بسم الله الرحمن الرحیم

راهنمای پزشکی قانونی و تحقیقات رایانه ای

مترجمان:

دکتر وحید خطیبی بردسیری

(عضو هیات علمی دانشگاه آزاد اسلامی واحد بردسیر)

مهندس بهروز صادقی

(عضو هیات علمی دانشگاه پیام نور استان خراسان رضوی واحد تایباد)

مهندس فرزاد حسین زاده پیر غیبی

(عضو هیات علمی دانشگاه آزاد اسلامی واحد بندر لنگه)

مهندس منیره اسفندیاری

(مدرس دانشگاه پیام نور استان خراسان رضوی واحد تایباد)

انتشارات ارسطو

(چاپ و نشر ایران)

۱۳۹۳

سرشناسه : نلسون، بیل
Nelson, Bill
عنوان و نام پدیدآور : راهنمای پزشکی قانونی و تحقیقات رایانه‌ای
مشخصات نشر : مشهد: ارسطو، ۱۳۹۴.
مشخصات ظاهری : ۵۳۰ ص.: مصور، جدول، نمودار
شابک : ۴-۵۸-۷۵۵۸-۶۰۰-۹۷۸
وضعیت فهرست نویسی : فیپای مختصر
یادداشت : فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
شناسه افزوده : فیلیپس، آملیا Phillips، Amelia
شناسه افزوده : استوارت، کریستوفر Steuart، christopher
شناسه افزوده : خطیبی بردسیری، وحید ، ۱۳۶۰-، مترجم
شناسه افزوده : صادقی، بهروز ، ۱۳۶۱-، مترجم
شناسه افزوده : حسین زاده پیر غیبی، فرزاد ، ۱۳۶۱-، مترجم
شماره کتابشناسی ملی : ۳۷۹۱۷۸۲

نام کتاب : راهنمای پزشکی قانونی و تحقیقات رایانه‌ای
مترجمان : وحید خطیبی بردسیری - بهروز صادقی - فرزاد حسین زاده پیر غیبی
منیره اسفندیاری
ویراستار: سرکار خانم مهندس منیره اسفندیاری
ناشر : ارسطو (چاپ و نشر ایران)
صفحه آرایی ، تنظیم و طرح جلد : پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۳۹۳
چاپ : مهتاب
قیمت : ۴۵۰۰۰ تومان
شابک : ۴ - ۵۸ - ۷۵۵۸ - ۶۰۰ - ۹۷۸
تلفن های مرکز پخش : ۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۰۵۱
www.chaponashr.ir

فهرست مطالب

عنوان **صفحه**

پیش گفتار

امروزه با رشد فزاینده فضای مجازی و امکانات فراهم شده توسط شبکه های اینترنتی، باید گفت جوامع بشری هرچند از مزایای گوناگون و منحصربه فردی برخوردار شده اند اما از طرفی همین ارائه تسهیلات و امکانات در مواردی می‌تواند فضایی را برای مجرمین این حوزه فراهم نماید تا با سوء استفاده از ناآگاهی افراد جامعه، به اهداف شوم خود دست یابند، بطوریکه بر اساس آمار رسمی، رشد جرایم رایانه ای و خصوصا جرایم مرتبط با فضای مجازی در کشورعزیزمان ایران، نسبت به دیگر انواع جرایم، قابل ملاحظه و چشمگیر می باشد. پزشکی قانونی رایانه ای در حقیقت بیان و بررسی شیوه های موجود ایمن سازی امکانات و داده های رایانه ای در مقابل نفوذ متجاوزین خارجی، دسترسی ها و شنودهای غیر مجاز، جاسوسی از داده های رایانه ای و نامه های الکترونیکی و تلفن همراه، سرقت‌های رایانه ای، جرایم مرتبط با عفت و اخلاق عمومی جامعه، هتک حیثیت و نشر اکاذیب، چگونگی پردازش صحنه های وقوع جرم و جنایت را شامل می‌شود. نوشتار حاضر که حاصل سالها تجربه و تجزیه و تحلیل روش‌های پزشکی قانونی رایانه ای می‌باشد، سعی دارد ضمن تبیین اصول و مبانی پزشکی قانونی رایانه ای، با معرفی نرم افزارهای تخصصی در این حوزه مانند ProDiscover Basic و FTK Imager که در زمینه کشف و برخورد با جرایم این حوزه بسیار مفید می باشند، به ارائه راهکارها و شیوه‌های نوین و به روز بپردازد.

امید است توانسته باشیم گامی مفید در جهت مقابله با جرایم رایانه ای و فضای مجازی برداشته باشیم.

بهروز صادقی

فصل اول:

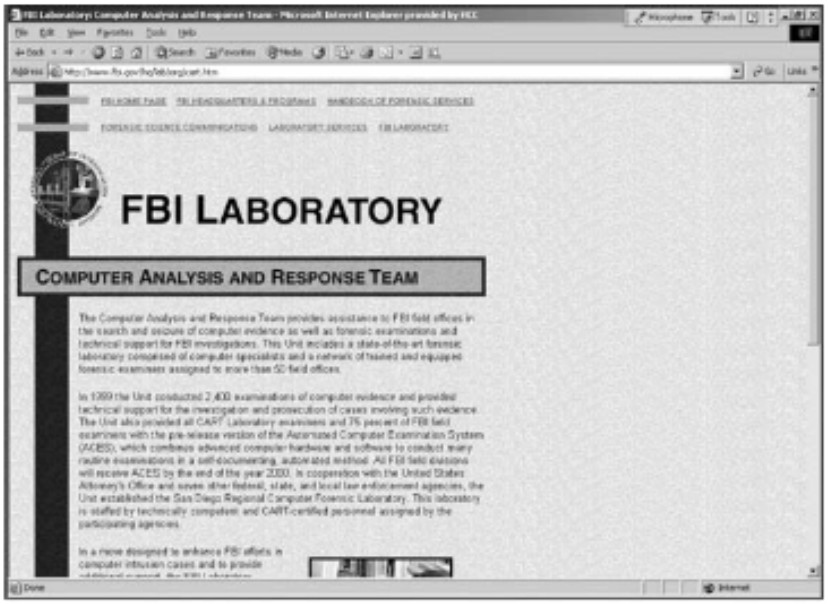
پزشکی قانونی و تحقیقات رایانه ای

به عنوان یک شغل

پس از مطالعه و تکمیل تمرینهای این فصل، قادر خواهید بود:

- پزشکی قانونی رایانه ای را تعریف نمایید.
- توصیفی از چگونگی آماده شدن برای انجام تحقیقات رایانه ای را ارائه داده و همچنین می توانید تفاوتهای بین تحقیقات شرکتی و تحقیقات آژانس ها و یا همان نهادهای اجرای قانون را بیان نمایید.
- می توانید اهمیت حفظ و انجام رفتارهای حرفه ای در این خصوص را بیان کنید.

درسالهای گذشته زمینه پزشکی قانونی و تحقیقات رایانه ای رشد چشمگیری داشته‌اند. این فصل، شما را با علم پزشکی قانونی و تحقیقات رایانه ای آشنا نموده و مسائل و مشکلات آنها را که در این صنعت شایع می‌باشند توصیف می‌کند. این کتاب روش‌های تحقیقات قدیمی‌را با تکنیکهای تحلیل وحل مساله سیستم‌های قدیمی‌وکلاسیک ترکیب کرده و آنها را به تحقیقات رایانه ای اعمال می‌کند. درک کاملی از این قوانین به همراه استفاده از ابزارهای پزشکی قانونی رایانه ای از شما، یک تحلیلگر مجرب وکار آزموده ای در زمینه پزشکی قانونی رایانه ای خواهد ساخت.



شکل ۱-۱- آزمایشگاه پلیس ایالتی آمریکا

آشنایی با پزشکی قانونی رایانه ای

داده‌ها و مستنداتی که در یک رایانه ذخیره می‌گردند بسته به طبیعتی که دارند، توسط قوانین مختلفی مورد حمایت و نظارت هستند. که در این حالت، بسیاری از قوانین قابل اعمال به شواهد دیجیتال (رقمی) بواسطه پرونده‌های موجود در دادگاه‌های ایالتی و فدرال تنظیم شده‌اند. متمم چهارم در قانون اساسی آمریکا حق هرکدام از افراد جامعه را در خصوص داشتن امنیت در حوزه‌های مختلف شخصی، مسکونی، مالکیت و ... محترم شمرده و اجازه نمی‌دهد به طور مثال مورد جستجو، تحقیق و یا مصادره و تصرف قرار گیرند. با ادامه رشد مفاهیم فقهی در این متمم که نقش مهمی را در تعیین اینکه آیا تحقیق و تفحص در خصوص شواهد رقمی‌نیز صورت پذیرد یا خیر، تضمین جستجو در این خصوص را بررسی می‌کند. هر چند زمانیکه می‌خواهیم در باب یک پرونده جنایی به دنبال شواهد بگردیم بسیاری از محققان هنوز رایانه مضنون و محتوی آن را بصورت خاص در نظر گرفته تا از مشکلات بعدی جلوگیری کنند. در یک پرونده خاص و قابل توجه، دیوان عالی ایالت پنسیلوانیا انتظارات مردم درخصوص حریم خصوصی را مورد بررسی قرار داد. تحقیقات اصلی و اولیه صورت گرفته توسط پلیس FBI، پلیس ایالتی و پلیس محلی منجر به کشف یک سری از یادداشتها و دستورالعمل‌های تولید شده توسط رایانه شدکه همگی آنها با یکدیگر مرتبط بودند و همه آنها در داخل ویا خارج منطقه بصورت کاملا حرفه ای پنهان سازی شده بودند. تحقیقات صورت گرفته نتایج بهتری را نیز در خصوص مضنونین احتمالی نشان داد. مثلا اینکه DAVID COPENHEFER که در همان نزدیکی صاحب یک کتاب فروشی بوده و با قربانی همسرش رابطه شخصی داشته بود، می‌تواند به عنوان یک مضنون مطرح شود. بررسی و تحلیل زباله‌های مغازه COPENHEFER نشان می‌داد که علائمی‌از باج گیری موجود می‌باشد. جستجوهای بعدی شواهد بیشتری را بر علیه او به نمایش گذاشت. بطوریکه شواهد و مستنداتی مبنی بر تماس وی با قربانی در روز سه شنبه بدست آمد. و نیز تماس با همسر مقتول در روز جمعه، یادداشتهای باج‌گیری دیگر دنباله‌ای ازیادداشتهای مخفی پی در پی درانتها نقشه کلی عملیات گروگان گیری دردادگاه تجدیدنظر، دادگاه عالی پنسیلوانیا به این نتیجه رسید که شواهد فیزیکی، از

جمله شواهد پزشکی قانونی رایانه ای، برای مجرم دانستن کتاب فروش کافی می‌باشد. استدلال COPENHEFER این بود که: هرچند رایانه او به صورت قانونی و به موجب حکم توسط پلیس مورد بررسی قرار گرفته است، تلاش برای پاک کردن سوالاتی که از او پرسیده شده است همگی جزء قوانینی است که توسط متمم قانون اساسی تصویب شده است. این در حالی بود که دادگاه عالی ادعای وی را ردکرده و گفته بود: تلاش وی برای مخفی کردن شواهد و قراین این جرم هیچ تناسب قانونی با مفهوم قانون خصوصی افراد ندارد. اینکه فرد تصوری از قانون داشته باشد دلیل این نیست که واقعا قانونی می‌باشد که اگر اینطور بود دیگر نیازی به تحقیق و پی گیری جرایم نبود. امروزه تقریبا هر حوزه قضایی ایالات متحده پرونده‌هایی دارد که به نوعی مرتبط با شواهد وادله رایانه ای می‌باشد. قوانین جنایی دولت کانادا نیز در اصل حالت، فدرال داشته و عموما در دادگاه‌های ایالتی به اجرا در می‌آید.

پزشکی قانونی رایانه ای درمقابل دیگر رشته‌های مرتبط

بر اساس گفته‌های شرکت سهامی‌خاص DIBSVSA که یک شرکت خصوصی در آمریکا می‌باشد و در زمینه پزشکی قانونی رایانه به صورت تخصصی فعالیت می‌کند، پزشکی قانونی رایانه به صورت تخصصی فعالیت می‌کند، پزشکی قانونی رایانه ای یعنی جمع آوری و تحلیل علمی‌داده‌های ذخیره شده روی رسانه‌های ذخیره سازی رایانه ای، بطوریکه این داده‌های جمع آوری شده و نتایج تحلیل شان به عنوان شواهد مستند در دادگاه مورد استفاده قرار گیرند. البته شما می‌توانید تعریف مشابه به این راه در وب گاه FBI نیز به نشانی WWW.FBI.gov مشاهده کنید.

به طور معمول، تحقیق از رایانه‌ها شامل جمع آوری اطلاعات رایانه ای بصورت کاملا ایمن، بررسی داده‌های مضنون و مشکوک جهت تعیین جزئیات مانند منشا و محتوی، ارائه اطلاعات مبتنی بر رایانه به دادگاه و سرانجام اعمال قوانین به اقدامات رایانه ای صورت گرفته می‌باشد . بطور کلی، پزشکی قانونی رایانه ای داده‌هایی را که می‌توانند از هارددیسک یک رایانه یا یک رسانه ذخیره سازی دیگر بازیابی شوند را مورد بررسی قرار

می‌دهد.

