارت کمتری نیاز دارند، مانند انجام یک فرایند خودکار. تعدادی از نرم افزارهای جرمیابی توسط بررسی کننده قابل استفاده هستند. بسته به توانایی نرم افزار، برخی از آنها قادر به بازیابی رمزهای عبور، ارتباط داده ها بین شواهد الکترونیکی و انجام جستجوهای کلمات کلیدی هستند.

جریان روند انجام آزمایش در رایانه در پیوست H ارائه شده است: نمودار جریان بررسی رایانه موجود است. نمودار جریان در بخش زیر توضیح داده شده است.

۵.۲.۳.۱- امتحان "سیستم مرده"

"سیستم مرده" سیستمی است که اجرا نمی شود، بدون برق خاموش می شود. هنگامی که سیستم "مرده" است، دیگر داده های فرار در مناطق ذخیره موقت مانند حافظه RAM، فرآیندهای در حال اجرا، حافظه پنهان یا گفتگوی برنامه های فعال در رایانه در دسترس نخواهند بود.

بررسی "سیستم مرده" باید داده های زیر را در نظر بگیرد:

* فایل های فعال، فایل های حذف شده، فایل اولیه، پارتیشن اولیه، دیسک خاموش و فایل های سایه
* بخش های مصنوعی دستگاه - فایل های سیستم عامل، رجیستری فایل، ابرداده های فایل، فایل های رمزگذاری شده، فایل های لاگ و فایل های پایگاه داده
* مرور سابقه، ایمیل، رسانه های اجتماعی و اشتراک فایل نظیر به نظیر

۵.۲.۳.۲- امتحان "سیستم زنده"

"سیستم زنده" سیستمی است که در حال اجرا است، در حالی که برنامه ها ممکن است در حال اجرا باشند و با پردازش داده ها به طور پیوسته می توان آنها را به روز کرد. به دلیل شواهد ارزشمندی که می توان در یک سیستم زنده کشف کرد، خاموش کردن آن ممکن است باعث از بین رفتن داده های ناپایدار مانند داده های ذخیره شده در ابر، داده های رمزگذاری شده، فرآیندهای در حال اجرا، اتصالات شبکه و سیستم فایل های نصب شده شود. بررسی یک سیستم زنده باید داده های زیر را در نظر بگیرد:

* حافظه با دسترسی تصادفی (RAM)
* فرآیندهای در حال اجرا
* اتصالات شبکه
* تنظیمات سیستم
* رسانه ذخیره سازی

* خدمات ابری

بسته به مورد در دست بررسی ممکن است بررسی یک سیستم زنده بر روی هر یک از داده های فوق انجام شود.

۵.۲.۳.۳- پردازش خودکار

پردازش خودکار اغلب با استفاده از ویژگی های موجود در نرم افزار جرمیابی انجام می شود. دامنه پردازش خودکار معمولاً در ابتدای بررسی توسط بررسی کننده تعیین می شود. این دامنه می تواند برای سایر موارد در محدوده مشابه تحقیق تکرار شود. به عنوان نمونه، مقایسه هش در تصاویر در فایل پورنوگرافی کودک. فعالیت ها و توالی های مشترک برای پردازش خودکار عبارتند از:

۱. استخراج داده های سیستم عامل و کاربران

۲. فایل های مانند ZIP، RAR و فایل های رمزگذاری شده را نصب کنید.

۳. بخش های مصنوعی از قبیل صندوق پستی و تاریخچه اینترنت را استخراج و رمز گذاری کنید.

۴. تجزیه و تحلیل امضا

۵- فایل ها و پوشه های حذف شده را بازیابی کنید

۶. پارتیشن های حذف شده را بازیابی کنید

۷. بررسی انواع فایل خاص

۸- بسته به نوع مورد، از این روشهای تحلیل استفاده می شود:

* جستجوی کلید واژه
* تشخیص کاراکتر نوری (OCR) در فایل های PDF
* تصاویر کوچک برای مشاهده آسان ایجاد کنید
* تصاویر را از فیلم ها استخراج کنید
* تشخیص رنگ پوست برای فیلم ها
* مقایسه هاش

۹. پردازش لاگ های مربوط به سیستم عامل (به عنوان مثال ورود به سیستم ویندوز)

این مرحله باعث صرفه جویی در زمان می شود زیرا می تواند شبانه و یا آخر هفته با حداقل نظارت انجام شود، اگرچه از قدرت محاسباتی بالایی استفاده می کند.

۵.۲.۳.۴- بازیابی اطلاعات

بازیابی اطلاعات شامل بازیابی اطلاعات در رسانه های ذخیره سازی می شود که حذف شده اند، آسیب دیده اند، پنهان شده اند یا از بین رفته اند. در بعضی موارد، رسانه ذخیره سازی آسیب دیده، خراب یا فرمت شده باعث می شود داده ها غیرقابل دسترسی باشند. بنابراین بازیابی اطلاعات شامل فرایند تثبیت رسانه ذخیره سازی نیز می باشد تا داده ها از رسانه استخراج شوند.

دو نوع بازیابی اطلاعات وجود دارند: **بازیابی منطقی و بازیابی فیزیکی**

بازیابی منطقی در صورت دستیابی به رسانه های ذخیره سازی انجام می شود، اما داده های فرمت شده، خراب، پنهان یا گم شده ساخته می شوند. روند بازیابی معمولاً با استفاده از نرم افزار جرمیابی انجام می شود.

بازیابی فیزیکی هنگامی انجام می شود که محیط ذخیره سازی به دلیل خرابی مکانیکی یا خرابی الکترونیکی غیرقابل دسترسی باشد. روند بهبودی بسیار خسته کننده است و به مهارت پیشرفته ای نیاز دارد. در بعضی موارد برای انجام بازیابی فیزیکی به اتاق مخصوصی نیاز است، به عنوان مثال تعویض سر در هارد دیسک نیاز به انجام آن در یک اتاق کلاس ۱۰۰ دارد. در موارد دیگر، تجهیزات ویژه ای برای بازیابی اطلاعات مورد نیاز هستند. به عنوان مثال، هنگام تعویض کابل در درایو USB، دستگاه لحیم کاری لازم است.

همه DFL ها نمی توانند دارای یک بازیابی فیزیکی باشند زیرا هزینه بالایی دارد و یک بررسی کننده ماهر نیز لازم است تا کارها را انجام دهد. با این وجود، داشتن یک مرکز بازیابی منطقی برای DFL کافی است. بیشتر نرم افزارهای تجزیه و تحلیل جرمیابی با یک ویژگی بازیابی منطقی همراه هستند، بنابراین بررسی کننده برای صرفه جویی در هزینه ها می تواند از ویژگی پیشنهادی یا ارتقای آن استفاده کند.

۵.۲.۳.۵- فیلتر کردن

استفاده از فیلترها بر روی یک فایل تصویری قبل از تجزیه و تحلیل می تواند به کاهش میزان داده هایی که بررسی کننده برای مشاهده و تجزیه و تحلیل نیاز دارد کمک کند. تکنیک های محبوب فیلتر کردن از مجموعه های هش برای فیلتر کردن سیستم عامل های شناخته شده یا فایل های برنامه (لیست سفید) یا جستجوی مربوط به هش در پایگاه های داده های مواد غیرقانونی شناخته شده (لیست سیاه) استفاده می کنند. فیلتر کردن فقط می تواند زمانی مورد استفاده قرار گیرد که تنها انواع خاصی از یافته ها به فایل مربوط هستند. فایل ها را می توان با تجزیه و تحلیل امضا فیلتر کرد – بر اساس اندازه، تاریخ، مالک و جزئیات بیشتری که در درون فرا داده ها قرار دارند. این ویژگی فیلتر کردن در اکثر نرم افزارهای جرمیابی تجاری ارائه می شود.

۵.۲.۴- روش های آزمایش دستگاه تلفن همراه

دستگاه های تلفن همراه چالش بی نظیری را برای بررسی کننده به وجود می آورند زیرا تنوع سیستم عامل ها، مارک ها و مدل های بی شمار، فراوانی داده ها و تنوع انواع داده های ذخیره شده در آنها بسیار زیاد است.

در زیر روش های عمومی متداول انجام شده بر روی دستگاه های تلفن همراه توضیح داده شده اند.

۵.۲.۴.۱- پردازش خودکار

پردازش دستگاه های تلفن همراه به دلیل سخت افزار و نرم افزار بسیار متفاوتی که در این دستگاه ها استفاده می شود، اغلب نیاز به رویکرد متفاوتی نسبت به رایانه ها دارد. برنامه های کاربردی با فرکانس بسیار بیشتری به روز می شوند، و تغییرات اغلب می توانند عمده باشند. به همین دلیل، ابزار جرمیابی اختصاص داده شده به طور خودکار بسیاری از داده ها را پردازش می کند، اما تأیید دستی این پردازش اغلب لازم است. تعدادی از ابزارهای موجود از نوعی "پردازش فازی" استفاده می کنند، یعنی می توان گفت که پردازش به گونه ای انجام می شود که باعث می شود بر اساس منطق مناسبی باشد.

۵.۲.۴.۲- فیلتر کردن

فیلتر کردن داده های تلفن همراه معمولاً در سطح نوع داده انجام می شود. داده ها با استفاده از ابزارهایی در حین پردازش در گروه هایی مانند داده های ارتباطی و فایل های رسانه ای فیلتر می شوند. این گروه ها سپس بیشتر تقسیم می شوند. به عنوان مثال داده های ارتباطی را می توان به سوابق تماس و پیام تقسیم کرد. سطح فیلتر ارائه شده به تحلیلگر بستگی به ابزاری دارد که مورد استفاده قرار می گیرد، با این حال، این فیلتر به تحلیلگران این امکان را می دهد تا انواع داده های کلیدی را به سرعت بررسی کنند. آنها می توانند شامل پیامک های ارسال شده و دریافت شده و سوابق مکالمه برای برقراری تماس بین مظنونان باشند.

۵.۳- تجزیه و تحلیل

در مرحله تحلیل، بررسی کننده مدارک الکترونیکی را بر روی تصاویر جستجو می کند. این کار می تواند بسیار وقت گیر باشد و برای تفسیر انواع سیستم های فایل، سیستم عامل ها و برنامه های کاربردی، نیاز به دانش زیادی دارد. بسیاری از عوامل مختلف بر زمان و حجم کاری که برای مرحله تجزیه و تحلیل لازم هستند تأثیر می گذارند. این عوامل شامل میزان رسانه های ذخیره سازی مورد تجزیه و تحلیل، اندازه رسانه های ذخیره سازی، پیچیدگی سیستم های فایل مورد

استفاده، میزان استفاده از سیستم عامل، پیشرفته بودن کاربر، پیچیدگی نرم افزار و تکنیک های مورد استفاده توسط کاربر کامپیوتر و غیره می شوند.

