بررسی صحنه‌های جرم الکترونیکی

حسین تراب زاده کارشناس ارشد رایانه مرکز تشخیص هویت پلیس آگاهی ناجا

تاریخ دریافت: ۸۸/۲/۱۵ تاریخ پذیرش:۸۸/۳/۲۴

چکیده:

ممکن است از رایانه به عنوان وسیله ای جهت ارتکاب جرم استفاده شود و یا حاوی ادله هایی مربوط به جرم باشـد و یا حتی به عنوان اهداف ارتکاب به جرم قلمداد شـوند. در هر صورت این تجهیزات معمولا حاوی ادله‌های بسیار خوبی جهت کشف جرم می‌باشند که درک نقـش و ماهیـت این ادله و چگونگی برخورد و مواجهه با صحنه‌های جرم حاوی این نوع از ادله به نحوی که بدون کمترین آسیب بتوان به آنها دست یافت و همچنین نحوه پاسخگویی به مراجع قانونی از اهداف این مقاله می‌باشد.

کلید واژه: جرم، صحنه جرم، صحنه جرم الکترونیک، ادله الکترونیکی

مقدمه:

امروزه رایانه و سایر دستگاههای الکترونیکی در تمامی جوانب زندگی مدرن نفوذ کرده اند. با وجود اینکه تا چندی پیش تنها می‌توانسـتیم رایانه‌ها را در اتاق‌ها ببینیم ولی امروزه این وسـیله در ابعاد بسـیار کوچکتر و در اشـکال مختلف در دست همه افراد قابل مشاهده است.

این وسیله سودمند که تا پیش از این به صورت ابزاری در جهت کمک به اجرای قانون مورد استفاده قرار می‌گرفت امروزه کاربرد دیگری نیز پیدا کرده و به وسیله ای در دست مجرمین برای ارتکاب به جرم تبدیل شده است. حال در این میان وظیفه کارشناسان بررسی صحنه جرم در مواجهه با صحنه اینگونه از جرایم به لحاظ ماهیت بسیار شکننده ای که ادله موجود در اینگونه صحنه‌ها دارند بسیار دشوار است.

ادله الکترونیکی چیست؟

ادله الکترونیکی شامل داده‌ها و اطلاعاتی در ارتباط با جرم است که توسط تجهزات الکترونیکی ذخیره سازی و یا جابجا می‌شوند. این ادله زمانیکه داده‌ها و یا تجهیزات فیزیکی جمع آوری و مورد تجزیه و تحلیل قرار می‌گیرند قابل دستیابی هستند.

چگونگی مواجهه با ادله الکترونیکی در صحنه‌های جرم

در جمع آوری، نگهداری و تجزیه و تحلیل ادله الکترونیکی بایستی دقت بسیاری را داشته باشیم.معمولا چگونگی مواجهه با ادله الکترونیکی در صحنه‌های جرم شامل مراحل زیر می‌باشد

- محافظت، تشخیص و شناسایی ادله الکترونیکی
- مستند سازی صحنه جرم
- جمع آوری ادله الکترونیکی
- بسته بندی و حمل و نقل و نگهداری ادله الکترونیکی

اطلاعات موجود در این مقاله با این فرض است که:

- قوانین مورد نیاز در خصوص جستجو، ضبط و توقیف ادله مشکوک وجود داشته و اجازه این کار را به ما می‌دهند
- صحنه جرم به خوبی محافظت شده و مستند سازی (عکسبرداری، تهیه کروکی و یاداشت

برداری) می‌شود

- نیازمندهای اولیه بررسی صحنه‌های جرم(مانند دستکش و...) موجود بوده و استفاده می‌شوند [۲]

توصیه می شود که کارشناسان خبره محلی را پیش از آنکه مورد نیاز باشند شناسایی کرده و هماهنگی لازم را با آنان داشته باشیم.

الف – تجهیزات الکترونیک: انواع و ادله بالقوه

می توان ادله الکترونیکی را در بسیاری از دستگا ه‌های الکترونیکی امروزی یافت. در ادامه به شرح انواع تجهیزات الکترونیک معمول که ممکن است در صحنه‌های جرم با آن مواجه شویم پرداخته شده است و در خصوص کاربردهای هر کدام توضیح لازم داده شده است. همچنین در خصوص ادله بالقوه ای که می توان در انواع تجهیزات رایانه ای به آن دست یافت نیز توضیح داده شده است.

توجه:برخی از تجهیزات رایانه ای که دارای حافظه می‌باشند به نحوی هستند که با قطع جریان برق یا با اتمام شارژ باطری، اطلاعات خود را از دست می‌دهند. باید دقت کرد که در این موارد پس از تعیین نحوه جمع آوری، نسبت به جمع آوری این تجهیزات اقدام و سپس تدابیری اندیشیده شود که این تجهیزات به هنگام نگهداری حتما به منبع تغذیه متصل باشند. [۱]

رایانه:

تعریف: معمولا یک ست رایانه ای شامل یک واحد پردازش مرکزی یا CPU، واحدهای ذخیره سازی اطلاعات، صفحه کلید، صفحه نمایش و موس می‌باشد. ممکن است این دستگاه به صورت مستقل ویا به صورت وصل به شبکه باشد. انواع مختلفی از رایانه‌ها وجود دارد که شامل رایانه‌های قابل حمل یا Laptop، رومیزی، داخل رکی، مینی رایانه‌های و رایانه‌های Mainframe می شوند. علاوه بر آن برخی تجهیزات جانبی نیز وجود دارند که از آن جمله

می‌توان به چاپگر، اسکنر، مودم و برخی تجهیزات ذخیره سازی اشاره نمود. به عنوان مثال یک رایانه رو میزی شامل کیس،مادر برد، CPU، تجهیزات ذخیره سازی داده ها، صفحه کلید و موس می‌باشد.

موارد استفاده: برای تمامی اعمال محاسباتی و ذخیره سازی اطلاعات شامل پردازش گرهای متنی، محاسباتی، ارتباطی و گرافیکی دارای کاربرد می‌باشد.

ادله بالقوه: معمولا ادله در فایل‌های ذخیره شده بر روی دیسک سخت،حافظه‌های قابل حمل و سایر تجهیزات قابل دسترسی می‌باشد. به عنوان مثال

فایل‌های ایجاد شده توسط کاربر

فایل‌های ایجاد شده توسط کاربر می‌تواند شامل اطلاعات بسیار مهمی در خصوص جرم رخداده شده باشند. این فایل‌ها ممکن است حاوی دفترچه آدرس‌ها و یا بانک‌های اطلاعاتی باشند که به نحوی با جرم مورد پیگیری ارتباط داشته و یا حاوی عکس‌ها وفیلم هایی در خصوص جرایم جنسی علیه کودکان ویا حاوی اطلاعاتی در خصوص ارتباط بین اجزای تیم مجرمین به صورت پست الکترونیک یا نامه باشند[۶].