محققان رایانه ای به مانند یک باستان شناس که یک سایت را حفاری می‌کنند، اطلاعات را از یک رایانه و یا مولفه‌های رایانه ای بازیابی می‌کنند. اطلاعات بازیابی شده شاید قبلا نیز روی هارد ذخیره شده باشند اما کشف و یا پیدا کردنشان راحت به نظر نمی‌رسد. در مقابل، پزشکی قانونی رایانه ای اطلاعاتی را در خصوص اینکه چگونه یک مهاجم یا هکر برنامه ریزی می‌نماید تا به شبکه خاصی نفوذ کند را جمع آوری می‌نماید. محققان متخصص در زمینه پزشکی قانونی رایانه ای سعی می‌کنند با بررسی فایل‌های تعیین وضعیت رایانه ای به اطلاعاتی درخصوص نحوه هجوم هکرها به شبکه دسترسی یابند، در این بین اطلاعاتی مانند اینکه کاربران چه زمانی و چگونه وارد شبکه شده اند و یا به چه نشانی‌های اینترنتی دسترسی یافته اند و یا حتی اینکه از چه مکانی وارد رایانه و یا شبکه راه دور شده اند نیز از اهمیت خاصی برخوردار می‌باشند . در نظر داشته باشید که، این متخصصان سعی دارند بفهمند که چه پرونده‌هایی از سارقان و هکرها باقی مانده و یا آنها چه تغییراتی را در رایانه قربانی شده صورت داده اند. در فصل ۱۱ اینکه کجا و چگونه بایستی از نتایج پزشکی قانونی رایانه ای استفاده شود توضیح داده می‌شود. از طرفی دیگر، پزشکی قانونی با مفهوم بازیابی داده‌ها که در رایانه‌ها رخ می‌دهد متفاوت است. چرا که بازیابی داده یعنی اینکه اطلاعاتی که به صورت اشتباه و یا در اثر یک حادثه مثل قطع جریان برق، پاک شده اند را بتوانیم بازیابی کنیم با این هدف که مطمئن باشیم داده بدست آمده آنقدر معتبر باشد که بتوان از آن به عنوان سند و شاهدی در مراجع قانونی استفاه کرد. این شواهد می‌توانند "تهمت‌آمیز" و یا "تبرئه آمیز" باشند.

محققان پزشکی قانونی زمانی که یک دیسک را به عنوان مثال بررسی می‌کنند از قبل مطمئن نیستند که حاوی اطلاعات مهمی‌باشد ولی سعی می‌کنند با بررسی و جستجوی رسانه‌های ذخیره سازی و داده‌های یافت شده احتمالی آنها را کنار یکدیگر گذاشته تا بتوانند به عنوان سند و مدرک ارائه دهند. ابزارهای نرم افزاری پزشکی قانونی رایانه‌ای دراکثرموارد و پرونده‌ها قابل استفاده می‌باشند. در موارد بسیار مهم حتی، محققان می‌توانند ازمیکروسکوپ های الکترونیکی برای بررسی دقیق فضای ذخیره سازی اطلاعات

که احتمالا به صورت عمدی خراب شده و یا قالب بندی مجدد شده اند بهره ببرند. هر چند که این روش هزینه بر نیز می‌باشد.

به مانند شرکت‌هایی که متخصص در زمینه بازیابی داده‌ها هستند شرکتهایی نیز هستند که در زمینه بازیابی فاجعه تخصص دارند و سعی می‌کنند از داده‌های حاصل از پزشکی قانونی رایانه‌ای جهت بازیابی اطلاعاتی که مشتریانشان از دست داده اند بهره ببرند که عموما سعی دارند از تکنیکهایی مانند گرفتن پشتیبان از داده‌ها، استفاده از سامانه‌های برق پشتیبان (UPS) و نظارت بر خطر جهت جلوگیری از پاک شدن احتمالی اطلاعات استفاده کنند.

محققان عموما به صورت گروهی کار می‌کنند بطوریکه وظیفه آنها در سه بخش زیر آورده می‌شود:

- ارزیابی آسیب پذیریی و مدیریت ریسک
- تشخیص نفوذ به شبکه و پاسخ به حوادث
- تحقیقات رایانه ای

شکل ۱-۲ سه گانه تحقیقات

پاسخ نفوذ

هر ضلع از این مثلث بیانگر یک گروه ویا یک نهاد می‌باشند که مسئول اجرای وظیفه مرتبط با خودشان هستند. هر چند که هرکدام نیز بصورت مستقل عمل می‌کنند اما وقتی یک تحقیق وسیع لازم باشد با یکدیگر همکاری دارند. با ترکیب این گروه‌ها با یکدیگر و ایجاد یک تیم واحد بدون نیاز به متخصص از دیگر مراکز، می‌توان تمامی‌جنبه‌های حتی با فناوری‌های برتر را در خصوص تحقیقات رایانه ای بررسی وانجام داد.

عبارت "محیط شبکه‌های سازمانی" به سامانه‌های محاسباتی اشتراکی بزرگ اشاره دارد که ممکن است شامل سیستم‌های مستقل و متفاوت نیز باشند. در شرکتهای کوچکتر، یک گروه ممکن است تمامی‌وظایف موجود در آن مثلث را به تنهایی انجام دهد و یا برای انجام آنها با یک شرکت کوچک دیگر حتی وارد عقد قرارداد گردد. زمانی که یک نفروارد گروه ارزیابی آسیب‌پذیری و مدیریت ریسک می‌گردد بایستی درابتدا جامعیت ایستگاه‌های کاری ایستاده آنها و سرویس دهنده‌های شبکه را مورد آزمایش و اعتبار سنجی قرار دهد.که خود شامل بررسی امنیت فیزیکی سیستم‌ها و سیستم‌های عامل آنها و احتمالا نرم افزارهای کاربردی شان می‌شود. کسانی که در این گروه کار می‌کنند آسیب پذیری سیستم‌های عامل و برنامه‌های کاربردی آنها را بررسی می‌کنند و خود سعی می‌کنند با نفوذ و حمله به این شبکه‌های خودی، آسیب پذیری آنها را در مقابل حملات جانبی مورد ارزیابی قرار دهند که البته این افراد خود سالیان سال در سیستم‌های عامل یونیکس و مدیریت ویندوز تجربه کافی کسب نموده اند. این افراد همچنین بایستی مهارتهای لازم را در تشخیص نفوذ به شبکه‌ها و پاسخ‌دهی به حوادث مختلف کسب کنند. این افراد با بررسی فایل‌های سیستمی‌حوادث را رصد می‌کنند. زمانیکه یک حمله خارجی تشخیص داده شد این متخصصین سعی می‌کنند ضمن رویارویی، مکان یابی و تشخیص روش حمله، دسترسی بیشتر به شبکه را مانع شوند و سپس مدارک لازم را جمع آوری می‌نمایند تادر دعاوی قضایی مورد استفاده قرار گیرند. منظور از دعاوی قضایی یعنی، مراحل قانونی صدور مسئولیت کیفری و یا مدنی در دادگاه صالح. اگر در یک فعالیت غیر قانونی یک کاربر داخلی نیز مشارکت داشته باشد تیم تشخیص نفوذ و پاسخ ده به حمله، با مکان یابی

کاربر مربوطه و مسدود کردن دسترسی او به شبکه، پاسخ مناسب را به این گونه حملات می‌دهند. بطور نمونه، اگر یک فرد در یک شبکه اجتماعی یک نامه الکترونیکی نامناسب را به دیگر کاربران آن شبکه ارسال نماید افراد متخصص تشخیص می‌دهند که این نامه از یک گروه داخل شبکه خودشان ارسال شده است پس یک تیم متخصص امنیتی را به محل اعزام می‌کنند. کارکنانی که در زمینه ارزیابی آسیب پذیری عمل می‌کنند معمولا بطور چشم گیری با قسمت تحقیقات رایانه ای همکاری دارند. تیم تحقیقات رایانه ای، تحقیقات را مدیریت کرده و تحقیقات پزشکی قانونی صورت گرفته در زمینه سیستم‌هایی که مشکوک به حمله هستند را نیز تحلیل و مدیریت می‌کند.

درک مفهوم "قانون موردی/ قانون مبتنی بر پرونده"

از آنجاییکه سرعت رشد رایانه و فناوری‌های مربوط به رسانه‌های دیجیتال (رقمی) بسیار زیاد می‌باشد قوانین و اساسنامه‌های موجود فعلی نمی‌توانند با نرخ این تغییرات خود را تطبیق دهند. بنابراین وقتی که هیچ اساسنامه و یا حتی قانون خاصی وجود ندارد، از مفهوم "قانون موردی" برای حل مساله کمک می‌گیریم. " قانون موردی" به مراجع قانونی اجازه می‌دهد تا از تجربه پرونده‌ها و موارد قبلی که مشابه پرونده فعلی می‌باشد استفاده نمود و ابهامات موجود در قوانین را اشاره و مورد بررسی قرار داد. هر پرونده جدید بر اساس مسائل خاص خودش ارزیابی می‌گردد. دانشگاه رودایسلند بسیاری از موارد و پرونده‌هایی را که در گذشته اتفاقات افتاده اند را در خود نگهداری می‌کند. مثلا در مورد وب‌گاه‌ها می‌توان به مورد زیر اشاره نمود که : یک محقق با داشتن حکم بازرسی مربوط به خرید و فروش مواد مخدر می‌تواند پرونده‌های یک رایانه را مشاهده نماید. اما این در حالی است که او همزمان با این کار مثلا تصاویر مرتبط با آزار جنسی کودکان را نیز دنبال می‌کند. و او به جای اینکه منتظر بماند تا حکم جدید دراین مورد را نیز دریافت نماید جستجوی خودرا ادامه می‌دهد. در نتیجه تمام شواهد مرتبط با این تصاویر از بین می‌رود. در اینجا است که باید گفت برای جلوگیری از تکرار چنین وقایعی، محققان باید از احکام جدید و تازه مطلع باشند. به یاد داشته باشید که البته، "قوانین موردی" نباید منجر به ایجاد جرائم

جنایی جدید گردند.

توسعه منابع پزشکی قانونی رایانه ای

یک محقق مدارک پزشکی قانونی رایانه ای موفق کسی است که بتواند با بیش از یک محیط رایانه ای آشنا شده و کار کند. مثلا علاوه براینکه با سیستم‌های عاملی مانند داس و یا ویندوز آشنا بوده وکار می‌کند باید بتواند با محیط‌های دیگر مانند لیناکس، مکینتاش و ... نیز تعامل داشته باشد. البته که نمی‌توان کسی را یافت که در همه زمینه‌های رایانه متخصص باشد. هرچند شاید یک محقق در مورد فناوری موضوعی که در مورد آن در حال تحقیق می‌باشد هیچ اطلاعاتی نداشته باشد که برای موفق بودن در این زمینه حتمابایستی با افراد حرفه ای در زمینه‌های رایانه، شبکه، برنامه نویسی و... در ارتباط بود. می‌توان فهرستی از افراد متخصص را با در نظر گرفتن نوع تخصص‌شان و پروژه‌های اخیری که با هم کار کرده اند را نیز تهیه نمود تا در موقع لزوم از آنها استفاده نمود.

می‌توان به گروه‌های رایانه ای دولتی و یا حتی خصوصی بپیوندیم. مثلا در پسفیگ نورس رست گروهی بنام CTIN تشکیل شده است که ماهانه با یکدیگر قرار ملاقات گذاشته و در خصوص مشکلاتی که مجریان قانون با آنها مواجه می‌شوند با یکدیگر به بحث و تبادل نظر می‌پردازند. که البته این سازمان غیر انتفاعی در امر آموزش رایگان نیز اقدامات خوبی انجام داده است. پس شما می‌توانید در منطقه خودتان یک چنین گروهی را ایجاد نمایید. مانند سازمان (HTCIA) که در زمینه امنیت و تحقیقات رایانه ای با دیگران به تبادل اطلاعات می‌پردازد. بعلاوه شما می‌توانید گروهی از متخصصانی را که با آنها تا به حال کار کرده اید را تشکیل داده و با استفاده از روشهای ارتباطی جدید مانند پست الکترونیک با آنها در ارتباط باشید به عبارتی شما بایستی روابط حرفه ای با افرادی که در یک زمینه فنی متفاوت از حوزه تخصصی خودتان، متخصص می‌باشند را پرورش دهید. مثلا اگر شما در زمینه سیستم عامل ویندوز تخصص دارید می‌توانید با افرادی که تخصص آنها در زمینه سیستم‌های عامل دیگری مانند لیناکس، یونیکس و یا مکینتاش می‌باشد ارتباط کاری برقرار نمایید.این گروه‌های کاربردی می‌توانند بسیار مفید باشند به

ویژه زمانیکه شما نیاز به اطلاعاتی در مورد سیستم‌های عامل مهم دارید.

بطور مثال می‌توان به یک رسوایی اخلاقی که در سال ۱۹۹۶ اتفاق افتاد اشاره کرد. در این رسوایی که توسط یک گروه کاربری حرفه‌ای کشف شد فرد مضنون ضمن نصب دوربین‌های تصویری در یک مکان خاص و با فراهم آوردن اسباب لهو و لعب برای خانم‌ها و کودکان از آنها در حین ارتکاب به امور غیر اخلاقی فیلمبرداری نموده و سپس ازاین تصاویر برای باج گیری از این افراد استفاده می‌کرده است. از آنجائیکه این فرد برای انجام امورش به رایانه نیز نیاز داشته است سیستم عامل COCODOS را برای این کار انتخاب نموده بود که چندین سال است منسوخ شده و به کار برده نمی‌شود.

بطوریکه داده‌های جمع آوری شده توسط محققان پزشکی قانونی، برایشان قابل فهم نبود لذا آنها با یک تیم کاربردی متخصص که در این زمینه قبلا تجارب خوبی داشته بودند ارتباط برقرار کرده و توانستند به کمک آنها به داده‌ها واطلاعات قابل فهمی‌از رایانه این فرد، دسترسی یابند. که در این رایانه، اطلاعات مربوط به جزئیات حوادث این چنینی مربوط به بیش از ۱۵ سال فعالیت مجرمانه با سوء استفاده از بیش ۴۰۰ خانم، ذخیره شده بود درانتها باید به این نکته اشاره کرد که اگر این همکاری صورت نمی‌گرفت منجر به این نمی‌شد که صدور حکم بسیار سنگینی برای این فرد مجرم و خلاف کار صورت پذیرد.