۵.۳.۱- تجزیه و تحلیل رایانه

۵.۳.۱.۱- دسته بندی آثار دیجیتال

درست همانطور که یک جنایتکار در صحنه جنایت آثار بدنی را باقی می گذارد، فرد مجرمی که از طریق رایانه مرتکب یک جرم می شود، در "صحنه جرم دیجیتال" اثری را باقی می گذارد. برخی از این ردپاها قابل کشف هستند، برخی از آنها می توانند پیکربندی شوند تا توسط بررسی کننده قابل کشف نباشند. در جدول زیر چند نمونه از آثار و پیکربندی های قابل کشف برای جلوگیری از ردپای قابل کشف ذکر شده اند.

جدول ۹. آثار قابل کشف و کشف نشده از رایانه

آثاری که قابل کشف هستند	آثاری که پیکربندی می شوند تا غیر قابل کشف باشند
موارد مصنوعی که در کامپیوتر به صورت پیش فرض ذخیره می شوند. احتمال یافتن این گونه آثار بالا است حتی اگر یک مظنون تلاش کند این آثار را بپوشاند.	موارد مصنوعی که می توانند پیکربندی شوند تا در کامپیوتر ذخیره نشوند. برای مثال، یک مرورگر وب جایی که کاربر می تواند سابقه دانلود را غیر فعال کند یا حذف کند.
بعضی از آثار قابل کشف: * فضای بیهوده * فضای اختصاص داده نشده * ورودی های MFT RAM*	بعضی از آثار غیر قابل کشف: * حافظه های پنهان * لیست هایی که اخیرا استفاده شده اند * فایل های لاگ * سوابق مرورگر * حافظه های پنهان مرورگر * برنامه هایی که بیشتر استفاده می شوند * داده های فرم * Pagefile.sys * Hiberfil.sys * کپی های سایه * سابقه دانلود

۵.۳.۱.۲- رویه هایی برای آثار (ردپاهای) متفاوت

داده ها و اطلاعاتی که باید از کامپیوتر استخراج شوند بستگی به نوع فایل دارند. به عنوان مثال در یک فایل مربوط به کلاهبرداری، داده ها / اطلاعاتی که معمولاً از رایانه استخراج می شوند به شکل صفحه گسترده، ایمیل و اسناد اداری هستند. در مورد کودک آزاری، داده ها / اطلاعات مربوطه ممکن است تصاویر، فیلم ها و پیام های ارتباطی باشند. روند تجزیه و تحلیل انواع مختلف بخش های مصنوعی در پیوست ا: فرایند تحلیل بخش های مصنوعی شاهد نشان داده شده است. بخش های زیر انواع داده هایی را که می توان از رایانه استخراج کرد، با جزئیات توضیح می دهند.

الف. نامه الکترونیکی

تجزیه و تحلیل نامه های الکترونیکی، به طور معمول کلاینت های پستی مانند Outlook، Thunderbird و Mail و همچنین حساب های وب میل را شامل می شود. کلاینت های مختلف پست الکترونیکی انواع مختلفی از بخش های مصنوعی را تولید می کنند. به عنوان مثال Outlook داده های مشهود را در فایل های پوشه شخصی مانند فایل های

PST، OST و PAB ذخیره می کند. Thunderbird پیام ها را در فایل های صندوق ورودی ذخیره می کند. معمولاً نرم افزار جرمیابی قادر به تجزیه و تحلیل این فایل ها است، اما لزوماً همه پیام ها استخراج نمی شوند. برخی از نرم افزارهای جرمیابی نمی توانند پیام های حذف شده را از فایل های پوشه شخصی بازیابی کنند، بنابراین ممکن است در این حالت به روش بازیابی داده ها نیاز باشد.

ب. اسناد اداری (پردازشگر ورد، صفحه گسترده، اسلاید)

تجزیه و تحلیل اسناد اداری به طور معمول با تجزیه و تحلیل امضای فایل آغاز می شود و با فیلتر کردن فایل های مورد علاقه دنبال می شود. تجزیه و تحلیل امضای فایل برای اطمینان از مطابقت آن، هدر فایل را با پسوند آن مقایسه می کند. اگر مطابقت نداشته باشد، ممکن است این امکان وجود دارد که عنوان یا افزونه را برای مخفی کردن محتوا تغییر دهید. فیلتر کردن فایل ها شامل استفاده از جستجوی کلمه کلیدی است. بیشتر نرم افزارهای جرمیابی قادر به انجام هر دو کار به صورت خودکار هستند.

هنگامی که بررسی کننده اسناد مرتبط را کشف کرد، بهتر است برای تجزیه و تحلیل محتوا به درخواست کننده مراجعه کنید. این امر برای اطمینان از اینکه واقعاً سند استخراج شده مربوط به فایل مورد بررسی است لازم است. هنگامی که درخواست کننده اسناد را تأیید کرد، بررسی کننده می تواند تجزیه و تحلیل بیشتری را در مورد سند، ابرداده اسناد، سازنده اسناد انجام دهد و تشخیص دهد که در کامپیوتر ارسال شده یا دریافت شده است.

ج. تصاویر و فیلم ها

برای انجام تجزیه و تحلیل بر روی تصاویر و فیلم ها، ابتدا باید بررسی کننده ایده کاملی در مورد درخواست کننده داشته باشد تا بداند چه چیزی را باید جستجو کند. اگر مستلزم جستجوی عکس های یکسان باشد، درخواست کننده باید عکسهای لازم را به بررسی کننده ارائه دهد. اگر شامل فایل هایی با هش های شناخته شده باشد، ممکن است درخواست کننده نیاز داشته باشد که به بررسی کننده اطلاع دهد، یا بررسی کننده بتواند از لیستی از هش های پایگاه داده شناخته شده استفاده کند. اگر بخش خاصی از یک فیلم را شامل می شود، درخواست کننده باید ویژگی های منحصر به فرد آن را بیان کند؛ به عنوان مثال، برای استخراج تمام تصاویر از ویدئویی که یک موتورسیکلت دارد.

تجزیه و تحلیل تصاویر به طور معمول با تجزیه و تحلیل امضا آغاز می شود. در مرحله بعد، بررسی کننده می تواند با استفاده از نمای تصویر کوچک تصاویر موجود در گالری را مرور کند.

در صورت نیاز به جستجوی مجموعه ای از تصاویر شناخته شده - به عنوان مثال در فایل کودک آزاری یا طرح های مسروقه - می توان از مقایسه هش برای انجام این کار استفاده کرد. برخی از نرم افزارهای جرمیابی ویژگی تشخیص تصویر مشابه را ارائه می دهند، و بررسی کننده می تواند با تهیه تصویر لازم برای نرم افزار از این ویژگی استفاده کند.

برای تجزیه و تحلیل فیلم، برخی از نرم افزارها قابلیت استخراج تصاویر ثابت از فیلم ها را ارائه می دهند. به عنوان مثال تصاویر Y، در هر X ثانیه / دقیقه. این تصاویر استخراج شده سپس می توانند به صورت گالری مشاهده شوند. این امکان پیش نمایش بسیار کارآمد فایل های ویدیویی را فراهم می کند.

در مواردی که مکان یا جزئیات تولید تصاویر و فایل های ویدئویی مهم است، بررسی کننده باید استخراج ابرداده از آن فایل ها را در نظر بگیرد. ابرداده مجموعه داده هایی است که اطلاعات دیگری را توصیف و به آنها می دهد، به عنوان مثال مختصات GPS که در آن عکس گرفته شده است، تاریخ و زمان ایجاد و همچنین دستگاهی که برای گرفتن تصویر استفاده می شود.

برخی از شاهد ها ممکن است هزاران عکس و فیلم داشته باشند، و غیر ممکن است که بررسی کننده یک فایل خاص ویدیویی یا تصویری را بیابید. بهترین روش برای انجام این کار استفاده از همه تصاویر استخراج شده و سپس انتقال آنها به درخواست کننده است.

کار ساده مشاهده محتویات تصاویر / فیلم ها نیازی به تخصص جرمیابی دیجیتال ندارد و بنابراین می تواند توسط درخواست کننده انجام شود. هنگامی که عکس ها / فیلم های مربوطه شناسایی شدند، می توان تجزیه و تحلیل

بیشتری را توسط بررسی کننده انجام داد تا داده های معنادار تری، مانند مختصات GPS و ایجاد یا تغییر داده ها انجام شوند.

د. مرورگر اینترنت

مرورگرهای اینترنتی در بسیاری موارد دارای ارزش آشکاری هستند. آنها به طور معمول شامل بخش های مصنوعی زیر هستند:

* تاریخچه بازدید از وب سایت
* فایل های محلی / فایل های موقت اینترنت
* نشانه ها / موارد دلخواه
* اطلاعات جلسات
* کوکی ها
* نام کاربری و کلمه عبور ذخیره شده
* ورودی از فیلدهای فرم
* جستجوی کلمات کلیدی اینترنت

تجزیه و تحلیل اثرات مرورگر می تواند برای پیشنهاد هدف یا قصد مهم باشد، به عنوان مثال کلمات کلیدی مورد استفاده در موتورهای جستجو که می توانند هدف را اثبات کنند.

مرورگرهای معروف شامل Mozilla Firefox، Microsoft Internet Explorer / Edge، Google Chrome و Apple Safari هستند. همه آنها داده ها را در فهرست کاربر ذخیره می کنند. به استثنای مرورگرهای مایکروسافت، همه مرورگرهای دیگر از پایگاه داده SQLite برای ذخیره بخش های مصنوعی ذکر شده در بالا استفاده می کنند.

بیشتر نرم افزارهای جرمیابی تجزیه و تحلیل اینترنت تجزیه و تحلیل مرورگر را ارائه می دهد. با این حال، با توجه به فن آوری در حال تحول که بعضی از مرورگرها به روز می شوند، ممکن است برخی از نرم افزارهای جرمیابی برای به روزرسانی پایگاه داده خود مدتی زمان نیاز داشته باشند. بنابراین برای بررسی کنندگان مهم است که ساختار اساسی مرورگرهای اینترنتی را درک کنند. از آنجا که امروزه بیشتر مرورگرها روی پایگاه داده SQLite کار می کنند، بررسی کننده ممکن است با استفاده از مرورگرهای پایگاه داده SQLite، تجزیه موارد مصنوعی را به صورت دستی در نظر بگیرد، که به صورت رایگان قابل دانلود است.