- دفترچه تلفن و آدرس ها
- فایل‌های صوتی و تصویری
- دفترچه قرار ها
- فایل‌های بانک اطلاعاتی
- فایل‌های متنی یا مستندات
- فایل‌های پست الکترونیک
- فایل‌های عکس و گرافیک
- Book mark ها و favorites های اینترنتی
- فایل‌های آماری

فایل‌های محافظت شده توسط کاربر

معمولا کاربران دارای فرصت کافی جهت پنهان کردن فایل‌های مهم خود به اشکال مختلف را دارند.به عنوان مثال ممکن است آنها فایل‌های مهم خود را رمز کرده و یا کاری کنند که برای دسترسی به این فایل‌ها نیاز به یک کلمه عبور یاشد. آنها همچنین ممکن است عمدا فایل‌های روی دیسک سخت را پنهان کنند و یا فایل‌های مربوط به یک جرم را با نام‌های غیر واقعی ذخیره کنند. در مجموع فایل هایی که بایستی به آنها توجه کرد شامل موارد زیر می باشد

- فایل‌های فشرده شده
- فایل‌های مخفی شده
- فایل‌های رمز شده
- فایل‌های تغییر نام یافته
- فایل‌های با رمز دسترسی
- فایل‌های Steganography

همچنین ممکن است فایل‌های مربوط به ادله را در مجموعه فایل‌های عمومی رایانه یا سیستم عامل قابل دسترسی باشند زیرا در بسیاری از موارد کاربران از اینکه این فایل‌ها وجود دارند و در رایانه ذخیره می شوند بی اطلاع هستند. کلمات عبور، فایل‌های اینترنتی، فایل‌های چرک نویس (Temp) و فایل‌های پشتیبان از این دسته فایل‌ها هستند که در اغلب موارد قابل بازیابی و تجزیه و تحلیل هستند.

توجه: هر فایل دارای بخشی است که دارای اطلاعات بسیار سودمندی در خصوص تاریخ و ساعت ایجاد، تغییر، حذف، دسترسی و همچنین نام کاربر ایجاد کننده و ویژگی‌های خود فایل می باشد. این اطلاعات با یک بررسی دقیق قابل دسترسی است.

فایل‌های ایجاد شده توسط رایانه

- فایل‌های پشتیبان

- فایل‌های تنضیمات
- کوکی ها
- فایل‌های مخفی
- فایل‌های تاریخچه
- فایل‌های Log
- فایل‌های چاپ شده یا در نوبت چاپ
- فایل‌های Swap
- فایل‌های سیستمی
- فایل‌های چرک نویس (Temp)

همگی جزو این دسته از فایل‌ها هستند

سایر داده‌ها با ارزش

- فضاهای خراب دیسک
- ساعت، تاریخ و کلمه عبور رایانه
- فایل‌های حذف شده
- فضاهای خالی
- پارتیشن‌های مخفی
- سایر پارتیشن ها
- فضاهای رزرو شده روی دیسک
- فضاهای Slack
- اطلاعات Registery نرم افزارهای نصب شده
- فضاهای سیستمی
- کلاسترهای گم شده
- متادیتاها

● فضاهای تخصیص نیافته
همگی جزو این فضاها می باشند

اجزاء

واحد پردازش مرکزی (CPU)

توضیح: اغلب به آن تراشه گفته می شود و در واقع یک میکروپروسسور برای رایانه است. این قطعه در داخل جعبه کیس رایانه و روی مادربرد در کنار سایر اجزای الکترونیکی رایانه قرار می گیرد.

وظیفه اولیه: انجام تمامی محاسبات ریاضی و منطقی رایانه و کنترل تمام فعالیت ها

ادله بالقوه: ادله موجود در آن ممکن است شامل اطلاعات مربوط به دزدی‌ها و سرقت ها، جعل و یا کلاهبرداری باشد.

حافظه

توضیح: یک یا چند مدار قابل حمل داخل رایانه. اطلاعات داخل آن پس از خاموش شدن رایانه پاک می شود.

وظیفه اولیه: نگهداری دادها و برنامه‌های کاربر در زمان فعالیت رایانه.

ادله بالقوه: ادله موجود در آن ممکن است شامل اطلاعات مربوط به دزدی ها، سرقت ها، جعل و یا کلاهبرداری باشد.

۱. دستگاه‌های کنترل دسترسی (Access control Devices)

کارت‌های هوشمند، دانگل ها، اسکنرهای بیومتریک

توضیح: یک کارت هوشمند، دستگاه کوچک دستی است که دارای یک میکروپروسسور می باشد و قابلیت نگهداری و ذخیره اطلاعات مالی، اطلاعات هویتی ، گواهی نامه‌ها و مدارک دیجیتالی مربوط به یک فرد به صورت رمز شده را دارا می باشد[۲].

کاربرد اولیه: ایجاد امکان دسترسی به یک رایانه یا برنامه رایانه ای

ادله بالقوه: اطلاعات هویتی، اطلاعات تصدیق هویت مربوط به یک کارت و یا یک کاربر، سطح دسترسی وی، تنضیمات، حدود اختیارات، و خود دستگاه.

۲. دستگاه‌های پاسخگوی خودکار (منشی خودکار)

توضیح:یک دستگاه الکترونیکی که به عنوان بخشی از یک تلفن و یا به عنوان رابطی بین تلفن و خطوط تلفن کار می کند. این دستگاه در برخی از مدل‌ها مجهز به یک ضبط صوت دیجیتالی یا آنالوگ نیز می باشد.

کاربرد اولیه: ضبط پیام‌های صوتی در مواردی که تلفن شونده حضور نداشته باشد و یا قادر به پاسخگویی نباشد و معمولا پیش از ضبط یک پیام صوتی را پخش می کند.

توجه: با توجه به اینکه باطری‌های امروزی دارای عمر محدودی می باشند، ممکن است داده‌ها پس از خالی شدن شارژ باطری از بین بروند. بنابراین لام است این گونه دستگاه‌ها در زمان نگهداری و یا سایر موارد به یک منبع تغذیه متصل باشند.

ادله بالقوه: این دستگاه‌ها می توانند حاوی پیغام‌های ضبط شده و در مواردی زمان و تاریخ تماس و سایر اطلاعات در خصوص تماس گیرنده باشند که در مجموع شامل موارد زیر است:

- اطلاعات مربوط به تماس گیرنده
- پیغام‌های حذف شده
- شماره هایی که پیش از این تماس گرفته اند
- یاداشت ها
- شماره تلفن‌ها و نام ها
- نوارها

۴.دوربین‌های دیجیتال

توضیح: دوربین دیجیتال دستگاهی برای ضبط عکس و فیلم می باشد که دارای یک منبع

ذخیره سازی و یک سخت افزاری جهت تبدیل و انتقال این عکس و فیلم‌ها به رایانه می باشد.

کاربرد اولیه: دوربین دیجیتال عکس‌ها وفیلم‌ها را گرفته و آنها را به قالب دیجتال تبدیل کرده و در حافظه خود نگهداری می کند که می توان به راحتی این فایل‌ها را به رایانه انتقال داد.