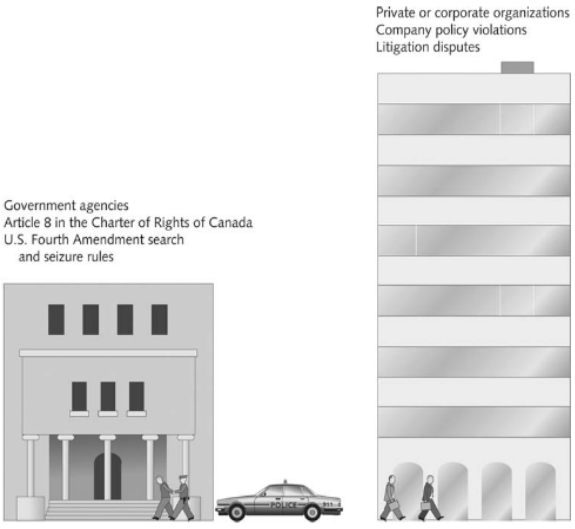
متخصصان خارجی در بسیاری از موارد که با شواهد دیجیتال سروکار دارند می‌توانند اطلاعات بسیار مفید و همراه با جزئیاتی را برای شما فراهم آورند. بطور مثال یک پرونده قتل که اخیرا اتفاق افتاد یک زن و شوهر که صاحب مغازه فروش محصولات شرکت مکینتاش بودند مورد بررسی قرار گرفت. در این پرونده ، پیکر بی جان زن مغازه دار درحالی (احتمالا مقتول) کشف شده بود که قصد متارکه با همسرش را داشته است اما به دلیل اعتقادات مذهبی از انجام این کار منصرف شده بود.

پلیس محلی حکم بررسی و تفحص از منزل و رایانه‌های آنها را در اختیار گرفت. زمانیکه کارآگاه به رایانه‌های آنها برای بررسی محتوی مراجعه نمود متوجه شدکه دیسک سخت ابتدا فشرده سازی شده و سپس اطلاعات آن پاک شده است. پس از برقراری ارتباط با یک متخصص سیستم‌های مکینتاش، این متخصص دو برنامه کاربردی که ازآنها برای فشرده

سازی اطلاعات استفاده شده بود را تشخیص دادند پس با بررسی اطلاعات بازیابی شده توسط این دو نرم‌افزار به یک فایل متنی دست پیدا نمودند که نشان می‌دهد همسر این زن به قتل رسیده، مبلغ ۳۵ هزار دلار برای خریدکوکائین و امور غیر اخلاقی هزینه کرده است. این شواهد دلایل کافی برای متهم به قتل عمد نمودن این مرد را به همراه داشت. همچنین می‌توان از تجارب و اطلاعات گروه‌های خبری، فهرستهای پست الکترونیک، روزنامه‌ها و موارد مشابه دیگر که در زمینه پزشکی قانونی رایانه ای فعالیت دارند بهره برد تا از کارشناسان این زمینه مشاوره‌های لازم را دریافت نمود. مثلا در یک پرونده، پس از بررسی صحنه جرم کارآگاهان نتوانسته بودند که به اطلاعات کدگذاری شده در یک رایانه مدل اینتل دسترسی پیدا کنند. آنها با تعریف مشخصات این مساله، یک نامه الکترونیک به فهرست پست‌های الکترونیک فرستادند و یکی از این اعضا توانسته بود مشکل را حل کند.

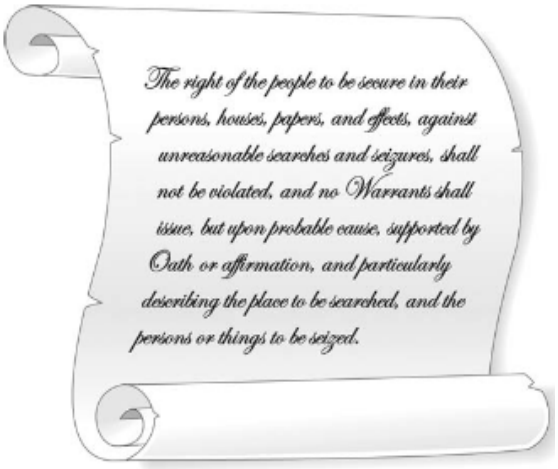
آماده شدن برای تحقیقات رایانه ای

تحقیقات و پزشکی قانونی رایانه ای از جهات مختلفی دسته بندی می‌شوند اما در این مبحث به دو دسته کلی زیر میتوان اشاره کرد: تحقیقات عمومیو تحقیقات خصوصی یا همان تحقیقات شرکتی.



شکل ۳-۱. تحقیقات عمومی و خصوصی

تحقیقات عمومی یعنی همان سازمان‌های دولتی که مسئولیت تحقیقات جنایی و پیگردهای قانونی را بر عهده دارند. سازمان‌های دولتی شامل سازمان‌های پلیسی محلی، شهرستانی، استانی و یا دولتی و حتی سازمان‌های فدرال نظارتی و اجرایی می‌باشند.



شکل ۴-۱- متمم چهارم قانون اساسی ایالات متحده آمریکا

قانون تحقیق و جستجو از حقوق افرادی که احتمالا مضنون به ارتکاب یک جرم هستند حمایت می‌کند. شما به عنوان یک محقق رایانه ای بایستی از عمل به این قوانین مطمئن باشید. البته اطلاعات به روز شده مربوط به این قانون توسط وزارت دادگستری در وب‌گاه (WWW.Vsdoj.gov) آن قابل مشاهده می‌باشد. در حالیکه تحقیقات عمومی‌معمولا شامل پرونده‌های جنایی و سازمانهای دولتی می‌باشد تحقیقات خصوصی بیشتر مرتبط با شرکت‌های خصوصی سازمان‌های دولتی غیر اجرایی قانونی و وکلا می‌باشند.

این سازمانهای خصوصی بصورت مستقیم توسط قوانین جنایی و یا موارد مرتبط با متمم چهارم قانون اساسی مدیریت نمی‌شوند بلکه مدیریت اصلی آنها بر اساس سیاستهای داخلی می‌باشد که رفتار مورد انتظاراز یک کارمند را در محیط کاری اش تعریف می‌کند. تحقیقات این شرکتهای خصوصی در مواردی می‌تواند شامل دادخواهی نیز باشد. هرچند تحقیقات خصوصی معمولا مرتبط با پرونده‌های مدنی می‌باشد اما یک پرونده مدنی خود می‌تواند تبدیل به یک پرونده جنایی گردد و البته یک پرونده جنایی نیز میتواند منجر

به یک پرونده مدنی گردد. اگر شما روند پزشکی قانونی رایانه ای خوبی را طی نمایید شواهدی را که در بررسی‌های خود به آنها دست می‌یابید را می‌توانید در جابجایی بین پرونده‌های مدنی و جنایی مورد استفاده قرار دهید.

آشنایی با تحقیقات آژانس‌ها و سازمان‌های مجری قانون

هنگام انجام تحقیقات رایانه ای عمومی، شما باید با قوانین شهری، شهرستانی، ایالتی، استانی و یا حتی فدرال و ملی درخصوص جرایم مرتبط با رایانه آشنا گردید از جمله اینها می‌توان به فرآیندهای قانونی استانداردسازی و ایجاد یک پرونده جنایی اشاره نمود. در یک پرونده جنایی، فرد مضنون معمولا برای مواردی مانند دزدی، قتل و غارت و یا کلاهبرداری مورد تحقیق و بازجویی قرار می‌گیرد. مثلا برای اینکه محقق (کارآگاه) متوجه شود که آیا یک جرم رایانه ای رخ داده است یا خیر می‌تواند سوالاتی مانند سوالات زیررا بپرسد:

برای ارتکاب جرم از چه ابزارهایی استفاده شده است؟

آیا این عمل به نوعی یک تجاوز ساده محسوب می‌شود؟

این جرم آیا یک دزدی، دزدی خانگی و یا یک خرابکاری بوده است؟

آیا مجرم با استفاده از ابزارهای فضای مجازی شنودی را انجام داده یا پست الکترونیک افراد را مورد حمله و استراق سمع قرار داده است؟

برای ارتکاب جرایم عموما رایانه‌ها و شبکه‌ها تنها ابزاری هستند که می‌توانند مورد استفاده قرار گیرند که ازاین نقطه نظر دقیقا شبیه به همان شاه کلیدهایی هستند که یک دزد خانگی برای ورود به یک خانه از آنها استفاده می‌کند. به همین دلیل, بسیاری از استانها سعی کرده اند برای نشان دادن اینکه یک جرم بوسیله رایانه انجام گرفته است زبانهای خاصی را برای کدگذاری جرایم معرفی نمایند. به این دلیل آنها تعاریف قانون را برای جرایم گسترش داده و بطور نمونه این معنا را به کلمه دزدی اضافه کرده اند که : جمع آوری داده‌های یک رایانه بدون اینکه صاحب آن رایانه اجازه داده باشد به طوری

که الان در کنار دزدان خانگی یا سارقان ماشین، سارقان رایانه ای نیز شکل معنایی پیدا کرده‌اند. بعضی ازایالتها نیز قوانین واحکام جزایی خاصی را تعیین کرده اند که جرایم مرتبط با رایانه را مورد خطاب و بررسی قرار می‌دهند. اما از طرفی، آنها مسائل مرتبط با رایانه‌ها مانند استانداردها و قوانین تجاوز، سرقت، خرابکاری و دزدی خانگی را در این قوانین لحاظ ننموده اند. در سال ۱۹۸۶(۲۷سال پیش) قوانین مرتبط به تخلف و تقلبهای رایانه ای به تصویب رسیده است اما تا چندی بعد، برخی از قوانین دولتی آن شکل واقعی به خود نگرفت. تا به امروز، بسیاری از قوانین ایالتی مرتبط با جرم و جنایت‌های رایانه‌ای هنوز در دادگاه‌ها در مرحله آزمون و خطا به سر می‌برند. در بسیاری از جرایم مهم و جدی، رایانه‌ها نقش آفرینی دارند که شناخته ترین آن، مربوط به سوء استفاده جنسی از افراد زیر سن قانونی می‌باشد. تصاویر دیجیتال (رقمی) که روی رسانه‌های ذخیره‌سازی مانند لوح‌های سخت، لوح‌های فشرده، راه اندازهای USB و ... ذخیره سازی می‌شوند در فضای اینترنت به اشتراک گذاشته می‌شوند. از آنجاییکه اطلاعات مربوط به کودکان و حتی بزرگسالانی که گم شده اند نیز در رایانه‌ها ذخیره می‌شوند، این نگرانی نیز در حوزه جرایم رایانه ای وجود دارد که چنانچه این دست اطلاعات به سرقت روند، در مواردی فجایع غیرقابل جبرانی ایجاد خواهند شد. قاچاقچیان مواد مخدر نیز معمولا اطلاعات مربوط به تراکنش‌های کاری خود را روی رایانه‌های شخصی شان و یا دستیاران دیجیتال شخصی (PDA) نگهداری می‌کنند.

این اطلاعات نیز در موارد خاصی، بسیار مهم می‌باشند چرا که به ماموران اجرای حکم کمک می‌کنند تا فرد مضمون دستگیر شده را محکوم کرده و مکان دیگر دست اندرکاران خرید و فروش مواد مخدر را پیدا کنند.علاوه بر این، در بعضی از پرونده‌ها، ایمیل‌های حذف شده، تصاویر دیجیتال و دیگر مستنداتی که در یک رایانه ذخیره شده‌اند می‌توانند به حل یک پرونده کمک نمایند.

پی گیری یک روال حقوقی

هنگامی‌که شما در حال تحقیق رایانه ای بر روی رفع مناقضات بالقوه جنایی هستید،

روال حقوقی که شما در حال انجام آن هستید به مواردی مانند رسم و رسوم محلی، قوانین قوه مقننه و حتی قواعد مربوط به شواهد و مستندات بستگی زیادی دارد. هرچند که در حالت کلی، یک پرونده جنایی عموما سه مرحله را طی می‌کند : شکایت، تحقیق و بررسی و دادستان (شکل۷-۱).

شکل ۵-۱- جریان کاری یک پرونده عمومی

معمولاً این طور انجام می‌گیرد که یک نفر، شکایت را نوشته وآنرا به قالب یک فایل آماده می‌کند، سپس یک نفر متخصص آن شکایت را بررسی می‌کند و با کمک دادستان شواهد را جمع آوری و تشکیل پرونده می‌دهد و اگر ارتکاب جرمی‌صورت گرفته باشد پرونده در دادگاه مورد بررسی قرار می‌گیرد. زمانی یک تحقیق جنایی می‌تواند شروع گردد که کسی مدارکی از یک عمل غیر قانونی راپیدا کند یا شاهدی برای آن بیابد. "شاهد" و یا "قربانی" (که عموما از آن به عنوان "شاکی" یاد می‌شود)، اتهامی‌را نزد پلیس مطرح می‌کند یعنی که فرض می‌کند که جرمی اتفاق افتاده است. با این فرضیات، مامور پلیس ضمن گفتگو ومصاحبه با "شاکی"، گزارشی را نیز تهیه می‌کند.

اداره پلیس، گزارش را به جریان انداخته و فرمانده پلیس تصمیم می‌گیرد که آیا یک تحقیق پلیسی آغاز گردد و یا اینکه از توضیحات به این نتیجه می‌رسد که جرمی‌صورت نگرفته و صرفا یک اتفاق و یا حادثه رخ داده است و آنرا به بخش حوادث پلیسی واگذار می‌کند. در این قسمت رکوردهایی که سر نخ‌ها منجر شده به جرایم که قبلا اتفاق افتاده‌اند نگهداری می‌شوند. از آنجاییکه مجرمین عموما در انجام بزهکاری‌هایشان از یک ترفند

خاص استفاده می‌کنند این ترفندها را می‌توان در این بخش پیدا کرد. مخصوصا در جرایم با فناوری‌های بالا این اتفاقات را راحت‌تر می‌توان ردیابی و به کارآگاه و یا محقق پلیس ارائه نمود. که البته این بخش حوادث مجهز به سیستم‌های رایانه ای و مدیریت پایگاه داده شده‌اند و یافتن یک رکورد خاص امروزه به مراتب راحت تر از سیستم‌های کاغذی سنتی می‌باشد.

باید اشاره به این واقعیت داشت که همه ماموران پلیس که متخصص رایانه نیستند بلکه تعدادی از آنها تنها مبتدیان در این زمینه می‌باشند و یا تعداد اندکی هستند که فراگرفته‌اند چگونه می‌توان اطلاعات ذخیره شده را بازیابی نمود.