این امر نه تنها به بررسی کنندگان اجازه می دهد تا از یک نرم افزار خاص مستقل باشند بلکه به آنها امکان می دهد نتایج نرم افزار را در برابر مرورگرهای پایگاه داده SQLite بررسی کنند.

و. نرم افزار

هر زمان که نیاز به تجزیه و تحلیل برخی نرم افزارها باشد، بیشتر اوقات مجبور هستیم استخراج و درک مصنوعات نرم افزار را شامل شود. نمونه هایی از چنین نرم افزاری شامل نرم افزار ارتباطی (به عنوان مثال Whatsapp و Skype)، نرم افزار پنهان کردن اطلاعات یا پیام ها (به عنوان مثال OpenStego)، رمز عبور ایمن (به عنوان مثال KeePass)، نرم افزار اشتراک گذاری فایل (به عنوان مثال uTorrent) و نرم افزار رمزنگاری (به عنوان مثال کیف پول Cryptocurrency) است.

اگرچه هیچ روش استاندارد برای چگونگی تجزیه و تحلیل کلیه مصنوعات نرم افزار به دلیل تنوع آنها وجود ندارد، اما معمولاً با جمع آوری اطلاعات در مورد منابع معتبر و قابل اعتماد در مورد مصنوعات نرم افزار انجام می شود. این یافته ها می توانند با انجام یک شبیه سازی تأیید شوند.

ه. فعالیت کاربر

سیستم عامل رایانه فعالیت های کاربر را در مکانهای مختلف دنبال می کند. مثال ها عبارتند از:

* زمان روشن و خاموش کردن

* تنظیمات نرم افزار
* لیست فایل های اخیرا استفاده شده
* استفاده از دستگاه
* ورود به سیستم کاربر
* اتصالات Wi-Fi
* برنامه های ترجیحی
* تنظیم محیط کاربر
* فایل هایی که بیشتر به آنها دسترسی داریم.

تحلیل این فعالیت کاربر، به درک بهتر از رفتار کاربر کمک می کند و حتی می تواند فعالیت های بدیهی را اثبات کند.
بسته به نوع سیستم عامل، بخش های مصنوعی در مکانهای مختلفی ذخیره می شوند. در مایکروسافت ویندوز، بیشتر بخش های مصنوعی در Event Logs ،Registry و Jump List ها ذخیره می شوند.
در سیستم عامل های X، مصنوعات موجود در کتابخانه و پوشه های ثبت شده ذخیره می شوند، در حالی که در سیستم های لینوکس، بیشتر داده ها در پوشه کاربر یا دایرکتوری "/ etc" یا "/ var" ذخیره می شوند.

ی. فایل های ورود به سیستم (Log)

تجزیه و تحلیل این فایل ها به ویژه در موارد حمله به سیستم ضروری است. بررسی کننده نه تنها فایل هاي گزارش شده را باید استخراج کند، بلکه آثاري از فایل هاي log / حذف نشده را نیز باید استخراج مي کند. نرم افزار تخصصی برای تجزیه و تحلیل فایل ورود به سیستم موجود است. اساس چنین تحلیلی جستجوی کلمات کلیدی خاص، الگوهای غیر طبیعی یا جستجوی سیاهه های مربوط در یک بازه زمانی مشخص است.

د. رمزگذاری

امروزه متداول ترین سیستم عامل ها امکانات رمزگذاری داخلی را ارائه می دهند. برای کاربر آسان است که رمزگذاری کامل دیسک را برای درایو سیستم فعال کند. توصیه می شود پیش از تحویل شاهد به DFL، رمزهای عبور یا کلیدهای رمزگذاری با استفاده از داده های زنده از صحنه جنایت جمع شوند.
همچنین می توانید در صورت امکان رمزهای دیگر (به عنوان مثال رمزهای عبور مرورگر) را از دیسک استخراج کنید. این رمزهای عبور و مجوزهای آنها می تواند برای ایجاد یک فرهنگ لغت برای انجام حمله با استفاده از تکنیک های تخصصی رمز عبور رمز استفاده شوند.
علاوه بر این، فعالیت های سنتی مانند جمع آوری شواهد فیزیکی، از جمع آوری شواهد فیزیکی، کلیدها یا رشته های بازیابی باید در تلاش برای یافتن رمزهای عبور انجام شوند.

ن. فضای اختصاص داده نشده

نواحی اختصاص داده نشده می توانند دارای بخش های مصنوعی از انواع شواهد ذکر شده در بالا باشند. با استفاده از نرم افزار خاص می توان جستجو و استخراج انواع فایل های خاص در مناطق اختصاص داده نشده را به صورت خودکار انجام داد. بررسی کننده باید مشخص کند که چه نوع فایل هایی را جستجو می کند زیرا بررسی داده ها کار بسیار وقت گیری است. بررسی داده ها روی فایل های تکه تکه شده خوب کار نمی کند. اکثر داده ها زمانی که در مناطق اختصاصا داده نشده یافت می شوند نمی توانند مربوط به یک کاربر خاص، مهر و موم های زمانی یا حتی مکانی در یک ساختار فایل باشند.

ت. ذخیره در ابر و از راه دور

هنگامی که یک بررسی کننده اثری از سرویس های ابر را در یک کامپیوتر کشف می کند، می تواند یکی از موارد زیر را نشان دهد:

* داده ها به صورت محلی در رایانه و از راه دور روی ابر ذخیره می شوند. یا
* داده ها به طور کامل در ابر ذخیره می شوند. کامپیوتر ممکن است به هیچ وجه حاوی اطلاعاتی نباشد.

در واقع داده هایی که از راه دور ذخیره می شوند ممکن است فقط در یک سرور واحد ذخیره نشوند بلکه می توانند در چندین سرور در ابر ذخیره شوند. بیشتر اوقات، حتی ارائه دهنده سرویس ابری نمی تواند بگوید که در کدام سرور خاص، مرکز داده یا در کدام کشور بخش خاصی از داده ها ذخیره می شوند.

بررسی کننده حتی ممکن است موقعیت هایی را پیدا کند که هیچ بایت داده ای از رایانه های یک شرکت قابل بازیابی نباشد، زیرا آنها صرفاً کامپیوترهای کلاینت و بدون هیچ گونه رسانه ذخیره سازی هستند، اما از منابع یک ماشین مجازی در ابر استفاده می کنند.

اگرچه از لحاظ فنی تهیه نسخه جرمیابی از ماشین مجازی که در ابر ساکن است بسیار آسان است، اما موارد قانونی وجود دارند که باید مورد بررسی قرار گیرند. بسته به قانون قابل اجرا، شناسایی و اخذ مجوز قانونی مناسب برای رهگیری چنین داده هایی ممکن است مسئله ای را ایجاد کند. همچنین باید اطمینان حاصل شود که داده ها مطابق رویه های قانونی در کشور درخواست کننده به دست آمده اند.

نقطه ضعف دیگر این است که احتمالاً داده های قابل بازیابی به مراتب کمتری برای استخراج وجود دارند. در واقع، اگر یک مظنون یک ماشین مجازی موقت ایجاد کرده تا جنایات خود را مرتکب شود و آن دستگاه را حذف کند، ممکن است هیچ مدرکی برای بازیابی ممکن است وجود نداشته باشد.

امکان دستیابی و تجزیه و تحلیل داده های ذخیره شده از راه دور به قانون و قضاوت آن بستگی دارد. به عنوان مثال، در بعضی از حوزه های قضایی، به منظور دستیابی به داده ها، بررسی کننده تحت شرایطی خاص مجاز است با استفاده از اعتبار مظنونین به کامپیوتر راه دور متصل شود. سایر حوزه های قضایی ممکن است چنین دستیابی را قبول نکنند. در این موارد، از کانالهای رسمی می توان برای درخواست حفظ و دسترسی به داده ها از ارائه دهنده استفاده کرد.

ث. حافظه رایانه ای (RAM)

هنگامی که حافظه رایانه در حالی که رایانه ضبط شده هنوز کار می کند، استفاده شود، می توان آنرا در DFL تحلیل کرد. شناخت ساختارهای حافظه سیستم عامل های مختلف به منظور تجزیه و تحلیل حافظه و تخلیه حافظه، مهارت های بسیار بالا و فنی را می طلبد، بنابراین فقط یک بررسی کننده مجرب باید کار را انجام دهد. برای تجزیه و تحلیل حافظه نرم افزار خاصی لازم است. نمونه هایی از این موارد Volatility و Rekall هستند که بصورت رایگان در اینترنت در دسترس عموم هستند.

بخش های مصنوعی معمولی که می توانند از زباله های حافظه استخراج شوند عبارتند از:

* فرآیندهای در حال اجرا، از جمله حافظه آنها
* اطلاعات فرآیند (به عنوان مثال دسته ها)
* کلیدهای رمزگذاری
* فایل های باز
* نام کاربری، کلمه عبور
* اسناد ذخیره نشده

۵.۳.۱.۳- مجازی سازی

یک تصویر بیشتر از هزار کلمه ارزش دارد - این موضوع مخصوصاً برای مجازی سازی صادق است. با استفاده از مجازی سازی، بررسی کننده می تواند محیط سیستم عامل یک شاهد را به همان روشی که مظنون آن را دیده است، مشاهده

کند. پیدا کردن شواهد از درون یک ماشین مجازی، گاهی اوقات می تواند سریع تر از تجدید ارتباط آثار داده از فایل تصویری باشد. نمونه آن مشاهده نرم افزار بازی های تقلبی است.
هنگام نصب یک تصویر، باید آن را با محافظت از نوشتن نصب کنید یا فقط پارامترهایی را با حافظه نهان نوشتن بخوانید، به سیستم عامل مجازی اجازه می دهد فایل های لاگ را بنویسد، بدون اینکه روی یکپارچگی فایل تصویر تأثیر بگذارد.
برخی از سیستم عامل ها از شروع به کار در محیط های مجازی امتناع می ورزند. این امر به طور معمول با جایگزینی برخی از درایورها و با پیکربندی تنظیمات سیستم، با استفاده از نرم افزارهایی مانند OpenGates و OpenJobs قابل حل است. اگر سیستم عامل مجازی با یک رمزعبور شروع شود، بررسی کننده باید رمز عبور را کرک کند یا آن را حذف کند.