ادله بالقوه:

- عکس ها
- نوارها و کاتریج‌های قابل حمل
- صدا
- ساعت و تاریخ اخذ تصاویر
- فیلم ها

۵. PDAها

توضیح: یک PDA دستگاه کوچک دستی است که دارای قابلیت‌های محاسباتی،تلفن، فکس، پیجر، اتصال به شبکه و سایر قابلیت‌ها می باشد و عموما به عنوان یک دستگاه منشی شخصی از آن استفاده می شود. یک رایانه دستی که دارای تمام قابلیت‌های یک رایانه رومیزی می باشد. برخی از آنها دارای دیسک نمی باشند ولی دارای درگاههایی جهت اتصال مودم، دیسک سخت و یا سایر دستگاه‌ها می باشند. این دستگا ها به راحتی قادرند اطلاعات خود را با سایر رایانه‌ها یکی کنند.

کاربرد اولیه: یک دستگاه با قابلیت محاسباتی، ذخیره سازی و ارتباطی دستی

توجه: با توجه به اینکه باطری‌های امروزی دارای عمر محدودی می باشند، ممکن است داده‌ها پس از خالی شدن شارژ باطری از بین بروند. بنابراین لام است این گونه دستگا ه‌ها در زمان نگهداری و یا سایر موارد به یک منبع تغذیه متصل باشند.

ادله بالقوه:

- دفتر تلفن

- قرارهای ملاقات
- مستندات
- ایمیل ها
- دست نوشته ها
- کلمات عبور
- دفترچه آدرس ها
- پیام‌های متنی
- پیام‌های صوتی

۶. دیسک سخت

توضیح: یک جعبه کوچک پلمپ شـده که حاوی تعدادی دیسـک و هد می باشـد و برای ذخیره سـازی و نگهداری اطلاعات از آن اسـتفاده می شـود. می تواند در داخل کیس رایانه یافت شود و یا به صورت مستقل و به عنوان یک دستگاه جانبی باشد.

کاربرد اولیه: منبع ذخیره سازی اطلاعاتی مانند برنامه ها، متن ها، تصاویر، فیلم ها، فایل‌های چندرسانه ای و...

ادله بالقوه: به ادله بالقوه مربوط به رایانه مراجعه شود.

۷. کارت‌های حافظه

توضیح: منبع ذخیره سازی اطلاعاتی که حتی با قطع جریان برق داده‌های خود را از دست نمی دهند. این دستگاه‌ها دارای این قابلیت هستند که حتی می توان اطلاعات پاک شده آنها را نیز بازیابی کرد. کارت‌های حافظه می توانند صدها و هزاران تصویر را در خود ذخیره کنند. دارای کاربردهای زیادی در دسـتگاه‌های رایانه، دوربین‌های دیجیتال، PDAها و... هسـتند. به عنوان مثال هایی از آن می توان به حافظه‌های فلش، کارت‌های هوشنمد، حافظه‌های قابل حمل تراشه ای و... اشاره کرد.

کاربرد اولیه: فراهم آوردن یک فضای ذخیره سازی قابل حمل.

ادله بالقوه: به ادله بالقوه مربوط به رایانه مراجعه شود.

۸. مودم‌ها

توضیح: در انواع داخلی و خارجی، بی سیم و کارت PC موجود است.

کاربرد اولیه: به منظور ایجاد ارتباط آسان بین دو رایانه و یا رایانه و شبکه با استفاده از خطوط تلفن، بی سیم و یا سایر بسترها بکار می رود.

ادله بالقوه: خود مودم.

۹. تجهیزات شبکه

-کارت‌های شبکه محلی (LAN):

توضیح: کارت شبکه ای که می تواند باسیم یا بی سیم باشد.[۷]

کاربرد اولیه: برای اتصال رایانه‌ها به منظور ردوبدل کردن اطلاعات و یا به اشتراک گذاری منابع بکار می رود.

ادله بالقوه: خود دستگاه، آدرس MAC

- روترها، هاب‌ها و سویچ‌ها

توضیح: این تجهیزات الکترونیکی در سیستمهای شبکه رایانه‌ها دارای کاربرد است. این تجهیزات هر یک قابلیت خاصی را در زمینه شبکه فراهم می کنند. این تجهیزات می توانند همزمان ارتباطات زیادی را در اختیار ما قرار دهند.

کاربرد اولیه: تجهیزاتی برای توزیع راحت داده‌ها در سطح شبکه.

ادله بالقوه: خود تجهیزات و در خصوص روترها تنضیمات آنها.

- سرورها

توضیح: یک سرور رایانه ای است که برخی سرویس‌ها را برای سایر رایانه هایی که از طریق شبکه به آن متصل هستند فراهم می کند. هر رایانه ای حتی یک لپ تاپ را می توان به

عنوان یک سرور پیکربندی کرد.

کاربرد اولیه: فراهم آوردن منابع اشتراکی مانند ایمیل، بانک نرم افزار، وب سرور، و پرینت سرور بر روی شبکه.

ادله بالقوه: به ادله بالقوه مربوط به رایانه مراجعه شود.

– کابل‌های شبکه و متصل کننده‌ها

توضیح: کابل‌های شبکه می توانند دارای رنگ‌های مختلف، ضخامت‌های مختلف و ظاهر مختلفی باشند و همچنین دارای شکل‌های ارتباطی مختلفی بسته به تجهیزات مختلف که به آنها متصل می شوند باشند.

کاربرد اولیه: اتصال تجهیزات مختلف رایانه ای از طریق شبکه.

ادله بالقوه: خود تجهیزات.

۱۰. پیجرها

توضیح: دستگاه کوچک دستی قابل حملی که می تواند حاوی ادله با ارزش ولی فراری نظیر شماره‌های تلفن، پیام‌های صوتی و ایمیل باشد.

کاربرد اولیه: دستگاهی برای ارسال و دریافت پیام‌های الکترونیکی، شماره‌ها (شماره تلفن‌ها و...) و اعداد و حروف (مانند ایمیل‌ها).

توجه:برخی از تجهیزات رایانه ای که دارای حافظه می‌باشند به نحوی هستند که با قطع جریان برق یا با اتمام شارژ باطری، اطلاعات خود را از دست می‌دهند. باید دقت کرد که در این موارد پس از تعیین نحوه جمع آوری، نسبت به جمع آوری این تجهیزات اقدام و سپس تدابیری اندیشیده شود که این تجهیزات به هنگام نگهداری حتما به منبع تغذیه متصل باشند. [۱]

ادله بالقوه:

- اطلاعات مربوط به آدرس ها
- ایمیل ها

- شماره‌های تلفن
- پیام‌های متنی
- پیام‌های صوتی

۱۱. رسانه‌های ذخیره سازی قابل حمل

توضیح : رسانه ها برای ذخیره سازی اطلاعات دیجیتال هستند مانند فلاپی دیسک ها ، سی دی ها ، دی وی دی ها ، کاتریج ها ، نوارها و ...)

کاربـــرد اولیـــه : تجهیـــزات قابل حملی که می توانند اطلاعـــات مربوط به برنامه ها ، متون ، تصاویر ، فیلم ها ، فایل‌های چند رسانه ای و غیره را نگهداری کنند .