برای اینکه عملیات آموزش و عملیاتی این گروهها با یکدیگر متفاوت باشد گروه CTIN سه سطح از متخصصان اجرای قانون را تعریف کرده است:

سطح اول: جمع آوری شواهد و مستندات دیجیتال که توسط یک افسر پلیس حاضر در صحنه وقوع جرم می‌تواند انجام گردد.

سطح دوم: مدیریت تحقیقات با فناوری سطح بالا، آموزش به محققان در این زمینه که به دنبال چه باشند, یادگیری اصطلاحات رایانه ای و اینکه چه چیزهایی را می‌توان از یک سند دیجیتال به دست آورد و یا نمی‌توان. کارآگاهان که به این کار گمارده شوند معمولا پرونده را مدیریت می‌کنند.

سطح سوم: متخصصانی که آموزش می‌بینند تا شواهد و ادله دیجیتال را بازیابی نمایند که معمولا این کار توسط یک متخصص در زمینه پزشکی قانونی رایانه ای و یا بازیابی داده‌ها و یا حتی متخصصان پزشکی قانونی شبکه و محققان جرایم اینترنتی، صورت می‌پذیرد. این فردی که آموزش‌های لازم را دیده است بسته به پس زمینه و تجربه ای که در گذشته داشته است شاید به عنوان مسئول اصلی ومدیر یک پرونده انتخاب گردد.

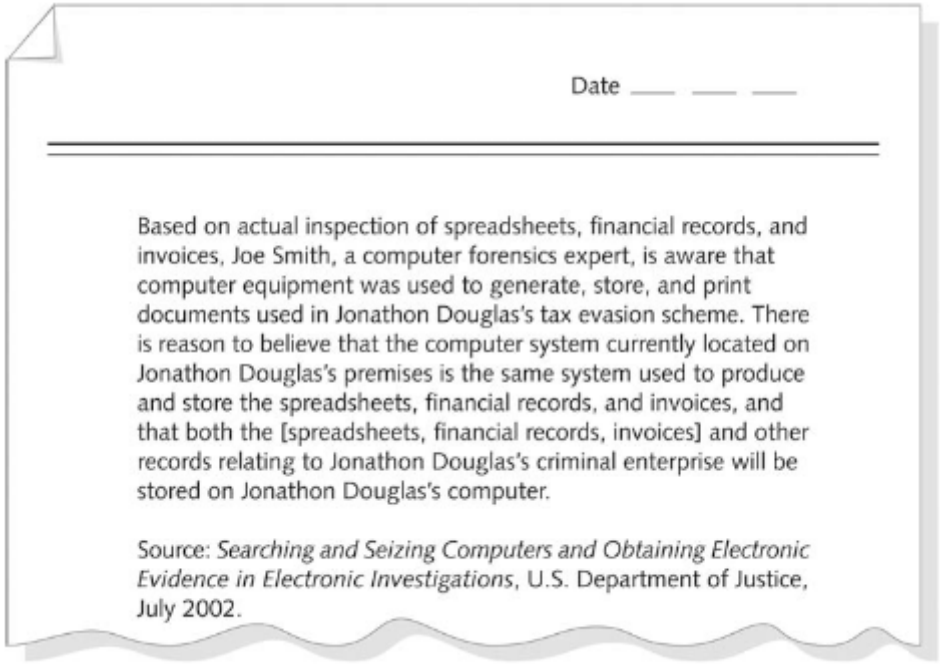
اگر شما به عنوان یک محقق در یک پرونده انتخاب شده اید ابتدا از سطح تخصص افرادی که با آنها کار می‌کنید اطلاع پیدا کنید. شما باید دوره‌های آموزشی سطح سوم را برگزار کنید تا تحقیقات را بدرستی انجام داده و جنبه‌های پزشکی قانونی این پرونده را

مدیریت کنید. شما با ارزیابی حوزه کلی پرونده که شامل شناخت سیستم عامل رایانه، سخت افزار و دیگر قطعات جانبی می‌شود شروع کنید. سپس بررسی کنید که آیا برای پردازش همه شواهد موجود، منابع لازم موجود هستند یا خیر؟ مثلا زمانیکه اطلاعات روی PDAها، گوشی‌های تلفن همراه و یا دیگر رسانه‌های همراه ذخیره شده باشند جمع آوری شواهد ومستندات، بسیار سخت تر می‌باشد. همچنین باید بررسی کنید که آیا ابزارهای مناسب جهت جمع آوری و تحلیل شواهد را در اختیار دارید و یا اینکه نیازمند این هستید که از دیگر متخصصان در زمینه جمع آوری وپردازش شواهد بهره ببرید.

پس از جمع‌آوری منابعی که لازم دارید شما بایستی تمامی‌امور مربوط به شاکی را انجام دهید. پس از تشکیل پرونده که شما آن را انجام داده اید اطلاعات به دادستان ارجاع داده می‌شود و وظیفه شما زمانی به پایان می‌رسد که تمامی‌شواهد دیجیتال را از رسانه‌های دیجیتال موجود به درستی جمع آوری و تهیه نموده باشید. به عنوان یک محقق، شما بایستی مدارک و مستندات جمع آوری شده را به همراه گزارش مربوطه به وکیل ارائه دهید. بسته به حال وهوای جامعه و نوع جرم ارتکاب شده، دادستان می‌تواند یک مدعی‌العموم، بازپرس قضایی، نماینده دولت دردادگاه مدعی العموم استانی یا کشوری، وکیل شهرستان و یا دادستان کشورتان باشد.در یک پرونده جنایی و یا عمومی اگر شما اطلاعات کاملی داشته باشید که بتوانید یک حکم تحقیق و تفتیش را پی‌گیری نمایید شاید نماینده مدعی‌العموم از شما بخواهد که یک استشهادنامه تهیه نمایید این استشهادنامه یا همان سوگند نامه، که بیشتر حاوی سوگند در خصوص حفظ و نگهداری از حقایق و شواهد یک جرم می‌باشد، به همراه درخواست صدور حکم تفتیش قبل از جمع آوری داده‌ها و شواهد، به قاضی ارجاع داده می‌شود. شکل ۶-۱ یک استشهادنامه را به صورت نمونه نشان می‌دهد.

نوشتن استشهادنامه که بایستی حاوی شواهد لازمه برای تفهیم اتهام می‌باشد از جمله وظایف شما در نوشتن آن گزارش می‌باشد. سپس بایستی یک استشهاد محضری با ادای سوگند تنظیم نمایید تا این اطمینان را بدهید که اطلاعات موجود در استشهادنامه صحیح می‌باشد. (در فصل۱۴ در مورد سوگند نامه محضری مطالب بیشتری ارائه خواهد شد)

پس از اینکه قاضی حکم تفتیش را تایید و امضاء نمود آماده اجرا می‌باشد به این معنی که شما می‌توانید بر اساس حکمی‌که به شما داده شده است به جمع آوری شواهد بپردازید. پس از جمع آوری شواهد، آنها را پردازش و تحلیل نموده تا به این اطمینان برسید که واقعا جرمی‌صورت گرفته و یا خیر؟ پس شواهد می‌توانند در جلسه دادگاه که برای محاکمه و یا استماع می‌باشد ارائه گردند. در اینجاست که قاضی یا نماینده رسمی‌هیات قضات و یا حتی هیات ژوری می‌توانند به صدور حکم بپردازند.



Date ___ ___ ___

Based on actual inspection of spreadsheets, financial records, and invoices, Joe Smith, a computer forensics expert, is aware that computer equipment was used to generate, store, and print documents used in Jonathon Douglas's tax evasion scheme. There is reason to believe that the computer system currently located on Jonathon Douglas's premises is the same system used to produce and store the spreadsheets, financial records, and invoices, and that both the [spreadsheets, financial records, invoices] and other records relating to Jonathon Douglas's criminal enterprise will be stored on Jonathon Douglas's computer.

Source: *Searching and Seizing Computers and Obtaining Electronic Evidence in Electronic Investigations*, U.S. Department of Justice, July 2002.

شکل ۶-۱ یک نمونه استشهادنامه

آشنایی با تحقیقات خصوصی یا شرکتی

تحقیقات خصوصی یعنی همان وکلا و شرکتهای خصوصی که اختلافات مدنی را که ناشی از تغییرات و تناقضات سیاسی و یا اختلافات دادخواهی می‌باشد مانند فسخ غیر قانونی قراردادها، بررسی می‌کنند. هنگامی‌که شما یک تحقیق رایانه ای را برای یک شرکت

خصوصی انجام می‌دهید به یاد داشته باشید که هر چند شما در حال انجام وظیفه می‌باشید اما زندگی و کسب و کار مردم نباید دچار وقفه ای گردد.

بازاریان معمولا تلاش می‌کنند تا اقامه دعوی و یا شکایات را به حداقل برسانند چرا که آن را روشی هزینه بر می‌دانند. جرایم مربوط به حوزه شرکت‌های خصوصی می‌توانند شامل مواردی مانند موارد زیر باشد: آزار واذیت از طریق پست الکترونیک، تحریف داده‌ها، تبعیض جنسی و سنی، اختلاس، خرابکاری و یا حتی جاسوسی صنعتی که خود به معنی فروختن اطلاعات حساس و محرمانه یک شرکت معتبر به شرکت رقیب می‌باشد. اینجاست که متوجه می‌شویم هر فردی که به رایانه دسترسی داشته باشد می‌تواند مرتکب این جرایم گردد. اختلاس از جمله جرایم معمول رایانه ای می‌باشد که عموما در بنگاههای کوچک رخ می‌دهد.

بطوریکه صاحب این بنگاه و یا مغازه عموما مشغولیت کاری بیشتری داشته و به یک نفر بیشتر اعتماد دارد مثلا مدیر داخلی، تا امور داخلی آن دفتر را مدیریت نماید. حال اگر این مدیر داخلی به هر دلیلی ناپدید گردد، اختلاس تازه خود را نشان می‌دهد و جمع آوری مدارک کافی برای متهم کردن مدیر هم کار سختی است و البته شاید صاحب شرکت از عهده آن بر نیاید. خرابکاری مشارکتی نیز اغلب توسط یک کارمند ناراضی انجام می‌گیرد. بطور نمونه این کارمند ناراضی که می‌خواهد در شرکت رقیب به دنبال کار بهتری بگردد کلیه اطلاعات شرکت را روی حافظه‌های جانبی نمونه برداری می‌کند که البته این نوع از جرایم می‌تواند منجر به جرم دیگری به نام جاسوسی صنعتی نیز گردد که البته هر سال تعداد آن نیز افزایش می‌یابد.

محققان بزودی خواهند توانست تحقیقات خود را از طریق سایت انجام داده بدون اینکه نیاز به آزمایشگاه خاصی داشته و یا اینکه بخواهد یک کارمند را در انجام وظایفش روی یک رایانه دچار وقفه کنند. فرض کنید یک مرکز مراقبت کارمندی داروگر در یک کلاهبرداری از شرکت بیمه نقش داشته است بطوریکه پول بیشتری از شرکت بیمه دریافت کرده است و پول را به حساب شخصی خودش واریز نموده است رایانه سرویس دهنده این مرکز مستندات مربوط به قبوض بیماران و اطلاعات مهم آنها را مانند داروهای

مصرفی، شرایط پزشکی، درمان‌های صورت گرفته و... نگهداری می‌کند که البته اگر این سیستم برای بیش از یک مدت کوتاه از حالت برخط بیرون باشد صدمات جبران‌ناپذیری برای بیماران به همراه دارد. به همین دلیل محققان نمی‌توانند مدارک را با خود ببرند بلکه مجبورند یک فایل نمونه و تصویر از آن را تهیه کرده و بعد از دقایق کوتاهی سیستم را به حالت برخط و به روز برای ادامه کار در اختیار بیماران قرار دهند.

ایجاد سیاستهای شرکتی

یکی از روش‌هایی که می‌تواند کمک کند به این که خطر ارتکاب جرایم کاهش یابد آن است که قوانینی طراحی و پیاده سازی شوند که کارمندان بتوانند به راحتی آنها را درک کرده و انجام دهند. که مهمترین این سیاستها آنهایی می‌باشند که قوانین را برای استفاده از منابع رایانه ای و شبکه شرکت توسط کارمندان آن، وضع می‌کنند. ایجاد سیاستهای یک شرکت یک حیطه قدرتی را ایجاد می‌کند که در مواجهه با بازجویی‌های داخلی مشکلی ایجاد نگردد.

این حیطه مشخص می‌کند در صورت بروز مشکل، چه کسی حق قانونی دارد که بازرسی را انجام دهد ویا اینکه چه کسی می‌تواند شواهد را جمع آوری کند و یا چه کسی حق دارد به شواهد و مستندات دسترسی داشته باشد.

سیاستهایی که به خوبی تعریف شوند به محققین این اجازه را می‌دهد که عملیات تحقیقاتی را به درستی انجام دهند.

نمایش یک پیام هشدار آمیز

یکی دیگر از روشهایی که یک سازمان دولتی یا حتی خصوصی را از به جریان انداختن یک دعوی قضایی منصرف می‌کند آن است که یک پیام هشدار آمیز روی صفحه نمایش رایانه نمایش داده بشود. این اتفاق معمولا زمانی رخ می‌دهد که رایانه بخواهد به یک شبکه داخلی یا یک شبکه خصوصی مجازی (VPN) متصل شده ودر اینجاست که به کاربران

نهایی این اخطارداده می‌شود که این سازمان کلیه حقوق نسبت به کنترل آن سامانه رایانه‌ای و شبکه را برای خود محفوظ می‌داند. اگر این حقوق به طور واضح بیان نگردد، شاید کاربران برای خود احساس امنیت کرده و خلوت خود را صرف دسترسی غیر مجاز به شبکه برنمایند. این پیام هشدار به فرد، حق انجام یک عملیات تحقیقاتی را نشان می‌دهد. که اگر این پیغام به درستی انتخاب گردد دیگر هیچ سازمانی نیاز به اقامه دعوی و مشکلات ناشی از آن ندارد. اگر یک سازمان، سیاستهای درستی را تبیین نماید کلیه حقوق جستجو و بررسی برایش محفوظ خواهد بود.