۵.۳.۱.۴- فرآیند دستیابی به داده های جمعی

برخی موارد شامل تعداد زیادی رایانه با انبوه داده ها هستند. برای اجرای وظیفه جرمیابی، برای تسریع کار باید یک استراتژی اجرا شود. یک راه برای انجام این کار جدا کردن کار تجزیه و تحلیل جرمیابی از وظیفه تحلیل محتوا است.
بررسی کنندگان بر روی کارهای تجزیه و تحلیل جرمیابی مانند بازیابی، تجزیه، نصب و پردازش شاهد ها تمرکز می کنند، در حالی که بازپرس ها با دانش خاص موردی، تجزیه و تحلیل محتوا را انجام می دهند.
برای اطمینان از عملکرد مناسب ممکن است فرآیندهای مناسب برای رسیدگی و مشاهده فایل های استخراج شده نیاز به ایجاد و پیاده سازی بین بررسی کنندگان و بازپرس ها داشته باشند.
روش دیگر برای پردازش داده های جمعی، انجام تریاژ است. تریاژ در بخش ۵.۲.۲ در این سند توضیح داده شده است.

۵.۳.۱.۵ کمک های مجازی سازی

برای کمک به درک داده ها و جریان های پیچیده، کمک به مجازی سازی می تواند مفید باشد. برخی از نمونه های این گونه کمک ها عبارتند از:

جدول ۱۰. روش کمکی های بصری

خطوط زمانی	آنها می توانند برای نمایش رفتار کاربر استفاده شوند، زمانی که فرد مظنون وارد می شود، زمانی که او به یک رسانه خاص متصل می شود، زمانی که او به یک روتر بی سیم خاص وصل می شود و زمانی که او یک وب سایت خاص را مشاهده می کند.
نمودارهای رابطه	اینها می توانند پاسخ هایی به پرسش هایی از این قبیل بدهند: چه کسی با چه کسی ملاقات کرده است؟ در چه زمانی؟ با استفاده از چه واسطه ای؟ چه اطلاعاتی ارسال / دریافت شده است؟ چه کسی چه چیزی را می داند؟ مظنون اصلی کیست؟
نمودارهای جریان پول	اینها می توانند کمک کنند به درک اینکه در چه نقطه ای از زمان یک میزان حافظه ارسال شده است و از طریق چه کانالی و توسط چه افرادی؟
نمودارهای ارتباطات	همانند نمودار رابطه است، اما آنها حتما شامل افراد نیستند. آنها می توانند نشان دهند اغلب چه مواقعی آدرس های IP خاص به سرورهای خاص از کشورهای متفاوت حمله می کنند.

بازنمودهای گرافیکی درک ارتباط بین داده ها را آسان تر می کنند. آنها همچنین می توانند بررسی کننده را قادر سازند تا روابط جدیدی را که قبلاً ذکر نشده بود، پیدا کند. معمولاً مبنای چنین نمودارهایی داده های خام هستند که به صورت

ساختاری ذخیره می شوند، به عنوان مثال در قالب CSV، TSV یا XML. این فایل ها در نرم افزار تحلیلی بارگذاری می شوند.

به عنوان مثال در لینوکس، دستورات ساده ای مانند *sort*، *awk* و *uniq* که در رابطه با *Graphviz* یا *dot* استفاده می شوند، می توانند به ترسیم نمایش های گرافیکی کمک کنند.

۵.۳.۲ تجزیه و تحلیل دستگاه های تلفن همراه

دستگاه های تلفن همراه حاوی سوابق و سیاهه های مربوط به ارتباطات، همراه با زمان و تاریخ ارتباطات خاص هستند. علاوه بر این، دستگاه های تلفن همراه ممکن است حاوی فایل های رسانه ای و مکان GPS باشند.

۵.۳.۲.۱ دسته بندی آثار دیجیتال

ردپای دیجیتالی موجود در دستگاه های تلفن همراه را می توان به سه گروه متمایز تقسیم کرد: داده های ارتباطی، فایل های رسانه ای و سایر داده ها. داده های ارتباطی می توانند شامل سوابق مکالمه، پیام های ها و سایر پیام های خدمات پیام رسانی باشند. فایل های رسانه ای، مانند رایانه ها، می توانند حاوی اطلاعاتی فراتر از آنچه توسط فایل به تصویر کشیده شده است باشند. به عنوان مثال، ابرداده روی فایل های رسانه ای ضبط شده در تلفن همراه، حاوی عنوان های جغرافیایی یا سایر اطلاعات مفید مکان و اطلاعات شناسایی تعبیه شده در خود فایل است.

۵.۳.۲.۲ رویه ها برای آثار مختلف

بخش های زیر انواع داده هایی را که می توان از دستگاه تلفن همراه استخراج کرد، توضیح می دهند.

الف. تاریخچه تماس

تاریخچه تماس قبل از دستیابی به دستگاه تلفن هوشمند، از فعالیت مکالمه مالک می تواند اطلاعاتی را ارائه دهد. بررسی کننده می تواند تماس های دریافتی، خروجی و از دست رفته شامل زمان و مدت زمان را مشاهده کند. این امر می تواند به بررسی کننده جرمیابی کمک کند تا نتیجه ای غیرمستقیم در مورد فعالیت های مشکوک به دست آورد، بنابراین DFL را در تسریع در روند تجزیه و تحلیل با ارائه یک فایل مختصر و روشن کمک می کند.

ب. لیست تماس

لیست تماس نه تنها نام مخاطب را ارائه می دهد، بلکه به طور بالقوه همچنین شماره خانه، شماره تلفن همراه و شماره کار را نیز ارائه می دهد. انواع دیگر اطلاعات از قبیل عنوان مخاطب، شرکت، آدرس و ایمیل های مرتبط نیز می توانند از لیست تماس استخراج شوند. برخی از دستگاه های تلفن هوشمند تصویری از مخاطب را در لیست تماس ذخیره می کنند که می تواند در شناسایی یک فرد خاص کمک کند. اطلاعات ذخیره شده در لیست تماس، روابط اجتماعی و کاری صاحب دستگاه گوشی هوشمند را در اختیار بررسی کننده قرار می دهد. علاوه بر این، بسیاری از افراد انواع مختلفی از اطلاعات حساب و کلمه عبور را در لیست مخاطبین ذخیره می کنند.

ج. پیام های متنی و ایمیل

برخلاف سابقه تماس و لیست تماس، که اطلاعات غیرمستقیم را ارائه می دهند، پیام های متنی و نامه های الکترونیکی اطلاعات صریح و روشن را ارائه می دهند که می تواند به عنوان مدرک در دادگاه استفاده شود. این بدان دلیل است که آنها حاوی متن دقیقی هستند که توسط کاربر دستگاه در نظر گرفته شده / ارسال و دریافت شده باشد.

د. فایل رسانه ای (تصاویر، فیلم ها، صدا)

از فایل های رسانه ای مانند تصاویر، فیلم ها و فایل های صوتی می توان به عنوان شواهد بالقوه دیجیتالی در دادگاه استفاده کرد. بسیاری از دستگاه های هوشمند مانند آیفون مختصات GPS را در محل فوق داده با نام Exchangeable File Format (EXIF) تصاویر تعبیه می کنند. سایر اطلاعات تعبیه شده در داده های EXIF می تواند شامل نام تجاری تلفن هوشمند، تاریخ و زمان گرفتن عکس ها و همچنین نرم افزاری باشند که در صورت وجود، برای تغییر تصویر استفاده می شود. این امر به بررسی کننده بینش بیشتری نسبت به فعالیت های صاحب تلفن هوشمند می دهد.

و. تاریخچه مرور اینترنت و جستجوی کلمات کلیدی

تاریخچه مرور اینترنت و جستجوی کلید واژه های انجام شده در دستگاه تلفن هوشمند، به بررسی کننده درک کلی از فعالیت های اینترنتی مالک می دهد. بررسی کننده انواع وب سایت هایی را که مالک بازدید کرده است و تا حدی سایت های مورد علاقه کاربر را کشف می کند.

ه. لیست های مربوط به چت و برنامه های پیام رسانی

چندین برنامه چت و برنامه پیام رسانی در دسترس است. به عنوان مثال می توان به ،Whatsapp ،Telegram ،Google Talk ،Windows Live Messenger ،QQ ،WeChat ،Weebo ،Line ،Skype و BlackBerry اشاره کرد. کاربران این برنامه ها معمولاً برای ذخیره اطلاعات از چت استفاده می کنند. از جلسات چت می توان به عنوان شواهدی دیجیتالی در دادگاه در مورد آنچه صاحب به دیگران ارتباط برقرار کرده استفاده کرد. برخی از سیاهه های مربوط به چت در فضای ذخیره سازی ابری یا محلی مانند رایانه پشتیبان تهیه می شوند، بنابراین تجزیه و تحلیل رایانه ممکن است برای به دست آوردن اطلاعات بیشتر مفید باشد.

برنامه های پیام رسانی همچنین می توانند سرویس VoIP (Voice over IP) را ارائه دهند. این امکان را به صاحب تلفن هوشمند می دهد تا با بسیاری از افراد با استفاده از پروتکل IP ارتباط برقرار کند، بدون آنکه سابقه ای در سابقه تماس دستگاه داشته باشد. مظنون ممکن است از این نرم افزار برای برقراری ارتباط با یک بزهکار یا یک قربانی استفاده کند. به عنوان مثال، در موارد کودک آزاری، مجرم ممکن است با استفاده از این برنامه های پیام رسانی با کودک ارتباط برقرار کند.

ن. حساب های شبکه اجتماعی

حساب های شبکه های اجتماعی مانند اینستاگرام، فیس بوک، توییتر و وبلاگ Tumblr اعتبار کاربران کاربر را در خود دستگاه ذخیره می کنند. با ذخیره اعتبارنامه به صورت محلی، کاربران لازم نیست هر بار که می خواهند از این سایت ها بازدید کنند، وارد سیستم شوند. این اعتبارات برای بررسی کننده بسیار ارزشمند هستند، زیرا می تواند برای دستیابی به حساب رسانه های اجتماعی مظنون استفاده شود، و این امکان را می دهد که داده ها از دستگاه استخراج شوند.

بسیاری از داده ها در حساب های رسانه های اجتماعی، لیست های تماس، پیام های بین افراد و گروه ها، تصاویر، فیلم ها، فعالیت کاربر ذخیره می شوند - لیست بی پایان است. به منظور استخراج داده های صحیح و نتایج حاصل از تجزیه و تحلیل به طور کامل و مختصر در گزارش های جرمیابی، باید بررسی کننده فایل واضح ارائه دهد.