ادله بالقوه : به ادله مربوط به رایانه مراجعه شود

۱۲. چاپگرها

توضیح: انواع مختلفی از چاپگرها وجود دارند که شـــامل حرارتی، لیزری، جوهرافشـــان و فشـــاری یا ضربه ای می شـــوند که به وســـیله یک کابل (سریال، موازی، USB) و یا حتی بی ســـیم مانند مادون قرمز به درگاه متصل می شـــوند. برخی از چاپگرها دارای حافظه داخلی می باشند که به آنها این امکان را می دهد تا چندین صفحه را جهت چاپ دریافت نموده و سپس نسبت به چاپ آنها اقدام کنند. برخی از انواع آن دارای دیسک سخت نیز می باشند.

کاربرد اولیه: چاپ عکس، متن و غیره از رایانه بر روی کاغذ.

ادلـــه بالقـــوه: برخی چاپگرها ممکن اســـت دارای LOG یا اطلاعاتی در خصوص زمان و تاریخ باشند و اگر متصل به شبکه باشند ممکن است اطلاعاتی در خصوص شبکه را در خود داشته باشند. به علاوه کاراکتر ست خاص یک چاپگر ممکن است سبب شناسایی آن شود.

- مستندات
- دیسک سخت
- کاتریج جوهر

- اطلاعات شبکه
- تصاویر باقی مانده بر روی ریبون ها
- ساعت و تاریخ فعالیت
- LOGهای کاری

۱۳. رسانه‌های ذخیره سازی قابل حمل

توضیح: رسانه‌ها برای ذخیره سازی اطلاعات دیجیتال هستند مانند فلاپی دیسک ها، سی دی ها، دی وی دی‌ها ، کاتریج ها، نوارها و...)

کاربـرد اولیـه: تجهیزات قابل حملی کـه می توانند اطلاعات مربوط بـه برنامه ها، متون، تصاویر، فیلم ها، فایل‌های چند رسانه ای و غیره را نگهداری کنند.

ادله بالقوه: به ادله مربوط به رایانه مراجعه شود.

۱۴. اسکنرها

توضیح: دستگاهی نوری که از مستندات تصویر تهیه کرده و این تصاویر را به صورت فایل در رایانه ذخیره می کند.

کاربـرد اولیه: تبدیل اسـناد، تصویر و... به فایل دیجیتالی که سـپس مـی توان آنها را دید، دستکاری کرد و یا به رایانه دیگری انتقال داد.

ادله بالقوه: خود این دسـتگاه می تواند ادله باشـد. قابلیت‌های خود دستگاه می تواند کمک خوبی در پرونده ای هرزه نگاری کودکان، جعل و سرقت باشد. بعلاوه نقص‌های خاص مانند خش و لک روی شیشه خود می تواند ادله خوبی باشد.

۱۵. تلفن‌ها

توضیح: یک دسـتگاه دسـتی که ممکن اسـت به تنهایی کار کند و یا دارای یک بخش ثابت و یک بخش متحرک باشـد و یا مسـتقیم به خطوط تلفن وصل باشـد. می تواند به عنوان منبع

تغذیه از باطری داخلی، سیم برق و یا خطوط تلفن استفاده کند.

کاربرد اولیه: ایجاد ارتباط با یک دستگاه تلفن دیگر به وسیله خطوط تلفن، رادیویی، سیستم سلولی و یا ترکیبی از آنها. تلفن‌ها قابلیت نگهداری اطلاعات را دارند.

توجه:برخی از تجهیزات رایانه ای که دارای حافظه می‌باشند به نحوی هستند که با قطع جریان برق یا با اتمام شارژ باطری، اطلاعات خود را از دست می‌دهند. باید دقت کرد که در این موارد پس از تعیین نحوه جمع آوری، نسبت به جمع آوری این تجهیزات اقدام و سپس تدابیری اندیشیده شود که این تجهیزات به هنگام نگهداری حتما به منبع تغذیه متصل باشند.

ادله بالقوه: برخی از تلفن‌ها می توانند نام ها، شماره‌های تلفن و اطلاعات مربوط به تماس گیرنده را در خود نگه دارند. برخی از آنها همچنین می توانند اطلاعات مربوط به قرارهای ملاقات، ایمیل‌ها و پیام‌های صوتی را نگهداری کنند.

- قرارهای ملاقات
- اطلاعات مربوط به تماس گیرنده
- شماره سریال‌های الکترونیکی
- ایمیل ها
- یاداشت ها
- کلمات عبور
- دفرچه تلفن
- پیام‌های متنی
- پیام‌های صوتی
- نمایشگرهای وب

۱۶. دستگاههای کپی

برخی از دستگاههای کپی ممکن است دارای حافظه جهت نگهداری موارد کپی باشند. دستگاه‌های کپی / اسکن ممکن است ابتدا از سند اسکن تهیه کرده در حافظه خود ذخیره کرده و سپس از آن کپی تهیه کند.

ادله بالقوه:

- مستندات
- زمان‌ها و تاریخ‌های فعال بودن
- LOG مربوط به کاربران

۱۷. کارت‌های اعتباری

این کارت‌ها حاوی اطلاعاتی بر روی نوار مغناطیسی روی یک کارت پلاستیکی می باشند.

ادله بالقوه: اطلاعات مربوط به کارت خوان که می توان از آن برای ردگیری استفاده کرد و بر روی کارت نگهداری می شود

- تاریخ انقضاء
- شماره کارت اعتباری
- آدرس مالک
- نام مالک

۱۹. ساعت‌های دیجیتالی

ساعت‌های دیجیتالی فراوانی وجود دارند که دارای قابلیت هایی نظیر یک پیچر هستند. این دستگاهها می توانند حاوی دفترچه تلفن‌ها و آدرس ها، قرارهای ملاقات، ایمیل ها، یاداشت‌ها و همچنین در مواردی اطلاعاتی در خصوص همسان شدن با رایانه ای خاص باشند.

ادله بالقوه:

- دفترچه تلفن
- قرارهای ملاقات
- ایمیل
- یاداشت ها
- دفترچه آدرس ها

۲۱. دستگاه‌های فاکس

این دستگاه‌ها می توانند برای ارتباط با شماره‌های خاص برنامه ریزی شده باشند، دارای فضایی برای نگهداری مستندات ارسالی و یا دریافتی باشد. برخی از آنها این قابلیت را دارند که از مستندات تصویر تهیه کرده و سپس در زمان خاصی برای شماره‌های خاصی ارسال کنند و یا فکس‌های دریافتی را ابتدا روی حافظه ذخیره کرده و سپس به چاپ آنها اقدام کنند.

ادله بالقوه:

- مستندات
- فیلم‌های مربوط به کاتریج
- شماره‌های تلفن
- LOG مربوط به موارد ارسالی و دریافتی

۲۲. دستگاه‌های تعیین موقعیت (GPS)

این دستگاه‌ها می توانند حاوی اطلاعات خوبی در خصوص مسیرهای قبلی طی شده، اطلاعات ذخیره شده مربوط به نقاط خاص و مکان هایی که فرد در آنجا حضور داشته باشد. برخی از آنها این اطلاعات را به صورت خودکار ذخیره کرده و LOG می کنند.