هر چند که قوانین کشورهای مختلف با یکدیگر متفاوت است. به طور نمونه، در برخی کشورها قانون بیان می‌کند که هر چند که یک شرکت در هر لحظه که اراده کند می‌تواند تحقیقات لازم را روی رایانه‌های خود شروع کند اما اگر فرد خاصی از کارمندان مضنون به ارتکاب جرمی باشند ابتدا بایستی به آنها در این خصوص اطلاع دهند.

عموما کاربران سامانه‌های رایانه ای، کارمندان و یا کاربران میهمان هستند بطوریکه حق دسترسی به اینترنت را دارا هستند اما کاربران میهمان تنها حق دسترسی به شبکه اصلی را دارند. معمولا شرکتها می‌توانند دو نوع پیام هشدار را مورد استفاده قرار دهند: یکی برای دسترسی کارمندان داخلی خود (دسترسی به صفحات وب در اینترنت) و دیگری برای کاربران میهمان که فقط به عنوان بیننده می‌باشند(دسترسی به صفحات وب اینترنتی). فهرست زیر سعی کرده است عبارات و اصطلاحات خاصی که می‌توانند در پیام‌های هشدار به کار روند را معرفی کند. قبل از استفاده از این هشدارها، ابتدا به دایره حقوقی سازمان مدنظر مراجعه نموده و مشورتهای لازمه را صورت دهید. بسته به نوع سازمان مربوطه، می‌توان از متون زیر در پیام‌های هشدار برای کارمندان داخلی استفاده نمود :

- دسترسی به این سیستم و شبکه محدود شده است.

- استفاده از این سیستم و شبکه تنها برای کارمندان رسمی‌امکان پذیر است.

- رئیس سازمان هر زمان که بخواهد می‌تواند شبکه و سیستم را رصد کند.

- استفاده از این سیستم، به معنای اعلام رضایت شما از رصد شدن توسط رئیس سازمان

می‌باشد.

- کاربران غیر مجاز و یا غیر قانونی که از این سیستم و یا شبکه استفاده کنند به مراجع قانونی جهت محاکمه معرفی خواهند شد.

شاید یک سازمان مثل یک دانشگاه این نظر را داشته باشد که شبکه‌ها و سیستم‌ها در هر لحظه ممکن، بایستی قابلیت نظارت را داشته باشند چرا که افراد دیگری از داخل هستند که می‌توانند از این امکانات استفاده کنند در حالیکه کارمند و یا دانشجو نیستند.از طرف دیگر، یک سازمان غیر انتفاعی، قطعا اطلاعات کاملی از شبکه خود داشته و از همه عبارات و اصطلاحات یاد شده نیز در منزل و پیام‌های هشدار خود استفاده خواهد کرد. حال اگر یک کاربر میهمان بخواهد دسترسی پیدا کند می‌توان از پیام‌های هشداری مانند موارد زیر استفاده نمود:

- این سیستم جزء اموال شرکت (الکس) می‌باشد.

- این سیستم، تنها مخصوص کاربران مجازمی‌باشد : دسترسی غیر مجاز خلاف قانون بوده و متجاوزین به مراجع قضایی معرفی خواهند شد.

- تمامی‌فعالیتها، نرم افزارها، ترافیک شبکه و ارتباطات داخل این شبکه در حال رصد می‌باشند.

به عنوان یک محقق رایانه ای شرکتی، از اینکه آن شرکت پیغام‌های هشدار مناسب و از قبل تعریف شده‌ای را داشته و نمایش می‌دهد اطمینان حاصل نمایید. چرا که بدون یک پیغام مناسب، شاید شما به راحتی نتوانید به وظایفتان عمل کنید چرا که کارمندان، بررسی‌ها و تحقیقات شما را به نوعی دخالت درامور شخصی خود خواهند دانست. و دادگاه نیز مدارک و مستندات را بررسی می‌کند و اگر پیغام‌های مناسب برای کاربران ارائه نگردد، دادگاه نیز رای به نفع آنها خواهد داد. البته قوانین ایالتی در خصوص انتظارات افراد از خلوت و تنهایی خودشان متفاوت بوده و از ایالتی به ایالت دیگر فرق می‌کند.

اما همه این ایالتها مفهوم حفظ حریم خصوصی را پذیرفته و رعایت می‌کنند. بعلاوه

اتحادیه اروپا و کشورهای عضو آن جریمه‌های سنگینی را برای افرادیکه بخواهند بدون رضایت دیگران اطلاعات شخصی آنها را از کشوری به کشور دیگر منتقل کنند در نظر می‌گیرد. بنابراین اگر شرکت خصوصی که شما در آن به عنوان کارآگاه و محقق رایانه ای کار می‌کنید بخواهد در کشورهای عضو اتحادیه اروپا کار پزشکی قانونی رایانه ای برای یک شرکت خاص را به عهده بگیرد، بطور نمونه، نمی‌تواند یک راه انداز شبکه را در رایانه آنها ایجاد کند بدون آنکه از آنها مجوز لازم را دریافت کرده باشد.

برخی ممکن است این استدلال را مطرح کنند که سیاستهای نوشته شده کل همان چیزهایی هستند که لازم می‌باشند. هر چند، در دادستانی داخلی یک پرونده خاص، پیغام‌های هشدار که برای کاربران در نظر گرفته شده اند جنبه حقوقی داشته و می‌توانند فرد مضنون را مجرم و یادر مواردی که این پیام‌ها نمایش داده نشدند حتی تبرئه نموده و حق را نیز به او بدهند.

تعیین درخواست کننده مجاز

همان گونه که بیان شد، تحقیقات بایستی اقتدار خود را حفظ کرده و جنبه قانونی داشته باشد. علاوه بر پیغام‌های هشدار که توضیح آن داده شد به مشاغل و شرکتهای تجاری این توصیه می‌گردد که یک درخواست کننده مجاز داشته باشند تا از طریق او امور مربوط به تحقیقات را انجام دهند. مدیریت اجرایی در یک سازمان بایستی اینگونه سیاستها را برای جلوگیری از تداخل منافع سازمانها، گروه‌هاو ادارات، انجام دهد. در سازمانهای بزرگ، رقابت بر سر حمایتهای مالی و مدیریتی می‌تواند تا حدی جدی گرفته نشود که گاهی مردم اتهامات کاذبی از سوء رفتارهای ایجاد شده را مطرح می‌کنند. چرا که یک شرکت رقیب نیز در همین زمینه مشغول به کار بوده است. برای جلوگیری از تحقیقات بی‌اهمیت و ناچیز، مدیریت اجرایی بایستی فرد یا افرادی را که مجری عملیات تحقیق و پزشکی قانونی کامپیوتری می‌باشند، رسمیت داده و معرفی نماید. عموما، هرچه تعداد افرادی که در گروه‌های تحقیق کار می‌کنند (محققین) کمتر باشد، بهتر است. نمونه‌هایی از گروههایی که می‌توانند(این اجازه را دارند) تا تحقیقات کامپیوتری را در یک شرکت

انجام دهند عبارتند از:

- **محققان امنیتی (حراستی) شرکت**
- **اداره نظم و انظباط اخلاقی شرکت**
- **اداره فرصتهای شغلی**
- **اداره ممیزی داخلی**
- **مشاوره عمومی‌یا بخش حقوقی**

دیگر گروها (ادارات) مانند گروه منابع انسانی، بایست درخواستهای خود را با گروههای مذکور هماهنگ کنند که این سیاست می‌تواند فرآیند تحقیقاتی را فرآیند نظم و انظباط کارکنان جدا کند.

انجام تحقیقات امنیتی(حراستی)

انجام تحقیقات کامپیوتری در بخش خصوصی به نسبت متفاوت از انجام آن در بخش عمومی‌و یا دولتی است.

زمانیکه شما در بخش عمومی‌تحقیقات خود را شروع می‌کنید بدنبال شواهدی مرتبط با اتهامات مالی هستید در حالیکه در تحقیقات خصوصی بدنبال شواهدی دال بر اتهامات مربوط به سوء استفاده‌های مالی از دارایی‌های شرکت و یا حتی در مواردی شکایت‌های کیفری هستید. در محیط‌های شرکتی عموما سه نوع از شرایط مطرح می‌باشد.

۱- سوء استفاده از دارایی‌های محاسباتی

۲- سوء استفاده از پست الکترونیک

۳- سوء استفاده از اینترنت

اغلب تحقیقات کامپیوتری در بخش خصوصی مرتبط با سوء استفاده‌های مالی می‌باشد. عموما از این سوء استفاده باعنوان **"نقض قوانین شرکت توسط کارمندان"** یاد می‌شود. معمولا شکایت‌های مطرح شده مربوط به سوء استفاده‌های کارمندان ازاینترنت و نامه‌های الکترونیک می‌باشد که در مواردی با سوءاستفاده ازمنابع کامپیوتری مانند سوءاستفاده

از نرم افزار یک شرکت برای تولید نرم افزاری مشابه برای شرکت دیگرهمراه می‌باشد. تحقیقات در زمینه پست الکترونیک می‌تواند از استفاده غیرمجازازپست الکترونیک شرکت برای اهداف شخصی گرفته تا ایجاد تهدید ورغب ووحشت به کمک پست الکترونیک باشد. یکی از جرایمی‌که با پست الکترونیک انجام می‌گیرد ارسال پیام‌های توهین آمیز و تهاجمی‌می‌باشد. این نوع پیام‌هامی‌تواند منجر به یک محیط کاری خصمانه گردد که البته می‌تواند خود منجر به آن گردد که شرکت و کارمندان آن نیز بر علیه یکدیگر وارد طرح دعوی گردند. از طرف دیگر، کارآگاهان کامپیوتری با سوءاستفاده‌های اینترنتی نیز درگیر هستند. سوء استفاده کارمندان از اینترنت نیز می‌تواند از وب‌گردی‌های روزانه در محل کار باشد تا دیدن عکسهای غیراخلاقی در محیط کاری. یک نمونه بسیار بد از این تصاویر غیراخلاقی رامی‌توان تصاویر غیراخلاقی گرفته شده از کودکان دانست. دیدن این گونه تصاویر در قوانین حقوقی اکثر کشورها مصداق عمل مجرمانه می‌باشد و اینجاست که محققان کامپیوتری بایستی با استفاده ازحداکثر تجربه حرفه ای بودن خود، این پرونده‌ها را مدیریت کنند. با اجرای مداوم این گونه سیاستها، می‌توان از دردسرهای ایجاد شده جلوگیری نمود.

نقش یک پزشک قانونی کامپیوتر آن است که به مدیریت، اطلاعات کامل و دقیقی ارائه کند تا آنها بتوانند مشکلات بوجود آمده را بررسی و تصحیح کنند (چگونگی انجام این کار در فصل‌های آینده بطور کامل ارائه می‌گردد). شما بایستی از تفاوت قائل شدن بین مشکلات ناشی از سوء استفاده‌های انجام شده از یک شرکت و نیز تناقضات جنایی بالقوه، مطمئن گردید. مشکلات ناشی ازسوء استفاده‌ها هرچند که سیاست‌های یک شرکت را می‌تواند مورد تهاجم قرار دهد اما اگردر خانه انجام گیرد دیگر شکل غیرقانونی به خود نمی‌گیرد. جرایم جنایی شامل اعمالی مانند جاسوسی صنعتی، اختلاس، قتل و ... می‌باشد در حالیکه اقداماتی که به نظر می‌رسند مربوط به سوءاستفاده‌های داخلی می‌باشند نیز می‌توانند مسئولیت کیفری و یا حتی مدنی داشته باشند از آنجاییکه هر تحقیق مدنی می‌تواند یک تحقیق جنایی نیز باشد شما بایستی هرپرونده ای راکه دردست اقدام دارید با بالاترین سطح امنیت و مسئولیت پذیری انجام دهید. بطور مشابه تحقیقات شرکتی و

خصوصی که شما انجام می‌دهید می‌تواند درشرایطی درگیر مسائل مدنی و غیرجنایی به نظر برسد.

اما همان طور که به تحقیقات و تحلیل‌های خود ادامه می‌دهید متوجه یک موضوع جنایی نیز می‌شوید پس با این احتمال به یادداشته باشید که کار شما می‌تواند زیر نظر قوانین مدنی و جنایی بررسی ونظارت گردد.

تشخیص دادن اموال شخصی از اموال شرکتی در بسیاری از شرکتها سیاست تنظیم شده آن است که بین اموال شرکت و کارمندان حد و مرزی مشخص گردد هرچند که در مواردی کار بسیار سختی است. مثلا در مورد دستگاه‌هایی مانند PDAها، گوشی‌های تلفن همراه، کامپیوترهای شخصی و... این تشخیص، کار سختی به نظر می‌رسد. به طور نمونه، یکی از کارمندان یک PDA برای خود خرید نموده و آن را به کامپیوتر شرکت متصل می‌کند و به محض اینکه مثلا از نرم افزار OUTLOOK برای یررسی نامه‌های الکترونیک خود استفاده کند قسمتی ازاطلاعات شخصی اودرکامپیوتر شرکت نسخه برداری می‌شود. در این حین، اطلاعات شرکت نیز می‌تواند روی دستگاه PDA نیز نسخه برداری گردد. در این حالت، حداقل سئوال که پیش می‌آید این است که: " اطلاعاتی را که روی PDA موجود می‌باشد متعلق به کارمند است یا به شرکت؟"

حال فرض می‌کنیم که شرکت یک PDA به کارمند به عنوان هدیه می‌دهد. آیا به نظرشما دراینجا شرکت نسبت به PDA حقی دارد یاخیر؟

به طور مشابه این اتفاق می‌تواند برای رایانه‌های جیبی و کیفی نیز رخ دهد. در این طور مواقع چه باید کرد؟

با توجه به اینکه کامپیوترها روز به روزدرزندگی انسانها بیشتر ورود پیدا می‌کنند، شما با این گونه موضوعات بیشتر برخورد خواهید نمود. و از آنجا که این گونه سئوالات نیز هر روز بیشتر و بیشتر می‌شود مدیران شرکتها نیز بایستی درسیاستهای خود دقت بیشتری نمایند. سیاست امن آن است که به هیچ کارمندی اجازه داده نشود دستگاه‌های شخصی خودش را به شبکه و یا کامپیوتر شرکت متصل نماید.