ت. تقویم و یادداشت ها

تقویم تصویری از فعالیتهای برنامه ریزی شده قبلی، فعلی و آینده صاحب تلفن هوشمند ارائه می دهد. از این تقویم می توان برای ارتباط دادن صاحب تلفن هوشمند با مکان ها و زمان های خاص استفاده کرد تا به دنبال شهود احتمالی باشد. همچنین ممکن است صاحب تلفن هوشمند یادداشت هایی را ذخیره کند که دارای اطلاعات ارزشمندی است که می تواند به عنوان مدرک در دادگاه ارائه شود.

ث. اتصالات (شبکه تلفن همراه، Wi-Fi، بلوتوث)

این موارد به بررسی کننده امکان می دهند فعالیت های شبکه که توسط دستگاه تلفن هوشمند مالک انجام شده است را بررسی کند. شبکه تلفن همراه تصویری را نشان می دهد که مالک در کدام کشور یا منطقه قرار گرفته است. Wi-Fi تصویری را ارائه می دهد که شبکه محلی (LAN) تلفن های هوشمند به آن متصل شده است. اتصالات بلوتوث درمورد نام مستعار دستگاههایی که با مالک تلفن هوشمند در ارتباط بوده اند به بررسی کننده می دهد.

ر. نقشه ها (مکان ها، راهنما، موارد دلخواه)

این موضوع به یک بررسی کننده جغرافیایی از حرکت مالک می دهد که می تواند به عنوان شواهد بالقوه در دادگاه از آن استفاده کند. مختصات GPS از حرکات کاربر نیز می تواند ضبط و تجزیه و تحلیل شود، مانند مواردی که برنامه های کاربردی ارائه می دهند. این موارد شامل Bings Maps ،Google Maps و Apple Maps است.

ز. نرم افزار (پردازش اسناد، PDF، و غیره)

اکثر تلفن های هوشمند ویژگی ایجاد و ویرایش اسناد را ارائه می دهند. نرم افزار پردازش اسناد مانند Word To Go و Sheet To Go ممکن است حاوی شواهد احتمالی مربوط به این فایل باشد.

۵.۴ ارائه (اسلاید)

مرحله ارائه (اسلاید) مستلزم جمع آوری یافته ها به روشی جالب و قابل فهم برای ذی نفعان است. پس از اتمام مرحله تجزیه و تحلیل، بررسی کننده باید یافته ها و نتایج را در گزارش جرمیابی ارائه دهد. بررسی کننده باید زمینه های پیچیده فنی را به واقعیت هایی نشان دهد که قضات، دادستان ها و سایر طرفهای درگیر آن به راحتی می توانند درک کنند. همچنین از آنها انتظار می رود که این حقایق را تفسیر کرده و نظر خود را در مورد معنای آنها ابراز کنند. در مواردی که تعداد زیادی از شاهد ها مورد تجزیه و تحلیل قرار می گیرند، ارائه بررسی کننده برای تیم دشوار خواهد بود. توصیه می شود برای تسهیل تطبیق شواهد دیجیتالی با داده های دیگر از تحقیقات، یک نرم افزار تحلیلی استفاده کنید. از این نوع ابزارها همچنین می توان برای نمایه سازی و جستجوی کلیه شاهد ها استفاده کرد و یک بررسی کلی از فایل در اختیار تیم تحقیق قرار داد.

۵.۴.۱ قابل قبول بودن شواهد الکترونیکی

ضوابط پذیرش شواهد الکترونیکی ممکن است از یک دادگاه به دیگری متفاوت باشند. به طور کلی، بررسی کننده هنگام ارزیابی شواهد الکترونیکی برای دادگاه باید معیارهای زیر را در نظر بگیرد:

جدول ۱۱- معیارهای عمومی برای پذیرش شواهد الکترونیکی

صحت	شاهد باید حقایق را به صورتی ارائه دهد که قابل بحث نباشد و نماینده حالت اصلی آن باشد.
کامل بودن	تحلیل بر اساس شاهد باید همه چیز را نشان دهد و نتیجه مطلوب را به دست دهد.
قابلیت اعتماد	شاهد نباید هیچ شکی باقی بگذارد که داده های جمع شده صحت و دقیق هستند.
متقاعد کردن	شاهد باید متقاعد کننده باشد بر اساس حقایقی که آن ارائه می دهد و باید قادر باشد ذی نفع را برای حقیقت آن در دادگاه متقاعد کند.
تناسب	روش های مورد استفاده برای جمع آوری شاهد باید عادلانه و متناسب با زمینه های قضایی باشند: پیش داوری (برای مثال سطح نفوذ یا اجبار) بر اساس حقایق مرتبط با هر یک از طرفین نباید بر ارزش شاهد تاثیر گذار باشد (برای مثال ارزش آن برای اثبات).

۵.۴.۲ نوشتن گزارش

گزارش جرمیابی باید به زبان روشن و قابل فهم نوشته شود. نتیجه باید به طور خلاصه نوشته شود و همچنین باید پاسخ مختصر به درخواست فایل، ارائه شده توسط درخواست کننده ارائه دهد.

توصیه می شود به جای قرار دادن مطالب اصلی، کلیه مشخصات فنی در بخش پیوست ذکر شده باشند. این امر به منظور تسهیل درک در خواندن گزارش است.

بررسی کننده همچنین باید از ارائه گزارشی که اثبات نشده است خودداری کند. به عنوان مثال، "مظنون فایل A را تغییر داده است". یک جمله مناسب می تواند "فایل A موجود در رایانه B تغییر یافته است" باشد.

یک نیاز مشترک برای گزارش جرمیابی در پیوست J موجود است: الزام مشترک گزارش جرمیابی این سند.

با توجه به پیچیدگی یک موضوع، برای بررسی کننده بیان یافته ها در گزارش مشکل است. استفاده از وسایل دیداری و نمایش های بصری مانند انیمیشن، اسلایدها، تصاویر و نمایش های زنده روش های خوبی برای تسهیل درک هستند.

۵.۴.۳ شاهد خبره

در برخی از حوزه های قضایی، یک گزارش جرمیابی ارائه شده برای ارائه در دادگاه برای بررسی کننده کافی است. اما در سایر حوزه های قضایی، بررسی کننده موظف است در جلسه دادگاه شرکت کند و شهادت کارشناسی خود را در رابطه با موضوع ارائه دهد.

شاهد خبره شخصی است که به واسطه آموزش، مهارت و یا تجربه، فراتر از حد متوسط افراد، دارای تخصص و دانش تخصصی است. دانش شاهد کافی است که دیگران بتوانند به طور رسمی و قانونی به نظر تخصصی (علمی، فنی یا موارد دیگر) وی درباره شواهد یا واقعیتی در محدوده تخصص خود، که به آن نظر کارشناس گفته می شود، اعتماد کنند.

در بعضی از حوزه های قضایی، وضعیت کارشناسی در مورد هر موضوع توسط قاضی دادگاه تصمیم گیری می شود و شخص فقط یک متخصص در آن موضوع است. در سایر حوزه های قضایی، کارشناس توسط موسسه حقوقی منصوب می شود و شخص مسئولیت هر موضوعی را در تخصص خود دارد.

حقوق و وظایف یک شاهد خبره از کشوری به کشور دیگر متفاوت است. برای بررسی کنندگان مهم است که خود را با قوانین، رویه های دادگاه، نقش و حقوق و وظایف خود در آن نقش آشنا کنند.

۶- تضمین کیفیت

هنگام اقامه اخبار جرم در دادگاه، کاوشگر تنها نه فقط نیاز به تفسیر پروسه آنالیز دارند. آنها همچنین نیاز خواهند داشت که تخصص خود، تجهیزات مورد استفاده خود، روش انتخابی خود، روش سروکار داشتن با اسناد و عوامل بیشتر در آن را تفسیر کنند. مهم است که روندهای به خدمت گرفتن موارد بالا در آزمایشگاه جرائم دیجیتال دایر و اجرا شود. بخش پیش رو اجزا بیشتری را توضیح می دهد بعلاوه اعتبار سنجی آن می بایست بدست آید.

۶-۱ مولفه های تضمین کیفیت

تضمین کیفیت اولیه ایکه در آزمایشگاه جرائم دیجیتال اجرا میشود شامل اما محدود به آنها نمیشود:

	چک لیست مربوط به اجزا تضمین کیفیت
آزمایشگاه	الف. ایجاد یک چارت سازمانی در سطح آزمایشگاه و سطح سازمان. ب. انجام ممیزی داخلی سالانه. ج. ایجاد یک رویه برای بررسی شکایت های داخلی و خارجی. د. انجام یک روش برای کنترل جمع آوری اسناد.
شرایط محیطی و تسهیلاتی	الف. ایجاد محوطه های آزمایشگاه- ورود و خروجی ها ب. تهیه لیستی از دسترسی و عدم دسترسی با کلید، کارتهای شخصی هویتی یا وسائل بیومتریک. ج. کنترل مرتب محیط آزمایشگاه – دما، رطوبت، پاکیزگی. د. تهیه برنامه امنیتی و سلامتی. ه- تهیه سیاست بازدید کننده. و- تهیه مرتب برنامه آزمایشگاه داری.
تجهیزات	الف. تهیه یک رویه برای اداره کردن، حمل و نقل، ذخیره سازی، استفاده، تعمیر،ترتیب و برنامه نگهداری تجهیزات. ب. قبل از کاربرد مطمئن شوید که تجهیزات بر اساس مشخصات کار می کنند. ج. اجرا برنامه نگهداری د. به روز نگاه داشتن لوازم آتش نشانی بر اساس الزامات و- نگهداری تجهیزات جمع آوری اسناد، کتب راهنما و ضمانت ها.
کارمندان	الف. صلاحیت های شغلی: -بررسی سابقه پیش از به خدمت گرفتن. -تهیه وظایف شغلی برای کارمندان به محض به کارگیری – بخش ۳.۳ را نگاه کنید. ب. توسعه شغلی و آموزشی: - ایجاد برنامه آموزشی برای کارمندان- بخش ۳.۳.۴ توسعه کارمندان را نگاه کنید. - کارمندان را برای آموزش روانه کنید. - به کارگیری مربیان برای کارمندان تازه استخدام شده. - ارزیابی صلاحیت کارمندان موجود با انجام آزمون های صلاحیت برای کارمندان تازه به خدمت گرفته.