ادله بالقوه:

- محل منزل فرد

- موقعیت‌های قبلی
- LOG مسافرت ها
- موقعیت نقاط خاص ذخیره شده
- نام نقاط خاص ذخیره شده

۲۳. سایر تجهیزات الکترونیکی

تجهیزات الکترونیکی بیشمار دیگری نیز وجود دارند که امکان گنجاندن آنها در این لیست نمی باشد ولی ممکن است در صحنه جرم یافت شوند.

ابزارها و تجهیزات پی جویی

نکتــه: بــرای جمع آوری ادلــه الکترونیکی به ابزارها و تجهیزات خاصی نیاز می باشــد و تجربه نشــان داده اســت که پیشــرفت فن آوری سبب تغییر این ابزارها و تجهیزات می شود. برای مستندســازی، جداســازی، بســته بندی و حمل ادله بایســتی به این ابزارها و تجهیزات دسترسی داشته باشیم.

بایستی آمادگی لازم جهت استفاده از ابزارها و تجهیزات خاص جمع آوری ادله الکترونیکی وجود داشته باشد زیرا هر صحنه ابزارهای خاص خود را در روند کار نیاز دارد. [۲]

ابزارها

هر واحد بررسی صحنه جرم الکترونیکی علاوه بر ابزارهای عمومی بررسی صحنه جرم(دوربین، دفترچه یاداشــت، نوار صحنه جرم، برگه‌های ترســیم کروکی و...) باید به ابزارهای زیر نیز دسترسی داشته باشد.

ابزارهای مستندسازی

- برچسب ویژه کابل
- برچسب نمدی با رنگ ثابت
- برچسب‌های چسبی

ابزارهای خاص جداسازی

سری کاملی از ابزارهای زیر در ابعاد و انواع مختلف و از نوع غیر مغناطیسی

- پیچ گوشتی‌های تخت و چهارسو
- پیچ گوشتی‌های شش پر
- پنس‌های کوچک
- پیچ گوشتی‌های خاص (ترجیحا ساخت شرکت‌های Compaq و Macintosh)
- انبردست‌های استاندارد
- پیچ گوشتی‌های ستاره ای
- سیم چین

تجهیزات خاص بسته بندی و حمل و نقل

- پاکت‌های Antistatic(ضد الکتریسته ساکن)
- بسته‌های حباب دار Antistatic
- بسط‌های کمربندی
- جعبه خاص ادله
- ملزومات بسته بندی (مانند انواع یونولیت یا چوب پنبه که الکتریسیته ساکن را جذب نمی کند)
- نوار بسته بندی
- جعبه‌های محکم در اندازه‌های مختلف

سایر موارد

- دستکش
- تسمه‌های پلاستیکی بزرگ
- فهرستی از شماره تلفن‌ها برای دریافت مشاوره یا کمک

- ذره بین
- کاغذ خاص چاپگر
- چراغ قوه کوچک
- فلاپی دیسک استفاده نشده
- سی دی خام استفاده نشده
- حافظه فلش استفاده نشده

ب – محافظت، تشخیص و شناسایی ادله الکترونیکی

اصل: کارشناسان بررسی صحنه جرم ابتدا باید اقدامات لازم را جهت محافظت از افراد و مسدومین صحنه جرم بعمل آورند سپس باید به نحوی اقدام نمایند که تمامی ادله موجود در صحنه از هرگونه تغییری مسون بمانند تا اطمینان لازم از صحت تمامی ادله (الکترونیکی و غیر الکترونیکی) بوجود بیاید. [۱]

روند: بعد از محافظت از افراد و ادله موجود در صحنه جرم، کارشناس صحنه باید نسبت به شناسایی ادله آشکار (معمولی و الکترونیکی) و همچنین ادله فرار اقدام کند. سپس کارشناس صحنه باید صحنه جرم را ارزیابی کرده و نحوه بررسی صحنه را طرح ریزی کند.

حفظ و ارزیابی صحنه

- تمامی اقدامات قانونی را برای حفظ صحنه جرم بعمل آورید. اگر شخص یا اشخاصی باید به لحاظ وضعیت خاص خود به خارج از صحنه منتقل شوند، مطمئن شوید پیش از ترک صحنه هیچ گونه ادله ای به همراه آنان نباشد. در این مرحله از پی جویی وضعیت ادله را تغییر ندهید، اگر روشن هستند، آنها را روشن باقی بگذارید و اگر خاموش هستند، آنها را خاموش باقی بگذارید.
- به روش‌های فیزیکی یا الکترونیکی (برحسب نیاز) از ادله فرار محافظت کنید. ممکن است ادله فرار در پیجرها، caller ID ها، منشی‌های الکترونیکی، تلفن‌های سلولی

و یا سایر دستگاه‌های مشابه یافت شوند. کارشناس صحنه جرم باید توجه کند که هر دستگاهی که ممکن است حاوی ادله فرار باشند باید سریعا محافظت شوند، مستندسازی شوند و از آنها عکس تهیه شود.

- تمامی خطوط تلفنی که به دستگاه هایی نظیر مودم‌ها و caller IDها متصل هستند باید شناسایی شوند. باید تمامی خطوط تلفن مستندسازی شوند، قطع شوند، و تک تک برچسب زده شوند البته در صورت امکان ترجیحا از طرف سوکت روی دیوار. همچنین ممکن است ارتباطات دیگری نظیر خطوط شبکه در صحنه وجود داشته باشند، در این حالت بهتر از مشاوره افراد یا شرکت‌های متخصص استفاده کنید.

نکته: ممکن است صفحه کلیدها، موس ها، دیسکت ها، سی دی‌ها و سایر تجهیزات حاوی اثرانگشت یا سایر ادله فیزیکی باشند، نسبت به حفظ آنها دقت کنید البته توجه کنید که برداشت اثر انگشت یا سایر ادله به روش‌های شیمیایی ممکن است سبب از بین رفتن ادله الکترونیکی شوند بنابراین دقت کنید که نسبت به برداشت این ادله پس از جمع آوری ادله الکترونیکی اقدام کنید.