حفظ رفتار حرفه ای

به عنوان یک محقق کامپیوتری و تحلیلگر پزشکی قانونی رفتارحرفه ای شما مهم می‌باشد چرا که اعتبار شما را تعیین می‌کند. به عنوان یک حرفه ای، شما بایستی همیشه بالاترین سطح رفتار اخلاقی را ازخود نشان دهید. برای انجام این کار بایستی در طول عملیات تحقیق و بررسی، بی طرفی و محرمانگی را رعایت نموده، به طور پیوسته دانش فنی خود را بهبود بخشیده و خود را به کمال برسانید. شما در دعاوی امروزه، مشاهده می‌کنید که دادستان باچه دقتی به شواهد و مدارک نظر دارد و به عنوان یک شاهد، شما بایستی از سابقه صداقت بالایی برخوردار باشید. حفظ بی طرفی به این معناست که شما در تحلیل‌هایی که انجام می‌دهید بایستی از ایراد نظرات بی پایه واساس اجتناب نمایید. همچنین از هرگونه اظهار نظر و نتیجه‌گیری قبل از تکمیل شواهد و بررسی‌های خود بپرهیزید.

حداکثر وظیفه شما جمع‌آوری شواهد کامپیوتری برای دادگاه می‌باشد. و در این مسیر نباید به فشارهای خارجی توجه داشته باشید. مثلا اگر دادستان شما را به کار گرفته است نباید افکار و عقاید و یا فشارهای او در تحلیل‌های شما اثرگذارباشد. شهرت و اعتبار شما بسته به بی طرفی شما در تمامی پرونده‌ها دارد. از طرف دیگر شما بایستی اصل محرمانگی اطلاعات شخصی دیگران را نیزدر تحقیقات خود حفظ کنید. و از بازگویی مطالب پرونده به افراد نیز مرتبط با جریان تحقیقات بپرهیزید.

اگر نیازبه دستگاهی دارید که در اختیاریک نفردیگرحرفه ای مانند خودشان است بدون ذکر جزئیات، فقط کلیات پرونده را برای دریافت آن دستگاه خاص به او بگویید.

تمامی‌تحقیقات شما بایستی محرمانه باشد تا زمانیکه به دادگاه به عنوان شاهد دعوت می‌شوید ویا اینکه دادگاه ویا دادستان مدارک ویا گزارش درمورد پرونده ازشما می‌خواهند.

در یک محیط شرکتی وقتی در مورد پرونده یک کارمند تحقیق می‌کنید، محرمانگی داده‌ها واطلاعات نقش بسیارمهمی را دارد. توافق بین کارمند وشرکت برای رسیدن به اینکه یا کارمند اخراج شده ویا اینکه استعفا داده واز شرکت برود درجهت جلوگیری از بازتابهای منفی آن بسیاراهمیت دارد.

اگر شما نام کارمند وجزئیات پرونده وی رابه دیگران بگویید، فسخ قرارداد وی با شرکت می‌تواند تبعات بدی را با خودهمراه داشته باشد. دربرخی موارد، پرونده می‌تواند یک پرونده جدی مانند قتل باشد که مراحل دادگاهی شدن آن نیزبسیار طولانی گردد. حال اگرکارآگاه با دیگر درخصوص شواهد دیجیتال مطالبی رابازگو کند، این پرونده شاید به خاطر تبلیغاتی که به نفع آن قبل ازشروع دادگاه می‌شود، مسیرطبیعی خود را طی ننماید. زمانیکه شما به دستوروکیل روی یک پرونده درحال تحقیق هستید، دو قانون زیررا درنظر داشته باشید: اول قانون وکیل- کار- نتیجه و دوم قانون وکیل- امتیاز مشتری.

این بدین معنی است که شما در مورد پرونده فقط با وکیل ویا تیم همکارخود صحبت کنید و هرگونه ارتباطی با دیگران درخصوص پرونده باید با اجازه وکیل صورت پذیرد.

علاوه برحفظ اصل بی‌طرفی و محرمانگی درتحقیقات خود شما بایستی رفتارحرفه‌ای خود را به تکامل یادگیری خود بهبود بخشید. زمینه کاری تحقیقات پزشکی قانونی کامپیوتری بطور مداوم درحال تغییر و تکامل است به همین دلیل شما نیز بایستی نسبت به تغییرات ایجاد شده در زمینه‌های مختلف کامپیوتری مانند سخت افزار، نرم افزار، شبکه و البته پزشکی قانونی کامپیوتری دانش خود را به روز نمایید.

یکی از بهترین روش‌های ارتقاء دانش وعلم شما می‌تواند چاپ مطالعات و روش‌هایی که شما دردرک حقیقت از آنها استفاده کرده اید درژورنالها ومجلات معتبرباشد. ژورنال و مجله به شما دریادگیری و به یادسپاری چگونگی انجام روالها و فرآیندهای کاری و نیز نحوه استفاده ازابزارهای نرم افزاری و سخت افزاری کمک خواهد کرد. که البته بایستی با ذکرتاریخ وجزئیات مهم، همراه باشد. پس ازثبت آنها دریک مجله، حتما روالی را برای مروراین مقاله‌ها جهت حفظ دستاوردهای قبلی برای خودتان تعریف نمایید.

اگر بخواهید یادگیری‌های حرفه‌ای خودتان را مداوم بهبود بخشید بایستی حتما در کارآگاه‌ها و همایش‌ها شرکت کنید و البته آموزش رسمی‌خود را نیز ادامه دهید. اگر شما حداقل مدارک کامپیوتری و رشته‌های مرتبط با آن را دارید بایستی حتما دانش حرفه ای خود را بهبود بخشید. اگر مدارک بالاتر و پیشرفته ای ندارید، دریک حوزه مطالعاتی خاص سعی کنید حرفه ای شوید مثلا در حوزه تجارت الکترونیک ویا قوانین بازاریابی.

امروزه بسیاری از دانشکده‌ها و دانشگاه‌ها برنامه‌های متنوعی را در سطوح مختلف فوق دیپلم، کارشناسی و یا حتی کارشناسی ارشد در حوزه‌های مرتبط با پزشکی قانونی کامپیوتری (البته در کشور آمریکا) ارائه می‌دهند. بسیاری از شرکتهای معتبر و عظیم هستند که تمایل به پرداخت هزینه‌های تحصیلی شما دارند هرچند که عموما آنها از شما تعهدی را در خصوص ادامه همکاری با ایشان قطعا درخواست خواهند داشت. علاوه برآموزش و یادگیری، عضویت در سازمانها و نهادهای حرفه ای به اعتبار شما می‌افزاید. بطوریکه این نهادها اغلب آموزش شما را انجام داده و بهترین محل برای تبادل اطلاعاتی درخصوص پیشرفتهای فنی درحوزه کامپیوتروپزشکی قانونی آن می‌باشند.

همچنین با مطالعه جدیدترین کتابها ومطالعه هرچه بیشترمقالات درخصوص تحقیقات و پزشکی قانونی کامپیوتری، خود را به روزنگه دارید. شما به عنوان یک محقق حرفه ای در زمینه مدارک پزشکی کامپیوتری، بایستی صداقت ودرستکاری را دردستور کارخود قرار دهید ودرتمامی‌زمینه‌ها وجنبه‌های زندگی خود درستکاری را سرلوحه کارتان قراردهید چرا که هرگونه اقدام نسنجیده ای می‌تواند منجربه تاسف وشرمساری شما گشته وبه وکیل رقیب شما این فرصت را می‌دهد تا دردادگاه‌ها اعتبارشما خدشه دارنماید.

خلاصه فصل:

- پزشکی قانونی رایانه ای روالهای پزشکی قانونی را به ادله دیجیتال اعمال می‌کند. این فرآیند شامل جمع آوری و تحلیل هدفمند اطلاعاتی است که می‌تواند در پرونده‌های مدیریتی، کیفری ویا مدنی استفاده شوند. از نظرحوزه نفوذ، تکنیک وهدف، پزشکی قانونی رایانه ای با پزشکی قانونی شبکه ای، بازیابی داده‌ها و بازیابی فجایع فرق می‌کند.
- قوانین مرتبط با ادله دیجیتال دردهه ۱۹۷۰ به تصویب رسیده اند.
- اگر می‌خواهید درحوزه پزشکی قانونی رایانه ای، متخصص حرفه ای گردید، بایستی با بیش ازیک نوع سیستم عامل وسخت افزار رایانه ای آشنا باشید. و برای اینکه بتوانید روز به روز به دانش خود بیفزایید بایستی با افراد حرفه ای و متخصص

درزمینه‌های تحقیقاتی، شبکه ای و رایانه ای ارتباطات جدید ایجاد کرده و آن را گسترش دهید.

- تحقیقات رایانه ای دربخش خصوصی با بخش دولتی یا عمومی‌فرق می‌کند. درتحقیقات عمومی(دولتی)
- بایستی قبل ازضبط و جمع آوری ادله دیجیتال حکم تجسس صادر گردد. متمم چهارم قانون اساسی ایالات متحده ونیزقانون‌های اساسی دربسیاری ازکشورهای دیگر، به تجسس وضبط دولتی اعمال می‌گردند. حین انجام تحقیقات دولتی به دنبال ادله ای می‌گردید که ارتکاب جرمی‌را اثبات کند. اما حین انجام تحقیقات خصوصی، به دنبال ادله ای می‌گردید که سوء استفاده‌های مالی ازاموال را، ویاحتی دعاوی کیفری را اثبات کند. بایستی ازپیام‌های هشدار دهنده استفاده گردد تا کارمندان به یاد آورند که شرکت دارای سیاستهای خاصی درخصوص استفاده ازاینترنت، رایانه، پست الکترونیک و... می‌باشد.
- شرکتها بایستی تعداد افراد مجازی را که می‌توانند تحقیقات را شروع کنند محدود نماید.
- ماموران تحقیقاتی پزشکی قانونی رایانه ای بایستی جهت حفظ اعتبارخود رفتارهای حرفه ای از خود نشان دهند.

فصل دوم:

آشنایی با تحقیقات کامپیوتری

پس از مطالعه و تکمیل تمرینهای این فصل، قادر خواهید بود:

- توضیح دهید چگونه می توان یک تحقیق کامپیوتری را آماده نمود
- یک رهیافت سیستماتیک برای انجام یک کارتحقیقاتی را ارائه دهید
- روالهای لازم برای تحقیقات مشارکتی با فناوری بالا را توصیف نمایید
- نیازمندیهای موجود برای نرم افزارها وایستگاه های کاری مخصوص ترمیم وبازیابی داده ها را توصیف نمایید
- چگونگی انجام یک تحقیق را توصیف نمایید
- چگونگی تکمیل ونقد یک پرونده را توصیف نمایید

این فصل یک دید کامل ازچگونگی مدیریت یک تحقیق کامپیوتری ارائه می‌دهد. شما در خصوص مشکلات و چالش‌هایی که پزشکان قانونی کامپیوتر با آنها مواجه هستند اطلاعاتی را کسب می‌کنید.

مثلا اینکه چه ایده‌ها و یا سوالاتی باید از ذهن آنها عبور کند تا بتوانند یک تحقیق را تکمیل کنند. این فصل به توضیح نرم افزار ProDiscover Basic که یکی از ابزارهای سودمند در زمینه پزشکی قانونی کامپیوتری می‌باشد می‌پردازد. در این فصل، شما همچنین جزئیات بیشتری نسبت به چگونگی انجام تحقیقات توسط دیگر ابزارهای پزشکی قانونی کامپیوتری فراخواهید گرفت و در انتها تکنیکهای حل مساله استاندارد را نیز کشف خواهید نمود. شما به عنوان یک کاربر کامپیوتر، می‌توانید با کارکردن با رابط گرافیکی کاربر(GUI) یک نرم افزار، به راحتی با آن ارتباط برقرار نمایید اما یک شخص حرفه ای درزمینه پزشکی قانونی کامپیوتری علاوه براینکه باید به راحتی بتواند ازطریق GUI با نرم‌افزار مخصوص این کارارتباط برقرارکند بایستی بتواند با سطوح اصلی سیستم عامل که بسیارمهم‌تر از GUI نیزهستند تعامل داشته باشد.

بسیاری از ابزارهای نرم افزاری دراین خصوص، ازطریق خط فرمان عمل می‌کنند و شما بایستی درمواقعی که تنها انتخابتان خط فرمان است از این نرم افزارها استفاده کنید. در ضمیمه D نمونه‌هایی ازچگونگی استفاده ازاین ابزارها ارائه شده است. دراین فصل برای انجام تمرین‌ها و فعالیتهای خواسته شده، ابتدا نحوه تهیه تصویر(Image) از یک درایو USB کوچک جهت انجام تحقیقات پزشکی قانونی، را فراخواهید گرفت. بعد از اینکه آموختید چگونه می‌توان داده‌های روی یک افزار ذخیره سازی کوچک را جستجو و یا پیدا

نمود، می‌توانید با تکنیکی مشابه به این کاررا روی یک دیسک بزرگترنیزاعمال کنید.

آماده سازی یک تحقیق کامپیوتری

به عنوان یک متخصص حرفه ای درزمینه پزشکی قانونی کامپیوتری، نقش شما اینست که نسبت به جمع آوری شواهد و مستندات از کامپیوتر فرد مضنون اقدام نموده و تعیین کنید که این فرد مضنون آیا مرتکب جرمی شده ویا اینکه قوانین و سیاستهای یک شرکت رانقض کرده است یاخیر؟ که اگرشواهد این‌ها را نشان دهد، شما بایستی پرونده‌ای را آماده نمایید. دراین پرونده مستنداتی جهت ارائه به دادگاه و یا مراجع ذی صلاح آمده است. این فرایند شامل انجام تحقیقات لازم روی کامپیوتر فرد مضنون می‌باشد هرچند که جهت تکمیل پرونده بایستی مسیرورروال ازقبل تعریف شده ای را طی کنید. با انجام روشمند هرپرونده، شما می‌توانید مدارک هرپرونده را بطور مناسب و کامل ارزیابی کنید وزنجیره مدارک را مستندسازی نمایید(زنجیره بازداشتی). این زنجیره یعنی همان مسیری که مدارک اززمانی که شما کارتحقیقات را آغازکرده تا زمانیکه پرونده مختومه اعلام می‌شود ویا به دادگاه ارسال میشود، طی می‌کنند.