	- شرکت در آزمون های متخصصی درون و برون آزمایشگاهی - به دست آوردن مجوزهای تکنیکی. انجام یک برنامه آموزشی مداوم برای کارمندان موجود برای حفظ مهارت.
روش جرم شناسی	الف. تهیه انگیزه نامه برای انجام بررسی های جرائم دیجیتالی ب. نگهداری یک سند از روش های جرم مانند جمع آوری داده ها به شکل زنده، به روز شده و در دسترس برای کاوشگر. ج. انجام تاییدیه برای روش های معرفی شده جهت حصول اطمینان از کاربرد صحیح آنها به توسط آزمایشگاه جرائم دیجیتال. د. انجام اعتبار به هنگام استفاده از هر روش: روش غیر استاندارد، روش منحصر به آزمایشگاه یا روش استاندارد خارج از حیطه آزمایشگاه. و. برای سهولت در عملیات از روش پذیرفته شده بین المللی مانند SWGDE استفاده کردن.
درخواست خدمات	پایه ریزی و راه اندازی یک سیاست و رویه در درخواست خدمات. که شامل: الف. روند پذیرش یا عدم پذیرش درخواست. ب. روند باز تسلیم درخواست. ج. نیاز داشتن به یک درخواست دقیق یا مورد عینی. د. قدردانی رسمی از درخواست کننده و کاوشگر، نشانه این است که هر دو طرفین موافق با کار کردن قبل از شروع انجام کار ادله قانونی و پس از تحویل دادن آن بوسیله امضا یک فرم، پاسخ به یک ایمیل یا پاسخ به یک نامه است. و. فرم ها یا دیگر روش های کاربردی برای مستند کردن درخواست. رجوع به پیوست ل: فرم درخواست خدمات آزمایشگاه جرائم دیجیتال اینترپل برای یک نمونه از فرم درخواست.
بررسی مدرک	ایجاد و راه اندازی سیاست و رویه ایی برای بررسی سند. شامل: الف. محافظت از سند ب.برچسب زنی مدرک ج. بسته بندی مدرک د. موارد سند سازی- شامل زنجیره توقیف و. مدرکی که بدون مراقبت باقی مانده است ه. احتیاطاط امنیتی و بررسی مدرک ی. ذخیره و ضبط پیوست ذ را نگاه کنید: بررسی مدرک الکترونیک برای جزئیات بررسی مدرک.
نتایج یافتن ادله قانونی	الف. نگاه داشتن اسناد تکنیکی برای تایید نتایج ادله قانونی. اسناد می بایست دلالت بر روند و تاریخ انجام آن توسط کاوشگر باشد. اصلاحات اسناد پیشین می بایست دنبال شود.

	ب. انجام بررسی تکنیکی و مدیریتی نتایج جستجو ادله. ج. تصویب نتایج حاصل از جستجو پیش از در اختیار گذاشتن آن برای درخواست کننده. پیوست د را ببینید: نیاز متداول در گزارش قانونی د. هنگام ارائه یک نظر میبایست به صورت روشن در گزارش قانونی مشخص شود. و. پایه ریزی یک روند برای اصلاح یک گزارش قانونی.

جدول ۱۲. چک لیست اجزا تضمین کیفیت

۶.۲ اعتبار سنجی آزمایشگاه

نتایج یافتن ادله قانونی بر نظام قضایی تاثیر می گذارد، در نتیجه باید درست و قابل اعتماد باشد.
آزمایشگاه می تواند اعتماد به نتایج یافتن ادله قانونی را با پیوستن به برنامه اعتبارسنجی تضمین نماید. بدنه اعتبار سنجی پروسه آزمایشگاه را بصورت سالانه ارزیابی کرده تا از تطابق با استاندارد جهانی اطمینان حاصل کند.
اگرچه بهره مندی از اعتبارسنجی توصیه میشود، بصورت کلی در بسیاری از کشورها بصورت داوطلبانه انجام میشود نه بصورت اجباری. یک آزمایشگاه که به برنامه اعتبار سنجی جهت جزئیات روند علاقمند است ممکن است به بدنه اعتبارسنجی کشور خود مراجعه کند.

مزایای اعتبار سنجی آزمایشگاه	
۱	**نتایج اعتماد به نتایج ادله یابی قانونی** هنگامیکه یک آزمایشگاه موارد گسترده ایی در سال دریافت می کند، عموما برای آزمایشگاه مشکل است که عملکرد فعالیت جرمیابی و کاوشگر ها را نشان دهد. استاندارد ایزو ۱۷۰۲۵ پروسه نظارت بر جنبه های کیفیت نتایج یافتن جرائم را توضیح می دهد. با اعتبار سنجی، این پروسه به صورت سالانه ارزیابی میشود تا از باقی ماندن عملکرد بالا در آنها مطمئن شود. بعلاوه پروسه مدیریت و آزمودن مدرک می بایست بر اساس استانداردهای جهانی باشد، تا برای ذینفع های نتایج حاصل شده در آزمایشگاه اعتماد بوجود آورد.
۲	**سیستماتیک بیشتر با پروسه های استاندارد شده** یک آزمایشگاه با چندین کاوشگر می بایست از دنبال کردن مجموعه روندها توسط آنها اطمینان حاصل کند. این مورد شهادت بوسیله هر کاوشگریی که از همان آزمایشگاه آمده است را در دادگاه تضمین می کند که منسجم و اصولی است. بنابراین فهم سریع توسط کاوشگرها، قاضی ها و دیگر کارمندان دادگاه را راحت می کند. داشتن همچین اعتبار سنجی در جایگاه خود استانداردهای لازم در آزمایشگاه را پایه یزی کرده و از پیاده سازی آنها توسط کاوشگرها اطمینان کسب می کند.
۳	**تولید نتایج کیفی** یکی از الزامات در ایزو ۱۷۰۲۵ ایجاد توسعه های مستمر در روندهای آزمایشگاهی است. آزمایشگاه جرائم دیجیتال از اعتبارسنجی می تواند بوسیله پایه ریزی پیشرفت های مستمر بهره برده و اطمینان دهد که آزمایشگاه نتایج کیفی تری را تولید می کند. یک نمونه از چنین پایه ریزی هایی نظارت شهادت در دادگاه می باشد. کاوشگر ها قادرند بصورت مستمر و پیوسته شیوه های ارائه نتایج را در دادگاه بهبود بخشند در حالیکه مورد نظارت قرار بگیرند و بازخوردهای سازنده دریافت کنند.

جدول شماره ۱۳. مزایای اعتبار سنجی آزمایشگاه

۷. نتیجه/جمع بندی

مدارک الکترونیکی به جهت ماهیت آن که منحصر به فرد و متفاوت از انواع سنتی مدارک است چالش های جدیدی را در تفتیش و بررسی موارد خاص بوجود آورده. بنابراین، می بایست با ملاحظه لازم بررسی شود. هدف این سند فراهم کردن راهبردهای استاندارد برای مدیریت یک آزمایشگاه و بررسی مدرک الکترونیک است. این مهم دیگر کشورها را متقاعد می کند که مدرک الکترونیک و نتایج بدست آمده توسط کشورهای عضو اینترپل قابل قبول هستند.
کاوشگر و مدیریت آزمایشگاه همیشه می بایست سعی کنند که روش شناسی، راهبردها و رویه های با پیشرفتهای کنونی در تکنولوژی را به روز گردانند. تنها زمانی است که ما با هم می توانیم شدت جرائم را کاهش دهیم و به عدالت چنان که باید خدمت شود خدمت برسانیم.

۸. پیوست ها

پیوست الف

عوامل زیر توصیه هایی است برای مجموعه مهارت های کاوشگر آزمایشگاه. خواننده می بایست توجه کند که لیست جامع نبوده و نیاز دارد که به روز شود.

دسته	موضوع	مجموعه مهارت
بنیاد	**بنیاد کامپیوتر**	سازمان کامپیوتر، چگونه کامپیوتر داده ها را نگاه می دارد، بیت ها، بایت، تکامل رسانه های دیجیتال و سیستم های نگهداری
	سیستم پرونده	اعشاری، شانزده شماری، دودویی، ترتیب ذخیره کوچک، ترتیب ذخیره بزرگ، بخش ها، دسته ها، اسلک اسپیس، ابر داده ها، داده ها، FAT، NTFS، EXT،HFS.
	معرفی کاوشگریی و جرائم دیجیتال	اجرا قانون و مقررات، معرفی علم جرم شناسی، مدرک الکترونیک و ماهیت آن، دسته مدارک الکترونیک، روش شناسی، واژه شناسی جرائم
شناسایی	**جمع آوری اطلاعات**	جمع آوری مورد به صورت آنلاین، واقعیت های جمع آوری شده
جمع آوری و بررسی	**جمع آوری و بررسی**	وظایف پاسخگو اولیه و رویه عملکرد استاندارد، بدست آوردن اطلاعات بصورت زنده و غیر زنده، انتخاب بهترین روش کسب داده، روش تریاژ(ارجحیت داده ها)، وسیله تریاژ.
آنالیز	**بازیابی داده ها**	تکنولوژی نگهداری، نشانه های هارد دیسک و فلش آسیب دیده، بازیابی فیزیکی و منطقی، وسایل بازیابی داده ها، بازیابی وسایل استفاده کننده از داده ها.
	کامپیوتر جرم	تکنولوژی سیستم های عامل، ابر داده ها،دفتر ثبت، محصول مصنوعی،استخراج داده، آنالیز داده، تکنیک پنهان سازی داده،تحلیل مجمو داده های بزرگ، آنالیز حافظه.
	موبایل جهت جرم شناسی	تحول و تکنولوژی موبایل، کاربر، تکنولوژی پشتیبان مخابرات،انواع داده، وسایل جمع آوری و آنالیز، حراست از داده.
	شبکه جهت جرم شناسی	انواع شبکه، کوکی ها و فایل های تاریخی اینترنت، اعتبارنامه کاربر،وسایل شبکه جرم شناسی، بسته های مطالعه.
	صدا، ویدئو و عکس جرم شناسی	فهم تکنولوژی، افزایش، سندیت پرونده، مقایسه
	ظهور تکنولوژی	فهم تکنولوژی، دسترسی به داده از وسیله، استخراج داده، -جرم مربوط به شبکه مجازی -جرم مربوط به پایگاه داده

		-جرم مربوط به پهباد -جرم مربوط به وسیله نقلیه -جرائم مربوط به کشتی -جرائم پول پنهانی -جرائم بیومتریک
ارائه	**گزارش کتبی**	فرمت گزارش، نمایش موثر نتایج به ذی نفع
	دادگاه قضایی و ساختگی	قوانین مرتبط با مورد،قانون بین المللی، مشارکت بین المللی، ارائه شهادت متخصص در دادگاه، معرفی با ساختار دادگاه، تسلیم مدارک الکترونیکی در دادگاه.
رسوم	**رسوم**	دستورالعمل حرفه ایی رفتار، دستورالعمل رفتاری غیر اخلاقی
	مدیریت کیفی	فهم استانداردها، اداره کردن بررسی، سیستم مدیریت کیفی.
	سلامت و امنیت	شناسایی خطرات، اندازه گیری سلامت و امنیت، خود حفاظتی

پیوست ب: چک لیست تجهیزات ابتدایی آزمایشگاه

عوامل ذیل لیست پیشنهادی از تجهیزات ابتدایی است که یک آزمایشگاه می بایست از آن برخوردار باشد. خواننده می بایست دقت داشته باشد که این لیست جامع نبوده و بر اساس ماهیت موارد دریافتی ممکن است به بیشتر از آن نیاز باشد.