انجام مصاحبه اولیه

- شناسایی و دسته بندی تمامی افراد (شاهد ها، مظنونین و یا سایر افراد)
- مصاحبه و بازجویی از مالکین یا کاربران تجهیزات الکترونیکی که در صحنه یافت می شوند مطابق با قوانین جهت دستیابی به کلمات عبور، نام کاربری و... که برای دسترسی به سیستم ها، نرم افزارها و داده‌ها نیاز است (برای هر یک از آنها ممکن است به چندین کلمه عبور مانند کلمه عبور BIOS، ورود به سیستم، شبکه، ISP، فایل‌های کاربردی، عبارات رمز شده، ایمیل، فهرست قرارهای ملاقات و مخاطبین نیاز باشد.[۴]
- هدف از بکارگیری سیستم
- روش‌های محافظت و یا تخریب دستگاه
- هر گونه مستندات در خصوص سخت افزارها یا نرم افزارهای نصب شده بر روی

سیستم [۱]

نکته: برخی از کاربران زمان تعریف کلمه عبور دچار یکی از اشـتباهات زیر می شـوند که توجه به این نکات زمانی که کاربر همکاری لازم را ندارد ممکن است سودمند واقع شود

- کلمات عبور پیش فرض انتخاب شده باشد
- از کلمات عبور ساده و کوتاه استفاده نموده باشند
- از لغات لغت نامه ای استفاده نموده باشند [۵]

ج – مستندسازی صحنه جرم

اصل: مستندسازی صحنه جرم سبب می شود که یک تصویر دائمی از صحنه جرم را برای همیشه داشته باشیم. مستندسازی یک روند دائمی در طی پی جویی می باشد. این کار برای ضبط موقعیت و وضعیت رایانه ها، رسـانه‌های ذخیره سـازی، سایر تجهیزات الکترونیکی و سایر ادله مرسوم بسیار مهم می باشد. [۱]

نکته: مستندسازی صحنه جرم باید مطابق با قوانین جاری انجام شود.

روند: مستند سازی صحنه جرم باید با جزئیات کامل انجام شود.

مستندسازی صحنه فیزیکی

- بررسـی و مستندسـازی صحنـه فیزیکی ماننـد موقعیت موس و اجزا مربوط به سـایر تجهیزات (در سـمت چپ قرار داشـتن موس ممکن اسـت دلیلی بر چپ دسـت بودن کاربر باشد).
- مستندسـازی موقعیت و وضعیت سیسـتم کامپیوتر به همراه وضعیت روشـن، خاموش یا در حال اسـتراحت (Sleep Mode). اغلب رایانه‌ها دارای یک LED هسـتند که وضعیت رایانه را مشخص می کند. همچنین در صورت شنیده شدن صدای فن، احتمالا این موضوع بیانگر روشـن بودن رایانه اسـت و اگر رایانه گرم باشـد بیانگر این موضوع است که رایانه روشن است و یا به تازگی خاموش شده است.

- شناسایی و مستندسازی سایر تجهیزات الکترونیکی که جمع آوری نشده اند.
- برای ایجاد یک مستند تصویری عکسبرداری از صحنه جرم از زوایای مختلف بایستی به نحوی انجام شود که یک پوشش ۳۶۰ درجه از تمامی صحنه حاصل شود.
- عکسبرداری از نمای جلوی رایانه باید به نحوی انجام شود که محتویات صفحه نمایش و سایر متعلقات کاملا مشخص باشند. همچنین از آنچه که در صفحه نمایش وجود دارد باید نوت برداری شود. در این زمان ممکن است نیاز باشد از نرم افزارهای فعال فیلم تهیه نمود و یا مستندسازی بیشتری انجام داد.

نکته: حرکت دادن سیستم رایانه ای در حالی که نرم افزارهایی در آن در حال کار می باشند، ممکن است سبب تغییر داده‌های آن شود بنابراین باید از حرکت رایانه تا زمانیکه به صورت مطمئن خاموش شود خوداری نمود.

- مستندسازی بیشتر باید در فاز جمع آوری ادله انجام شود.

د- جمع آوری ادله

اصل: با ادله الکترونیکی مانند سایر ادله باید به دقت و به نحوی کار کرد که ارزش واقعی آنها حفظ شود و به هیچ عنوان دچار تغییر نشود. این اصل تنها در خصوص ادله یا تجهیزات فیزیکی صادق نیست بلکه شامل داده‌های الکترونیکی نیز می شود.بنابراین ادله الکترونیکی به دلیل خاص بودن نیاز به جمع آوری، بسته بندی و حمل و نقل خاص دارند. ملاحظات خاص در خصوص محافظت از داده‌ها باید انجام شود زیرا ممکن است این داده‌ها به وسیله منابع الکترومغناطیسی نظیر منابع تولید الکتریسته، مغناطیس، امواج رادیویی و سایر موارد دچار تغییر یا تخریب شوند.

باید دقت شود که در زمان ضبط ادله الکترونیکی صحنه جرم به خوبی محافظت و محصور شده باشد البته این محافظت باید در حداقل وسعت ممکن انجام شود. [۳]

برای حصول نتیجه بهتر قبل از هر کاری باید نسبت به شناسایی مالکین و کاربران تجهیزات دیجیتال اقدام نمود و سپس با قدم زدن و بررسی دقیق صحنه به نوع تجهیزات موجود و نحوه

ارتباط آنها با یکدیگر پی برد. [۴]

توجه: پیش از هر گونه اقدامی در خصوص جمع آوری ادله، باید دقت شود که تمامی مراحل مربوط به موقعیت یابی و مستندسازی آن طبق آنچه که در فصول ۳ و ۴ گفته شده است انجام شـده اسـت. توجه کنید که سایر انواع ادله مانند اثر پا، ادله بیولوژیک، اثرانگشت و... ممکن است در صحنه موجود باشند.

ادله غیر الکترونیک

بازیابی ادله غیرالکترونیک می تواند سبب دشوار شدن روند پی جویی یک جرم الکترونیک شود. توجه ویژه ای در خصوص اینکه آیا این گونه ادله غیر الکترونیک بازیابی و حفظ شده اند باید انجام شـود. مواردی که در تجزیه و تحلیل های بعدی ادله الکترونیک ممکن اسـت بکار آید چه بسـا در شـکل ها و قالب‌های دیگر (کلمات عبور یا نکاتی در خصوص سـخت افزار که نوشته شده باشند، راهنماهای کاغذی استفاده از سخت افزار یا نرم افزار، تقویم ها، متون، نسـخه‌های چاپی متن‌ها یا تصاویر رایانه ای و عکس‌های کاغذی) همگی باید برای بررسی و تجزیه و تحلیلهای بعدی مورد توجه قرار گیرند. ممکن است همه این موارد را در اطراف رایانه یا سایر تجهیزات الکترونیکی بدست آورید.

ادله مربوط به رایانه‌های مستقل و لپ تاپ

توجه: وجود چندین رایانه در یک صحنه ممکن اسـت نشـان از وجود یک شبکه رایانه ای باشد. همچنین اغلب رایانه‌های موجود در شرکت‌های تجاری به صورت شبکه کار می کنند. در این چنین مواردی بایستی دانش کافی در خصوص این سیستم‌ها داشته باشیم یا از مشاوره کارشناس این کار بهره مند شویم.

یک رایانه مستقل رایانه ای است که به هیچ شبکه یا کامپیوتر دیگری متصل نباشد. یک رایانه مسـتقل ممکن اسـت به شکل رایانه رومیزی یا لپ تاپ باشد. یک رایانه لپ تاپ، رایانه ای است که تمامی اجزای آن شامل کی برد، موس، صفحه نمایش، کیس به صورت یکپارچه در

کنار هم قرار دارند و بر خلاف رایانه رومیزی دارای یک باطری قابل حمل می باشد.