قسمت بعدی دوپرونده رابصورت نمونه ارائه می‌دهد. یکی درمورد جرایم کامپیوتری است ودیگری درخصوص نقض قوانین وسیاستهای یک شرکت هرکدام ازاین نمونه‌ها توصیفی ازمراحل اصلی تحقیقات پزشکی قانونی، شامل جمع آوری مستندات وشواهد، آماده سازی یک پرونده وبررسی مدارک رادربردارد.

ماموران اجرای قانون، همان طورکه درحال تحقیق روی یک پرونده جنایی هستند و یا مستنداتی راتهیه وجمع آوری می‌کنند ویا حتی درحین بازداشت افراد مضنون، کامپیوترهاویا قطعات کامپیوتری را نیزپیدامی‌کنند. این کامپیوترها عموماحاوی اطلاعاتی هستند که به این ماموران اجرای قانون کمک می‌کنند زنجیره حوادثی را که منجربه انجام یک جرم شده اند تکمیل کنند ویا مدارک اطلاعاتی خاصی را پیدا کنند که به محکومیت یک فرد مضنون بیشترکمک کند.

به عنوان یک نمونه ازپرونده ای که درآن ازکامپیوترها درارتکاب جرم استفاده شده بود،

می‌توان گفت که پلیس یک دلال مواد مخدررا شناسایی وبه منزل وی هجوم می‌بردودر آن یک کامپیوتر چندین دیسکت و درایورهای USB، یک PDA و یک تلفن همراه پیدا می‌کند.(شکل ۱-۲). پس اینها بسته بندی و برچسب گذاری گردید یعنی اینکه درکیف مخصوص مدارک قرارداده شده ویا برچسب‌های مخصوصی که صرفابرای تحقیق وتفحص می‌باشد، نشانه گذاری می‌گردند.

شکل ۱-۲. یک صحنه جرم

کارآگاه پرونده ازشما می‌خواهد که کامپیوتررابررسی نموده تا داده‌هایی که احتمالا می‌توانند به عنوان مدرک جرم استفاده شوند راجمع آوری وسازمان دهی نمایید. مانند فایلهایی که حاوی اسامی‌دلالان مواد مخدرهستند افسرتجسس به شما مستنداتی ازاقلامی‌را می‌دهد که اداره تحقیقات و تجسس آنها را جمع آوری نموده است که حاوی فهرستی از رسانه‌های ذخیره سازی است که جمع آوری شده اند. افسرتجسس همچنین تاکید ویادآوری می‌کندکه سیستم عامل ویندوز XP روی این کامپیوترنصب بوده است و هنگام کشف نیزماشین روشن ودرحال کاربوده است. او قبل ازخاموش کردن کامپیوتر از صفحاتی که درحال اجرا شدن بوده اند تصاویری را تهیه کرده است و آنها را به شما می‌دهد.

حال شما به عنوان یک محقق پزشکی قانونی کامپیوتری، ازاینکه کارآگاه روال درستی

را در جمع آوری مدارک طی نموده است بسیار خوشحال و سپاسگزار هستید. حال با داشتن این اسناد و مدارک دیجیتال، بسیارمهم است که شما تشخیص دهید داده‌های اصلی مانند آخرین زمان دسترسی به فایل چطورمی‌تواند توسط اولین ماموری که بر صحنه جرم حاضرشده است تغییر کرده باشد.

شما در ارزیابی‌های اولیه خودتان، فرض می‌کنید که فایلهای موجود در رسانه‌ها ذخیره‌سازی مانند پیام‌های نامه‌های الکترونیک، فایلهای پاک شده و یا فایلهای مخفی دست نخورده هستند. در اینجاست که شما می‌توانید از نرم افزارهای گوناگونی که در این زمینه کار می‌کنند استفاده کنید که البته اداره شما از نرم افزار ProDiscover Basic استفاده می‌کنند.

همچنین درپایان ارزیابی‌های اولیه، چالش‌های بالقوه ای که دراین پرونده می‌توانند باشند را مشخص می‌کنید.

از آنجا که قاچاقچیان مواد مخدراطلاعات مربوط به همدستان خود رادر اختیارنمی‌گذارند، احتمالا فایلهایی که شما آنها را پیدا کرده اید بصورت کلمه عبورکدگذاری شده وحفاظت شده اند. پس یا به یک متخصص احتیاج داریدکه فایل را رمزگشایی نماید ویا برای این کار به نرم افزارقوی که کلمه عبوررا پیدا وکشف می‌کند نیازمند خواهید بود.

مرور اجمالی بر نقض سیاست‌های یک شرکت

معمولا شرکتهای خصوصی و یا حتی دولتی سیاستهایی را در خصوص استفاده کارمندان از کامپیوترهای شان در نظر می‌گیرند. کارمندانی که معمولا وب گردی نموده و یا نامه‌های الکترونیک شخصی ارسال می‌کنند و یا برای انجام امور شخصی شان ازکامپیوترهای شرکت استفاده می‌کنند، وقت شرکت را هدر می‌دهند و از آنجا که این وقت، هزینه‌بر می‌باشد محققان زمینه پزشکی قانونی اغلب در این حوزه‌ها نیز وارد می‌شوند. در ادامه یک نمونه از سیاست‌های شرکتی را جهت جلوگیری از هدر رفت وقت ارائه می‌کنیم:

آقای استیو بیلینگ که مدیریک شرکت است چندوقتی است که شکایت‌هایی را ازطرف

مشتریان خود نسبت به عملکرد شغلی یکی ازعوامل فروش شرکت خود به نام آقای جورج مونت گومری، دریافت می‌کند. اوچندین سال است که به عنوان بازاریاب وعامل فروش کارمی‌کند. او دو روزاست که بدلیل بیماری بدون اینکه باکسی هماهنگ کند به محل کارش نیامده است. کارمندان دیگری به نام مارتا، نیز چندروزی است که بدون اطلاع قبلی سرکارخود حاضر نشده است. استیو به عنوان مدیر شرکت ازاداره فناوری اطلاعات خواسته است تا هاردیسک ودیگر رسانه‌های ذخیره سازی آقای جورج راضبط کند. او با این کارمی‌خواهد بررسی کند که آیا اطلاعاتی روی این کامپیوتر می‌باشد که نشان دهد مشکل جورج چیست؟ برای این کارشما بایستی یک روش نظام مند وباقاعده راطی نمایید. که درقسمت ذیر به توضیح آن می‌پردازیم تا داده‌های جمع آوری شده از میزجورج را نیز بررسی وتحلیل کنیم.

اتخاذ یک رویکرد صحیح

در این قسمت مراحلی را که برای انجام یک تحلیل استاندارد و لازم می‌باشد تا یک محقق کامپیوتری انجام داده و تشکیل پرونده دهد بیان می‌شود:

- **ارزیابی اولیه ای در مورد نوع پرونده در حال بررسی خود انجام دهید**

برای ارزیابی نوع پرونده کاری خود، با دیگران که همکار شما در پرونده هستند صحبت کرده و اطلاعات تکمیلی را در مورد حادثه کسب کنید. آیا قبل از شما ماموران اجرای قانون به سیستم‌های کامپیوتری دسترسی داشته و بررسی انجام داده اند؟ آیا نیاز داریدکه از صحنه وقوع جرم بازدید داشته باشید؟ آیا از کامپیوتر برای ارتکاب جرم استفاده شده است یا اینکه کامپیوتر حاوی اسناد و مدارکی است که برای بررسی یک جرم دیگر مفید هستند؟

- **یک طرح یا رهیافت اصلی برای پروند تعریف کنید**

مراحل اصلی که در تشکیل پرونده لازم هست را برای خود بازبینی و مشخص کنید.

اگر مضنون، کارمند بوده و شما می‌خواهید کامپیوترش را بررسی کنید، مشخص شود که شما در طول ساعات کاری می‌خواهید آن کامپیوتر را بررسی کنید و یا اینکه درساعات تعطیل بعد از ظهر یا آخر هفته. اگر یک پرونده جنایی را بررسی می‌کنید، بررسی کنید که ماموران اجرای قانون چه اطلاعاتی را تابحال جمع آوری نموده اند.

- **تهیه یک فهرست بررسی دقیق**

یک فهرست بررسی از مراحل و زمان تضمینی هرمرحله تهیه کنید.

- **منابعی که لازم دارید را مشخص کنید**

بسته به سیستم عامل کامپیوتری که شما روی آن کارمی کنید، فهرست نرم افزارهای لازم برای کارتان تهیه کنید.

- **اخذ و نسخه برداری از یک درایو مدارک وشواهد**

در برخی از پرونده‌ها، شاید لازم باشد چندین کامپیوتر را با داشتن دیسک‌هایZIP، CD و درایوهای USB، PDA و ... بررسی کنید.

تعیین ریسکها

مشکلاتی راکه معمولا درمواجهه با نوع پرونده ای که کارمی‌کنید انتظارشان رادارید فهرست کنید. این فهرست به عنوان یک ارزیابی دیسک استاندارد شناخته شده است. مثلا اگر به نظرمی‌رسد که فرد مضنون درزمینه کامپیوتراطلاعات خوبی دارد احتمال داردکه طوری برنامه ریزی کرده باشد که اگرکسی سعی کند واردکاوش با به حداقل رساندن خطرات کامپیوترشود تمام داده‌ها را ازبین ببرد ویا سیستم راخاموش کند.

تعیین کنید که چطور می‌توانید دیسکها را به حداقل رساند. بطور مثال، اگر شما روی

کامپیوترفرد مضنون کار می‌کنید که‌هارد آن را با کلمه عبور قفل کرده اند، می‌توانید قبل از شروع به کار، از رسانه اصلی ذخیره سازی نسخه برداری کنید که اگر درطول مراحل بازیابی اطلاعات نسخه ای خراب شود نسخه اصلی آن موجود می‌باشد.

آزمودن طراحی

تصمیماتی راگرفته اید و مراحلی را که کامل کرده اید را مرورکنید. اگر رسانه ذخیره سازی اولیه را نسخه برداری کرده اید یک قسمت ازآزمودن طرح این است که مقادیر درهم‌سازی شده را مقایسه کنید(در فصل‌های ۴/۵ بررسی شده اند) تا مطمئن گردید که داده‌های درست را نسخه برداری کرده اید.

تحلیل و ترمیم شواهد دیجیتال

با استفاده ازابزارهای نرم افزاری ودیگر منابعی که جمع آوری کرده اید وبا اطمینان ازاینکه تمامی‌خطرات وموانع را درنظرگرفته اید دیسک را برای پیدا کردن شواهد و مستندات دیجیتال بررسی کنید.

داده‌هایی را که ترمیم نموده اید بررسی و تحقیق کنید

اطلاعاتی راکه ازدیسکها ترمیم کرده اید شامل، فایلهای موجود، پاک شده نامه‌های الکترونیک و ... مشاهده کنید و فایلها را طوری سازمان دهی کنید تا در اثبات گناهکاری یا بی گناهی فرد مضنون کمک باشند.

گزارش پرونده را تکمیل کنید

درمورد آنچه داده اید وآنچه پیدا کرده اید گزارش کاملی را با ذکر جزئیات نوشته و ارائه دهید.

پرونده را نقد کنید

در رشته حرفه ای افراد، یکی ازمهمترین موضوعات خود ارزیابی می‌باشد. پس از اینکه پرونده ای را تکمیل کردید، آن را مرورکنید تا تصمیمات موفق و عملکردهای خوب خود را مشخص کنید وتعیین کنید که چگونه می‌توانستید عملکرد و کارآیی خود را بهبود بخشید. بسته به ذات و نوع تحقیقات صورت گرفته، میزان وقت و تلاشی که شما در هر مرحله صرف می‌کنید متفاوت خواهد بود. بطور نمونه، در اکثر پرونده‌ها از آنجا که شما یک طرح تحقیقاتی ساده ارائه می‌کنید دیگر مرحله‌های خاصی به نظر نمی‌رسند. اما اگر در یک پرونده از کامپیوترهای مختلف با موضوعات گوناگون قرار است شما تحقیق کنید یک طرح با جزئیات دقیق، با مرور دوره ای و بروزرسانی‌های منظم لازم و ضروری است یک رهیافت سیستماتیک اطلاعات لازم برای پرونده را به راحتی کشف می‌کند و هر چقدراطلاعات لازم دارید را به شما می‌دهد. در همه تحقیقات کامپیوتری، شما برای حوادثی که انتظارشان را ندارید باید آماده باشید، یعنی طرح‌های احتمالی را برای خود تعریف کنید. یک طرح احتمالی می‌تواند ازهرچیزی تشکیل شود تا در تکمیل تحقیقات شما را کمک کند از ابزارهای نرم افزاری و سخت افزاری جایگزین گرفته تا دیگر روشها و رهیافت‌های تحقیقی.

ارزیابی پرونده

همانطورکه بیان شد، تعیین نیازمندیهای یک پرونده بسته به تعیین نوع پرونده دارد که انتها همگی بسته به مواردی مانند ذات پرونده، نوع مدرک در دسترس و حتی محل مدارک دارد. در پرونده اخیر که نقض سیاستهای یک شرکت موضوع اصلی پرونده بود، از شما خواسته شده بود که در مورد جورج مونت گومری تحقیق کنید. آقای استیو که مدیر این شرکت بود از اداره فناوری اطلاعات خواسته بود تا جهت مشخص شدن نحوه عملکرد آقای جورج، سیستم کامپیوتری وی را ضبط کرده و مورد بررسی قرار دهند. پس از صحبت با همکاران جورج، استیو متوجه شد که جورج در کنار کار اصلی خودش، با استفاده از کامپیوتر و دیگر اموال شرکت، یک کسب و کار دیگر را نیز شروع کرده است.

بنابراین تمرکز مساله، از موضوع غیبت کارمند تبدیل شد به سوء استفاده شخصی کارمند از امکانات شرکت جهت انجام کسب و کار خودش.