شماره	مورد
۱	لپ تاپ
۲	نرم افزار آنالیز کامپیوتر
۳	نرم افزار بازیابی داده
۴	نرم افزار آنالیز موبایل
۵	نرم افزار آنالیز اینترنت
۶	نرم افزار ماشین مجازی
۷	سخت افزار عکس برداری
۸	سیستم لنگرگاه
۹	سیستم دسترسی به داده های دستگاه
۱۰	واسط با فضای خالی- جهت نگهداری مدارک الکترونیکی بدست آمده در دراز مدت و بلند مدت: -فلش -هارد دیسک اگسترنال -هارد دیسک -سرور
۱۱	ابزار کامپیوتر

۱۲	افزونه کابل قدرت
۱۳	پرینتر
۱۴	کاغذ خردکن

پیوست پ: نمونه فرم ثبت مورد

اطلاعات درخواستی آژانس	
نام:	دپارتمان/واحد:
عنوان شغلی:	آژانس:
شماره تماس:	شماره پرونده درخواست کننده:
ایمیل:	شماره پرونده آزمایشگاه جرم دیجیتال:

اطلاعات پرونده
سابقه پرونده
درخواست مخصوص پرونده
شرایط و ضوابط

۱- انتخاب روش: آزمایشگاه می بایست بهترین روش در دسترس را برای آنالیز جرائم دیجیتال انجام دهد.
۲- اظهارات سری: آزمایشگاه این اطمینان را می دهد که هر اطلاعات ارائه شده توسط درخواست کننده حاصل از انجام عملیات باید بصورت سخت ترین تدابیر سری رفتار شود.
۳- خطر یا از دست دادن سود: آزمایشگاه برای خطرات احتمالی مدرک یا از دست دادن منفعت صورت گرفته توسط درخواست کننده ناشی از عملیات انجام شده مسئول نمی باشد. اگرچه آزمایشگاه برای نگهداری مدرک بصورت سلامت در هر زمانی مسئول می باشد.
۴- مدرک غیر مدعی و رها شده: مدارک غیر مدعی یا رها شده در آزمایشگاه ظرف ۳۰ روز پس از ارتباط با درخواست کنندهبا صلاحدید آزمایشگاه معدوم خواهد شد. آزمایشگاه برای مدارک باقی مانده در مالکیتش پس از ۳۰ روز مسئول نبوده. پیش از معدوم کردن مدرک آزمایشگاه به درخواست کننده اطلاع می دهد.

درخواست کننده
آزمایشگاه
موارد بالا را خواندم و از شرایط اطلاع یافتم.
امضا
نام
تاریخ

پیوست ج: نمونه فرم ثبت مدرک

بخش الف: دریافت مدرک

شماره برچسب مدرک آزمایشگاه	تولید کننده	ظرفیت	توضیحات (شامل هر گونه عیب)	شماره سریال

درخواست کننده	آزمایشگاه
امضا فرستنده مدرک نام: تاریخ:	امضا نام: تاریخ:

بخش ب: تحویل مدرک

تمام مدارک لیست شده در بخش الف به اینجانب توسط آزمایشگاه عودت داده شد. با امضا ستون بالا دو طرف پذیرفتند که کار تمام شده و به اتمان رسید.

درخواست کننده	آزمایشگاه
امضا فرستنده مدرک نام: تاریخ:	امضا نام: تاریخ:

پیوست ث: نمونه بسته بندی مدرک

هارد دیسک در یک بسته پلاستیکی با برچسب امنیتی در دهانه کیف قرار داده شده است. کاوشگر اسم خود را بروی استیکر به همراه تاریخ و زمان بسته بندی مدرک می نویسد.

در این مورد، مدرک در یک کیف پلاستیکی با پوشش برچسب امنیتی گذاشته شده است. جزئیات مدرک، زنجیره مواردیکه باید بروی آن انجام شود مشخص است.

یادداشت های راهنما

اطلاعات پرونده

۱- شناسایی پروژه- به شماره ارجاع آن شی اشاره می کند.
۲- نام شی- اشاره به نام "کد" که توسط مدیر پروژه اختصاص داده میشود.
۳- نام متولی- به کاربر نهایی کامپیوتر اشاره می کند.
۴- رضایت- اگر رضایت برای ماشین لازم باشد، امضا تحویل دهنده ماشین گرفته شود.
۵- مدیر- اشاره به مدیر اختصاص داده شده برای پروژه که پرونده را رهبری می کند دارد.

اطلاعات کامپیوتر هدف

۶- محل سیستم- آدرس سایت، که ممکن است شامل شماره دفتر شود اگر مستقیما از یک دفتر گرفته شده باشد.

۷- نوع سیستم- دلالت بر این دارد که دستگاه یک دسکتاپ، لپ تاپ، سرور یا چیز دیگری است. اگرسیستم یک دستگاه مستقل است قسمت دیگر را علامت بزنید.

۸- نوع مدرک- نوع وسیله ایکه عکس یا کپی گرفته میشود.

۹- حالت سیستم- نشان دهنده این است که سیستم مورد ظن روشن، خاموش، لاگ آن یا غیره است. اگر سیستم روشن است مشخص کنید که چه شخصی آن را خاموش کرده است.

۱۰- زمان/تاریخ بایوس- اشاره به بایوس دستگاه مشکوک می کند.

۱۱- زمان/ تاریخ فعلی- اشاره به تاریخ و زمان کامپیوتر کاوشگر دارد.

۱۲- مجموع تعداد هارد درایوها در کامپیوتر- خود توصیف گر.

۱۳- هارد درایو توسط..... پاک شده- اشاره به این دارد که چه شخصی اجزا کامپیوتر را منفک کرده است.

۱۴- عکس های گرفته شده- لطفا مشخص کنید که عکس از کامپیوتر و هارد درایو گرفته شده یا خیر در صورتیکه پاسخ خیر است علت آن را بیان کنید.

کامپیوتر

۱۵- تولید کننده کامپیوتر هدف- نوع دستگاه و سایز هارد درایو

۱۶- شماره مدل- شماره مدل کامپیوتر

۱۷- شماره سریال- شماره سریال کامپیوتر.اگر بیشتر از یک شماره سریال در دستگاه وجود دارد آن را در هارد درایو یا وسیله دیگر کپی کنید.

۱۸- تولید کننده- نوع هارد درایو

۱۹- شماره مدل- شماره مدل هارد درایو

۲۰- شماره سریال- شماره سریال هارد درایو. اگر بیشتر از یک شمار سریال وجود دارد همه آنها را کپی کنید.

اطلاعات بدست آوردن

۲۱- بدست آمده توسط- اشاره به کاوشگری دارد که آن را بصورت فیزیکی بدست اورده است.

۲۲- محل عکسبرداری- اشاره به این مطلب دارد که در داخل سایت یا خارج از آن عکس گرفته شده است.

۲۳- روش بدست آوردن- اشاره به نوع نرم افزار برای عکس گرفتن وسیله دارد. بنویسید که از چه شماره ورژن سخت افزار استفاده شده.

۲۴- سخت افزار بدست آوردن- بوسیله چه سخت افزاری اطلاعات بدست آمده

۲۵- نوع مدرک- اشاره به درایوی دارد که عکس در آن قرار داده خواهد شد. نشان دهنده درایو لیبل، شماره سریال و شماره شناسایی دیسک درایو می باشد.

۲۶- سایز درایو- مجموع ظرفیت درایو را مشخص می کند به گیگابایت یا مگابایت

۲۷- سایز عکس- سایز عکس را به گیگابایت و مگابایت مشخص می کند.

۲۸- عکس تایید شده- هنگامیکه عکس کامل شده و تایید میشود. قسمت بله را علامت بزنید.

۲۹- خطا- بیانگر وجود خطا به هنگام روند تاییدیه می باشد. اگر وجود دارد خطا ها را در پشت برگ بنویسید.

۳۰- مقدار هش- ثبت مقدار هش بوجود آمده هنگام پروسه عکی برداری مطمئن شوید که مقدار هش تاییدیه و مقدار هش بدست آوردن با هم مطابقت داشته باشد.

پیوست ذ: بررسی مدرک الکترونیک

موارد ذیل پیشنهاد پایه برای بررسی مدرک الکترونیک می باشد.