اگر رایانه روشـــن اســـت، وضعیت فعلی آن را مستند سازی کرده و سپس مشاور ماهر خود را صدا بزنید ولی اگر چنین فردی را در اختیار ندارید کارهای زیر را انجام دهید

بعد از اینکه نسبت به حفظ صحنه مطابق مطالب گفته شده در بالا اقدام کردید، قبل از انجام هر کاری موارد زیر را به دقت مطالعه کنید

الف: از تمام کارهایی که انجام می دهید و هر گونه تغییری که روی صفحه نمایش، رایانه، چاپگر و سایر تجهیزات که در اثر اقدامات شما رخ می دهد یاداشت تهیه کنید.

ب: صفحه نمایش را مشاهده کنید و بررسی کنید که آیا روشن، خاموش یا در حال استراحت است سپس با توجه به وضعیت آن یکی از موارد زیر را انجام دهید

وضعیت ۱: صفحه نمایش روشن است و محتویات آن مشخص است

۱- از صفحه آن تصویر تهیه کرده و از اطلاعات آن را ثبت کنید.

۲- به مرحله پ بروید

وضعیت ۲: صفحه نمایش روشن است و صفحه آن سیاه است (حالت خواب) یا محافظ صفحه نمایش فعال است

۱- مقدار جزئی موس را حرکت داده (بدون فشـــار دکمه‌های آن). صفحه باید تغییر کند و یا چیزی را نمایش می دهد یا از شما درخواست کلمه عبور می نماید.

۲- اگر حرکت موس ســـبب هیچ گونه تغییری نگردید هیچ دکمه ای را فشـــار ندهید و هیچ کاری را توسط موس انجام ندهید.

۳- از صفحه آن تصویر تهیه کرده و از اطلاعات آن را ثبت کنید.

۴- به مرحله پ بروید.

وضعیت ۳: صفحه نمایش خاموش است

۱- وضعیت خاموش صفحه نمایش را توسط یاداشت ثبت کنید.

۲- صفحه نمایش را روشن کنید سپس بررسی کنید که کدام یک از وضعیت‌های ۱ یا ۲ را داراست و سپس کار را طبق آن وضعیت‌ها ادامه دهید.

پ: صرف نظر از وضعیت رایانه (روشن، خاموش یا در حال استراحت)، ارتباط رایانه را با برق قطع کنید البته از سمت پریز روی دیوار. اگر با یک رایانه لپ تاپ سرو کار دارید علاوه بر قطع برق، باطری آن را نیز جدا کنید. بعضی لپ تاپ‌ها دارای باطری دوم نیز هستند که باید آن را نیز جدا کنید.

ت: سایر ارتباطات (خطوط تلفن وصل به مودم، کابل ها، خطوط ISDN و DSL) را نیز کنترل کنید. اگر خط تلفنی وجود دارد تلاش کنید که شماره آن را بدست آورید.

ث: برای جلوگیری از هرگونه آسیبی به ادله بالقوه، هر گونه فلاپی دیسکی که ممکن است وجود داشته باشد را از رایانه خارج کرده و به صورت جداگانه بسته بندی کرده و برچسب بزنید. اگر ممکن است یک دیسکت خالی یا دیسکت ویژه را در فلاپی گردان قرار دهید. توجه کنید که نباید سی دی‌ها را خارج کرده و یا دکمه سی دی گردان را فشار دهید.

ج: نام مدل‌ها و شماره سریال‌ها را ثبت کنید.

ح: از تمامی ارتباطات و کابل‌های رایانه عکس تهیه کنید.

خ: تمامی اتصالات و انتهای همه کابل‌ها را برچسب بزنید (همچنین اتصالات به سایر دستگاه‌های جانبی) تا بتوان بعدا به دقت آنها را سرهم کرد. درگاههای استفاده نشده و انتهای استفاده نشده کابل‌ها را به عنوان استفاده نشده برچسب بزنید. درگاه‌های جانبی ارتباطی رایانه‌های لپ تاپ را شناسایی کرده تا بتوانید به سایر رسانه‌های ذخیره سازی دست یابید.

چ: ادله را بر اساس روند جاری سازمان ثبت کنید.

د: اگر نیاز به حمل و نقل ادله می باشد، آنها را مانند اشیای شکستنی بسته بندی کنید (مراجعه به فصل ۶).

رایانه‌های موجود در محیط‌های پیچیده

به وفور در محیط‌های تجاری می توان رایانه هایی را دید که به یکدیگر (به یک سرور یا با هم) متصل هستند. حفظ و بررسی صحنه‌های جرمی که رایانه‌های آن به صورت شبکه ای

می باشـــند دارای مشـــکلات خود بوده زیرا هر اقدام نادرستی ممکن است سبب از بین رفتن ادله شود. زمانیکه با یک صحنه جرم در محیط های تجاری روبرو می شوید باید بر اساس یک طرح و الگوی حســـاب شـــده اقدام نمود و از کمک یک مشـــاور ماهر بهره برد. البته باید دقت نمود که ممکن است در محیط یک خانه نیز شبکه رایانه ای وجود داشته باشد.

از نشـــانه‌های اینکه ممکن اســـت یک شبکه رایانه ای در صحنه وجود داشته باشد می توان به موارد زیر اشاره نمود:

- وجود چندین رایانه در صحنه جرم
- وجود کابل ها و درگاه‌های خاص شـــبکه (مانند آنچه در شـــکل سمت چپ دیده می شود)که ارتباط بین رایانه و دستگاههای مرکزی شبکه را فراهم می کند.
- اطلاعات کسب شده از مخبرین یا افراد حاضر در صحنه.
- وجود اجزای شبکه در صحنه برابر آنچه که در فصل یک گفته شد.

سایر دستگاه‌های الکترونیکی و تجهیزات جانبی

دستگاه‌های الکترونیکی مانند آنچه که در فهرست زیر به آن اشاره شده است ممکن است دارای ادله بالقوه در ارتباط با جرم به وقوع پیوســـته باشـــند. با این دســـتگاه‌ها هیچ گونه کاری را نبایـــد انجـــام داد مگر اینکه یک وضعیت اضطراری وجود داشـــته باشـــد. در صورت نیاز به دســـتکاری این دســـتگاه‌ها جهت دســـتیابی به اطلاعات آنها، برای اعتبار بخشـــیدن به این اطلاعات جمع آوری شده تمام کارها باید مستند سازی شوند. تعداد زیادی از این دستگاه‌ها که در لیســـت پایین آورده شـــده اند ممکن اســـت حاوی داده هایی باشند که در صورت اقدام نادرست از بین بروند.