چک لیست بررسی مدرک الکترونیک	
۱	**برچسب** • مدرک می بایست به خوبی به محض تحویل به آزمایشگاه لیبل زده شود. زدن برچسب بروی سند سخت است، آزمایشگاه می تواند برچسب را برروی بسته سند بچسباند. • لیبل می بایست بصورت کامل در مدت زمان حضورش در آزمایشگاه باقی بماند. • برچسب ها می بایست همچنین توانایی به تفضیل آوری اسناد فرعی همراه سند را داشته باشد مثلا: DFL-MP۰۱ یک گوشی و DFL-MP۰۱ برای سیمکارت موجود در گوشی.
۲	**بسته بندی** • سند می بایست با استفاده از یک ظرف مناسب بسته بندی شود. • ظرف می بایست قادر به باشد دسترسی به آن سند را قابل وصول سازد. • بسته توسط کاوشگر امضا شود و تاریخ زده شود. • هر زمان که به آن دسترسی صورت گرفت، شخصی که آن را انجام می دهد می بایست آن را مجدد بسته بندی کند، به محض اتمام پردازش، مهر و موم به امضا و تاریخ آن فرد شود.
۳	**مدرک** • ثبت دقیق سند الکترونیک می بایست انجام شود. موارد ثبت شده شامل انواع، شماره سریال، تولید کننده، هر گونه نقص و برچسب ها میشود. • لیست سیاهه مدرک در آزمایشگاه تشکیل میشود. • ثبت روند صورت گرفته برای جمع آوری داده ها برای هر قطعه از مدرک الکترونیک می بایست تشکیل شود. • حداقل آن می بایست شامل یک تاریخ، ابتدا اسم و برچسب باشد.
۴	**بدون مراقب رها نشود** • مدرکی که به خاطر عدم حضور کاوشگر یا به علت تمرکز بروی مدارک با اولویت بیشتر وارد چرخه بررسی نشده نمی بایست بدون مراقب رها شود. بدین ترتیب در محلی خارج از آزمایشگاه جهت دوری از آلودگی حفظ شود. • مدارک در هنگام پروسه جا به جایی بدون مراقب رها نشود

۵	**از منبع آلودگی به دور باشید** • مدارک الکترونیک به صورت مناسبی از محل آلوده به دور باشد. این منابع شامل: آب، گرما، رطوبت و میدان مغناطیسی است.
۶	**بایگانی** • مدرک الکترونیک می بایست در محل امن بادسترسی محدود نگهداری شود. • یک گزارش کامل و به روز از ورود و خروج اسناد از اتاق بایگانی تهیه شود.
۷	**حفظ و نگهداری** • یک کپی از سند اصلی الکترونیک به جهت حفظ یکپارچگی سند اصلی تهیه شود. • مقدار هش سند اصلی و کپی آن می بایست یکی باشد • بررسی و آنالیز می بایست بروی کپی مدرک الکترونیک صورت گیرد.

پیوست ر: فرم درخواست سرویس آزمایشگاه جراتم دیجیتال اینترپل

فرم ۰۱: درخواست آزمایش جهت همکاری

از این فرم رسما به عنوان درخواست همکاری از آزمایشگاه اینترپل استفاده میشود. این فرم می بایست بصورت کامل توسط NCB پر شود. یک اژانس اجرا قوانین جنایی متفاوت توسط NCB مجاز دانسته میشود تا فرم را پر کند با این وجود این فرم توسط NCB به اینترپل ارسال میشود

اطلاعات در این فرم برای اینکه آزمایشگاه اینترپل قادر است که همکار تهیه کند مورد ارزیابی قرار میگیرد. اطلاعات جزئی تر در زمان پاسخگویی سر وقت داده خواهد شد.

در صورت داشتن هر گونه سوال اینترپل با شماره تماس شخص که در فرم آمده تماس خواهد گرفت.

عضو درخواست کننده	
کشور عضو اینترپل	
NCB	
عنوان/ رتبه شخص تماس گیرنده	
نام خوانوادگی	
نام	
آدرس ایمیل رسمی	
شماره تماس	
تصویب همکاری مستقیم با شماره آژانس	• بله، NCB در خصوص تمام موضوعات مرتبط با این درخواست مطلع میشود • بله، هماهنگی تنها با تماس آژانس • خیر، هماهنگی توسط NCB

آژانس تماس گیرنده *(اگر متفاوت از NCB باشد)*	
نام آژانس	
آدرس	
شماره دفتر	
عنوان/ سمت شخص تماس گرفته شده	
نام خانوادگی	
نام	
آدرس رسمی ایمیل	
شماره موبایل	

جزئیات مورد	
جرم اصلی	
مجازات محکومیت بر اساس قانون کشور عضو	
درگر کشورهای دخیل/ شخصیت بین المللی بزه	
مدرک مربوط به	*مشکوک * قربانی * شخص ذینفع. توضیح:

توضیح مختصری از پرونده	

دلایل درخواست آزمایشگاه اینترپل (هر خانه را در صورت درست بودن علامت بزنید)
• فقدان تخصص/ دانش • فقدان منابع/وجه مالی • فقدان تجهیزات/نرم افزار • غیره. لطفا مشخص کنید.

مدارک: عمومی	
آیا به ماموران اینترپل نیاز است که در مدارک مداخله	• بله

کنند	• خیر
اگر بله...	
۱- آیا مدارک "ارجینال" است یا "کپی". تا حد ممکن مدارک را به کپی محدود کنید	• اصلی • کپی
۲- آیا کارمندان اینترپل می بایست کشور عضو را برای همکاری ملاقات کنند؟	• بله • خیر
۳- جزئیات تماس فرد(افراد) کشور عضویکه طی همکاری حضور خواهند داشت. لطفا مستحضر باشید که اینترپل این فرد را برای انجام وظایف مورد نیاز اینجا و برای تهیه گزارش جهت استفاده کشور عضو هدایت و راهنمایی خواهد کرد.	• مانند آژانس تماس گیرنده • متفاوت- لطفا مشخص کنید:

لطفا ماهیت همیاری مورد نیاز را از جانب اینترپل مشخص سازید

- استخراج اطلاعات از مدارک.

لطفا اطلاعاتی که قرار است بدست آید را ذکر کنید(مورد درست را انتخاب کنید):

- عکس/ ویدئو: مربوط به:
- فایل: مربوط به:
- پیامک: مربوط به:
- جزئیات تکنیکی:
- غیره: لطفا مشخص کنید:

* نحوه اطلاعات بدست آمده از مدارک، استخراج به وسیله کشور عضو انجام میشود.
* اطلاعات در نرم افزار یا محصولات موجود برای انجام وظیفه بروی مدارک.

آن عمل یا وظیف چیست؟
(مثلا باز کردن یک موبایل قفل شده)
فقط نرم افزار پیشنهادی سورس باز/آزاد؟ بله () خیر( )
خوش آمد(شروع) نرم افزار پیشنهادی اختصاصی؟ بله( ) خیر( )

بررسی مدرک و ثبت مقدمات
اگر مدارک(شامل مدارک اصل) نیاز به بررسی باشد، لطفا دستورالعمل مربوط به زیر
۱- لطفا دستورالعمل های مشخص یا الزامات مورد نیاز در بررسی را مشخص کنید:
۲- لطفا فعالیتهای خاص یا روندهایی که نمی بایست انجام می گرفت را مشخص کنید:
۳- لطفا هر دستورالعمل خاص در خصوص ثبت روند همکاری ،قسمت های خاص مدرک، یا روند بدست آوردن داده ها را مشخص سازید:
۴- لطفا هر اطلاعات دیگری مربوط به همکاری را ارائه دهید):به عنوان مثال، آیا آن مدرک به صورت خاموش است؟آیا تلاش دیگری پیش از آن برای بدست آوردن اطلاعات انجام شد؟)
۵- اگر اینترپل شخص ثالثی را برای انجام همیاری مربوط به این درخواست ضروری در نظر بگیرد،مشروط به پذیرش هر دو NCB ،آیاNCB قبول می کند که بدنبال کشور عضو دیگری باشد،

ضمانتهای کشور عضو	
NCB و آژانس تماس گیرنده ضمانتهای ذیل را به اینترپل ارائه می کنند.	
این درخواست همیاری در مقایسه با قوانین کشور عضو، بین اللمللی و قوانین اینترپل قابل اجرا است؟	**بله( )**
به صورت خاص، بند ۳ از قانون اینترپل بیان می کند: شدیدا انجام هر گونه مداخله یا فعالیت سیاسی، نظامی، مذهبی یا نژادی برای سازمان نهی شده است. درخواست همکاری در اینجا به هیچ طریقی منجر به تجاوز به بند ۳ قانون اینترپل نمیشود.	**بله( )**
هیچ چیز در قوانین کشور عضو NCB یا آژانس تماس گیرنده را از بدست آوردن اطلاعات درخواستی بواسطه درخواست همکاری منع نمی کند.	**بله( )**
جرمی که بواسطه آن درخواست صورت گرفته، ارتباط بین المللی داشته و یک جرم جدی در قوانین کشور عضو در نظر گرفته میشود	**بله( )**
NCB و آژانس تماس گیرنده درک می کند که شروط همکاری با اینترپل مشمول انطباق این درخواست با هر معیار قابل اجرا در چارچوب قوانین، مقررات اینترپل است	**بله( )**
اگرهر اطلاعاتی که قرار باشد از مدارک بدست آید، NBC و آژانس تماس گیرنده تلاش می کنند تا درخواست استخراج از اطلاعات مربوط به جرم صورت گرفته را محدود کرده و آن را با هدفی که بدنبال آن استخراج است مطابقت دهند.	**بله( )**
اینترپل میبایست موافق با تامین کمکی است که در ذیل این درخواست آمده است. به این منظور آژانس تماس گیرنده /NCB می بایست پیش از فراهم شدن همکار، یک تفاهمنامه ارائه شده بوسیله اینترپل را امضا کرده.	**بله( )**
در مواقعیکه اثر متقابل برای مدارک الزامی باشد، اینترپل می بایست همیاری و راهنمایی به پرسنل کشور عضو منصوب شده رسانده تا درخواست را برای این درخواست به صورت خلاصه	**بله( )**

انجام دهند و گزارش بیشتری از آن را تهیه کنند.به جز موارد خاص که اینترپل آن را مدنظر قرار می دهد، استخراج در فقدان پرسنل کشور عضو انجام نخواهد شد.	
پرسنل همراه کشور عضو چه از آژانس تماس گیرنده باشد چه از NCB، می بایست تایید کند که در استخراج اطلاعات مربوطه از مدارک برای برخورداری از متخصصین اینترپل، الزامات مطابق با قوانین آن کشور رعایت شده است.	**بله( )**
NCB و کشور تماس گیرنده اذعان می کنند که اینترپل نباید در خصوص استفاده از هر اطلاعات استخراج شده یا هر گزارش بدست آمده با همکاری اینترپل از هر مدرکی، مسئول باشد. هر گونه استفاده از چنین اطلاعات یا گزارشی در روند دادرسی یا غیر آن در صلاحدید و مسئولیت آژانس تماس گیرنده / NBC است.	**بله( )**

مدارک: ویژگی	
نوع مدرک	موبایل/ هارد درایو/ غیره:...
ساخت/مدل	
#سریال	
#IMEI	
شناسایی کننده محلی مدرک	
کد عبور/ پسورد	
اطلاعت مربوطه دیگر	
مدارک: ویژگی	
نوع مدرک	موبایل/هارد درایو/ غیره:...
شرح فیزیکی	
ساخت/مدل	
#سریال	
#IMEI	
شناسایی کننده محلی مدرک	

کد عبور/ پسورد	
هر گونه اطلاعات مربوطه دیگر	

پایان

ترجمه: یوشا آل ایوب
https://yousha.blog.ir