مثال هایی از سایر دستگاه‌های الکترونیکی (شامل تجهیزات جانبی رایانه)

- ضبط صوت ها
- منشی‌های تلفن
- کابل ها

- دستگاه‌های Caller ID
- تلفن‌های سلولی
- تراشه‌ها (وجود تعداد زیادی تراشه ممکن است نشان از یک سرقت تراشه باشد)
- دستگاه‌های کپی
- بانک سی دی
- قفل‌های سخت افزاری و یا سایر تجهیزات محافظت از کپی نرم افزار ها
- دستگاه‌های تهیه همزمان چندین کپی از سی دی ها، دی وی دی ها، دیسک‌های سخت و...
- دستگاه‌های خارجی
- دستگاه‌های فکس
- کارت‌های حافظه
- فلاپی دیسک ها، سی دی‌ها و دی وی دی ها
- دستگاه‌های GPS
- پیجرها
- کارت‌های PCMCIA
- چاپگرها (اگر در حال چاپ چیزی هستند اجازه دهید کارشان را به اتمام برسانند)
- اسکنرها
- کارت‌های هوشمند
- گوشی‌های تلفن
- رسانه‌های قابل حمل(Tape ها، کاتریج‌ها و...)
- VCR ها
- تجهیزات ارتباطی بی سیم

توجه: اگر رسانه قابل حملی را توقیف می کنید، دقت داشته باشید که دستگاه خاص استفاده از آن را نیز توقیف کنید (مانند TapeDrive ها و...)

ح - بسته بندی، حمل و نقل و نگهداری

اصـــل: به هیچ عنوان نبایدکاری کرد که ســـبب اضافه شـــدن، تغییر یـــا از بین رفتن داده‌های موجود در یک رایانه یا سایر رسانه‌ها شود. رایانه‌ها تجهیزات الکترونیکی بسیار ظریفی هستند که نســـبت به حرارت، رطوبت، ضربه یا تکان فیزیکی، الکتریســـیته ساکن، منابع مغناطیسی و امواج الکترو مغناطیسی بسیار حساس هستند بنابراین باید احتیاط خاص و ویژه ای را حین بســـته بندی، حمل و نقل و نگهداری ادله الکترونیکی داشـــته باشـــیم. همچنین باید در تمامی مراحل بسته بندی، حمل و نقل و نگهداری کار مستندسازی را ادامه دهیم. [۱]

نکته:مطمئن شـــوید که روند بســـته بندی، حمل و نقل و نگهداری ادله به درستی انجام شده است به نحوی که ادله دچار هیچ گونه تغییر، آسیب فیزیکی و یا تغییر در داده‌ها نشوند.

روند بسته بندی

الف: مطمئن شوید که تمامی ادله الکترونیکی جمع آوری شده پیش از بسته بندی به درستی مستندسازی شده اند، برچسب خورده اند و صورت برداری شده اند.

ب: دقت ویژه ای داشـــته باشـــید که آثار انگشـــت، جای پاها و سایر ادله غیرالکترونیک به خوبی حفظ شوند.

پ: رسانه‌های مغناطیسی را در بسته بندی‌های ضد الکتریسیته ساکن قرار دهید (پاکت‌های کاغذی یا پلاستیکی ضد الکتریسیته ساکن)

ج: از تا کردن، خم کردن یا خراشـــیدن رســـانه هایی مانند ســـی دی یا فلاپی دیسک‌ها جدا خوداری کنید.

چ: دقت کنید که تمامی جعبه هایی که از آنها برای بسته بندی ادله استفاده شده است دارای برچسب باشند.

توجه: اگر چندین سیســـتم رایانه ای را بســـته بندی می کنید دقت داشته باشید که هر سیستم را جداگانه و به صورت مشـــخص برچســـب بزنید تا در زمان سرهم کردن آنها اجزای هر یک مشخص باشد.

روند حمل و نقل

الف: ادله الکترونیک را از مجاورت منابع مغناطیسی دور نگه دارید. رادیوهای ترانزیستوری، بلندگوهای مغناطیسی و بخاری همگی مثال هایی از مواردی هستند که ممکن است به ادله آسیب وارد کنند.

ب:از نگهداری طولانی مدت ادله الکترونیک در داخل خودرو خودداری کنید. گرما یا سرمای زیاد و همچنین رطوبت ممکن است سبب آسیب دیدن ادله شوند.

پ: دقت داشته باشید که رایانه‌ها و یا سایر تجهیزاتی که به هر دلیل بسته بندی نشده اند وضعیت مطمئنی در داخل خودرو داشته باشند و از هرگونه تکان و لرزشی در امان باشند. به عنوان مثال کیس و صفحه نمایش را می توان روی صندلی قرار داد و آنها را به وسیله کمربند در جای خود محکم کرد.

ج: از ادله حین حمل و نقل به دقت مراقبت کنید.

روند نگهداری

۱: مطمئن شوید که ادله بر اساس قوانین سازمان نگهداری شوند.

۲: ادله را در جای مناسبی دور از هرگونه حرارت و رطوبتی نگهداری کنید و آنها را در برابر هرگونه منبع مغناطیسی، رطوبت، گرد و غبار و سایر مواد مضر دور نگه دارید.

توجه: دقت کنید که ادله بالقوه مانند تاریخ، ساعت و تنظیمات سیستم ممکن است در اثر نگهداری طولانی مدت از بین بروند. با توجه به اینکه باطری‌ها دارای عمر محدودی هستند بنابراین با اتمام شارژ آنها ممکن است این داده‌ها را از دست بدهیم. بنابراین باید به پرسنل مسئول (مانند نگهبان، رئیس آزمایشگاه و یا کارشناسان تجزیه و تحلیل ادله) نسبت به اینکه اینگونه ادله نیاز به توجه و رسیدگی فوری دارند آگاهی لازم داده شود.

نتیجه‌گیری:

بررسی صحنه‌های جرم الکترونیکی به لحاظ ماهیت بسیار شکننده و فراری که این گونه از

ادله دارند نیاز به دقت فراوان و داشتن اطلاعات کافی دارد و هر اقدام اشتباهی در این راه در واقع قدمی بی بازگشت خواهد بود لذا یک کارشناس در بررسی صحنه‌های جرم الکترونیک باید ابتدا دانش لازم در این خصوص را کسب نماید سپس با استفاده از این دانش به صحنه جرم قدم بگذارد. باید یادآور شـد که لزومی ندارد یک کارشـناس بررسـی صحنه‌های جرم الکترونیکی از دانشی در سطح یک کارشناس جرایم رایانه ای بر خوردار باشد بلکه با توجه به مطالب گفته شـده در این مقاله باید حداقل شـناخت کافی در خصوص انواع و ارزش ادله الکترونیکی و نحوه رویارویی با آنها را داشته باشد.

منابع:

- [1] Ashcroft ,John(2001) Electronic crime scene investigation for first responders
- [2]Shitz, Michel (2007)Computer Forensics ,Wiley
- [3]Angus Marshall (2008) Digital Forensics
- [4]Linda Volonion and Reynaldo anzaldua (2009)Computer Forensics
- [5]Robin bryant (2008)Digital Crimes
- [6] Carolyn M. Burns, Jeff Morley, Richard Bradshaw and José Domene(2008) The Emotional Impact on and Coping Strategies Employed by Police Teams Investigating Internet Child Exploitation
- [7] Luc Small(2007) Theft in a wireless world