شما می‌توانید به صورت زیر، این پرونده را ارزیابی نمایید:

- شرایط – پرونده سوء استفاده کارمند
- طبیعت پرونده- شغل جانبی با استفاده ازکامپیوترشرکت توسط کارمند
- مشخصات پرونده- گزارشها نشان می‌دادکه کارمند با سوء استفاده از امکانات شرکت، یک شغل جانبی را شروع کرده بود. او با در دست گرفتن ISP محلی شرکت، خدمات مثبت دامنه و تنظیمات مربوط به وب سایتهای آنها را انجام می‌داده است. همکارنش نیز شکایت خود را اعلان کرده و گفته بودند که او نه تنها وقت زیادی را روی این کار شخصی اش می‌گذاشته بلکه وظایف و مسئولیتهای محوله از قسمت شرکت را نیز انجام نمی‌داده است. طبق سیاست شرکت، مدیر شرکت می‌تواند در هر لحظه که ارادهنماید نسبت به بررسی و تحقیق از کامپیوترهای شرکت که در اختیار کارمندان می‌باشد اقدام کند. بطوریکه کارمندان هنگام کار با کامپیوترهای شرکت، اساس محرمانگی ندارند.
- نوع مدارک و شواهد - یک درایو USB با گنجایش کم
- سیستم عامل - مایکروسافت ویندوز XP
- قابلیت دیسک – FAT16
- محل مدارک – یک درایو USP که به کامپیوترکاری کارمند متصل بوده است.

با داشتن این جزئیات، می‌توانید الزامات پرونده را تعیین کنید.

اکنون می‌دانید که درمواقع، سوء استفاده ازامکانات شرکت، موضوع اصلی پرونده می‌باشد و شما به دنبال مدارک و شواهدی دال بر سوء استفاده کارمند شرکت ازامکانات در اختیارش برای انجام شغل شخصی خودش می‌باشد. در این درایو USB، بدنبال اطلاعاتی مرتبط با وب سایتها، ISP و یا نام‌های دامنه باید بود. می‌دانید که سیستم عامل کامپیوتر، ویندوزXP می‌باشد و فایل سیستمی‌آن FAT16 می‌باشد. اگر بخواهید این درایو USB را

نسخه برداری کنید و فایلهای مخفی و پاک شده را پیدا کنید بایستی از یک ابزار پزشکی قانونی کامپیوترقابل اعتماد استفاده کنید. از آنجاکه این درایو USB قبلا بررسی شده است، دیگر نیازی نیست که خودتان آن را مجدد بررسی نمایید.

شما می‌توانید این پرونده را پرونده "نام دامنه"، اسم گذاری کنید و مشخص کنید که کار شما این است که داده‌ها را از رسانه‌های ذخیره سازی جمع آوری کنید تا مشخص گردد که آیا جورج سوء استفاده کرده است یا خیر؟ به یاد داشته باشید که جورج فقط در مورد سوء استفاده مالی مضنون می‌باشد و این امکان وجود دارد که مدارکی که شما جمع آوری می‌کنید او را حتی تبرئه نماید یعنی اثبات کند که او بی گناه است. شما همیشه بایستی در پرونده‌هایتان از قبل قضاوت نکرده و در یافته‌های خود بی طرفانه عمل کنید. اگر که به صورت منظم و سیستماتیک عمل کنید، قطعا اینطور دوست دارید که نتایجی را بدست آورید که همیشه قابل اعتماد باشند.

نحوه برنامه ریزی تحقیقات خود

حال که شما الزامات و نیازمندی‌های پروند "نام دامنه" را مشخص کرده اید، می‌توان عملیات تحقیقی خود را برنامه ریزی نمایید. اکنون شما می‌توانید مراحل اصلی جمع آوری مدارک را شناسایی کرده وتحلیل پزشکی قانونی را انجام دهید. این مراحل که طرح اصلی شما برای تحقیقاتتان می‌باشد نشان می‌دهد که چه زمانی چه کاری را باید انجام دهید. برای انجام تحقیقاتتان روی این پرونده، بایستی مراحل اصلی زیر را انجام دهید که اکثر این مراحل درقسمتهای بعدی با جزئیات بیشتری توضیح داده خواهند شد.

- گرفتن درایو USB از مدیر جورج
- فرم مدارک راتکمیل کرده و زنجیره امانت داری را رعایت کنید.
- مدارک و شواهدرا به آزمایشگاه پزشکی قانونی خود منتقل کنید.
- مدارک خود را در جای مطمئن نگهداری نمایید.
- ایستگاه کاری پزشکی قانونی خود را آماده کنید.

- مدارک خود را ازجای مطمئنی که قبلا قرارداده بودید خارج کنید.
- از مدارک موجود نسخه برداری نمایید.(یعنی همان درایو USB)
- مدارک را مجددا درجای مطمئن قرار دهید.
- با ابزارهای پزشکی قانونی که در اختیار دارید فرآیند بررسی مدارک نسخه برداری شده را آغاز کنید.

قانون اول که درهمه تحقیقات انجام می‌گیرد حفظ و نگهداری مدارک است یعنی نباید دستکاری و یا مخدوش گردند.

از آنجاکه کارمندان اداره فناوری اطلاعات رسانه ذخیره سازی را مصادره و ضبط کرده است، بایستی برای بدست آوردن اسناد وشواهد به سراغ آنها بروید. مدیر اداره فناوری اطلاعات این اطمینان را می‌دهد که رسانه ذخیره سازی اطلاعات دریک محفظه امن نگهداری شده است. به یاد داشته باشید که هرچند این پرونده یک پرونده مرتبط با سیاستهای یک شرکت می‌باشد، اما بسیاری از پرونده‌های این چنینی، بدلیل اینکه نتوانسته بودند اصل امانت داری را رعایت کنند، به نتیجه مناسب و درستی نرسیده اند. اگر این اتفاق بیفتد، احتمال دارد که مدارک و شواهد مهم درخطر بیفتد.

برای مستند سازی کردن شواهد، شما بایستی جزئیات رسانه را ثبت کنید. جزئیاتی مانند اینکه، چه کسی شواهد را ترمیم و ریکاوری کرده است و یا اینکه چه زمانی و چه کسی آنها را دراختیار دارد. به کمک فرم امانت داری می‌توانید در مستندسازی اینکه مدارک و شواهد اصلی چه تغییری داشته و یا نداشته اند و یا اینکه مدارک نسخه برداری شده برای پزشکی قانونی دچار تغییراتی شده اند یا خیر؟

بسته به اینکه شما دریک اداره مجری قانون کار می‌کنید و یا اینکه در یک شرکت خصوصی هستید، بایستی یک فرم امانت داری مدارک مرتبط را پرکنید که همانطورکه گفتیم کاملا وابسته به محیط کارتان دارد. این فرم باید طوری انتخاب گرددکه خواندن و استفاده کردن ازآن راحت باشد. و می‌تواند حاوی اطلاعات مرتبطی با چند نوع مدرک باشد. بسته به اینکه مدیر اداری چه درخواستی داشته باشد شما می‌توانید یک فرم تک مدرکی (که هرکدام از مدارک را در یک صفحه مجزا فهرست برداری می‌کند.) و یا یک

فرم چند مدرکی را ایجاد و تکمیل کنید. (شکل۲-۲)

اگر لازم باشد، چگونگی استفاده از فرم امانت‌داری مدارک را مستندسازی نمایید در تهیه فرم امانت داری مدارک، هرچقدرکه راحتی پر کردن را بیشتر رعایت کنید، کاربری که می‌خواهد آن را پر کند راحت‌تر خواهد بود و از طرفی اگر از روش استانداردی در تهیه این فرم استفاده کنید این اطمینان را کسب می‌کنید که همه افرادی که می‌خواهند از اقلام جمع آوری شده استفاده کنند تعاریف مشابهی را خواهند دید. که این استانداردسازی فرم‌ها منجر به حفظ کیفیت خوبی شده و از گیج شدن و بروز مشکل دراستفاده از مدارکی که شما جمع آوری کرده اید، جلوگیری می‌کند.

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

شکل ۲-۲. یک فرم چند مدرکی ساده که در یک شرکت استفاده می‌شود.

یک فرم حفظ امانت داری مدرک معمولا شامل اطلاعات زیر می‌باشند.

- **شماره پرونده** – شماره ای است که سازمان شما هنگام شروع تحقیقات تخصیص

می‌دهد.

- **سازمان تحقیقاتی**– نام سازمان شماست. در شرکتهای بزرگ که شعبه‌های گسترده دارند، امکان دارد که چندین شرکت وسازمان تحقیقاتی روی پرونده آن درنقاط مختلف دنیاهمزمان کارمی‌کنند.
- **محقق (کارآگاه) (مامور تحقیق)** – نام مامور تحقیقی که روی پرونده کارمی‌کند. اگر چندین مامورتحقیق روی پرونده کارمی‌کنند کافیست نام سرپرست قیم تحقیقاتی را ذکرکنید.
- **ذات وطبیعت پرونده** – توضیح کوتاهی از پرونده ارائه می‌گردد. بطور مثال دریک محیط شرکتی این مورد می‌تواند "بازیابی داده‌ها برای دادخواهی" و یا "پرونده نقض سیاست کارمندی" باشد.
- **محلی که مدارک وشواهد بدست آمده اند** – محل دقیق مکانی که مدارک جمع آوری شده اند. اگر که از یک فرم چند مدرکی استفاده می‌کنید برای هرمکان جدید، بایستی یک فرم جدید نیزتهیه گردد.
- **توصیفی ازمدارک و شواهد** – فهرستی از اقلام مستندات وشواهد مثلا "هارد درایو 20GB" یا "یک درایو USB 128MB". در یک فرم چند مدرکی، توصیفی برای هرکدام ازاقلام مدارک وشواهد که بدست می‌آورید بنویسید.
- **نام شرکت فروشنده** – نام فروشنده (سازنده) مدرک کامپیوتری را بنویسد. مثلا در موردهارد دیسک 20GB می‌توانید Maxtor20GB بنویسید و یا برای درایو USB عبارت 1GB PNY TECHNOLOGY را بیابید. در فصلهای بعدی شاهد خواهید بود که درچگونگی بازیابی اطلاعات نام شرکت تولید کننده می‌تواند بسیار تاثیرگذار باشد.
- **شماره مدل با شماره سری** – اگر روی قطعه کامپیوتری شماره سری یا شماره مدل آمده باشد آن را دراینجا ذکر کنید. بسیاری ازقطعات کامپیوتری مانندهارد دیسک، تراشه‌های حافظه، کارتهای توسعه و ... بجای شماره سری، از شماره مدل استفاده می‌کنند.

- **مدرک توسط چه کسی بازیابی شده است** – نام مامورتحقیقی که مدارک را بازیابی و ترمیم کرده است، زنجیره امانتداری هر سند و مدرکی با این اطلاعات شروع می‌شود. اگر بطورمثال، شما نام خود را درج کنید، نشان داده اید که کنترل مدارک برعهده شماست واین مسئولیت را دارید که هیچ چیزی مدارک را خراب نکرده وهیچ کس به آن دست درازی ننماید. درحقیقت هرشخص که اسمش دراین قسمت آورده شود مسئول حفظ، انتقال وایمن سازی آن مدرک خواهد بود.
- **تاریخ و زمان** – تاریخ و زمانی که این مدرک وارد شده است که بیانگر زمان دقیق شروع امانت داری مدارک می‌باشد.
- **مدرک در کدام قفسه قفلدار نگهداری می‌گردد** - نشان می‌دهد که این مدرک کی و چگونه در کدام مکان امن مجاز قرار گرفته است.
- **شماره قلم/ مدرک توسط چه کسی پردازش شده است/ نوع مدرک/ تاریخ/ زمان** - زمانیکه شما یا هر مامور تحقیق مجازی مدرک را از قفسه ایمن آن برای بررسی و تحلیل برمی‌دارید نام خودتان و شماره آن قلم را یادداشت نموده و توضیح دهید چه کاری روی این سند انجام گرفته است.
- **صفحه** – بازاء هر مکان، فرم‌هایی که برای فهرست کردن همه شواهد استفاده شده‌اند، بایستی شماره صفحه داشته باشند. این شماره صفحه را بنویسید و برای هر دسته ازاین مدرک مجموع صفحات را نیز بیاورید. بطور مثال، اگر از یک مکان، ۱۵ عدد مدرک جمع آوری کرده اید وفرم شما تنها ۱۰ سطر دارد، بایستی دو تا فرم چند مدرکی را پرکنید بطوریکه فرم اول به صورت "صفحه ۱ از ۲" وفرم دوم بصورت "صفحه ۲ از۲" نوشته می‌شود.

شکل ۳-۲ یک فرم تک مدرکی را نشان می‌دهد که درهر صفحه تنها یک مورد از مدرک را فهرست کرده است. که در پیدا کردن یک قطعه خاص به شما خیلی کمک می‌کند. والبته فضا برای توضیحات بیشتری را نیز دارد. که این خود به شما بسیار کمک می‌کند هنگامی‌که بخواهید تحقیقات خود را تکمیل کرده و گزارش نهایی را ارائه کنید با این فرم، شما با دقت زیادی می‌توانید نسبت به مدارکی که یافت شده اند وآنچه که روی

آنها انجام گرفته است حساب باز کنید.

شما در تحقیقاتی که انجام می‌دهید می‌توانید از هر دو فرم تک مداری و چند مدرکی استفاده کنید. با استفاده از این دو فرم، شما می‌توانید فرم تک مدرکی را با خود مدرک نگهداری کنید و فرم چند مدرکی را درفایل گزارش خود نگهداری کنید. از آنجا که استفاده ازدو فرم باعث ایجاد افزونگی می‌گردد وخود می‌تواند به نوعی جهت افزایش کیفیت کنترل مدارک شما نیزمطرح گردد.

ایمن سازی مدارک و مستندات

تحقیقات کامپیوتری نیازمند آن می‌باشد که شما برای انجام روالهایتان یک پرونده را درست انجام دهید. بطور مثال، اگر مدارک یک پرونده حاوی یک سیستم کامل کامپیوتری و رسانه‌های ذخیره سازی مرتبط با آن باشد مانند فلاپی دیسک، کار تریج zip و یک درایو USB، باید وقتی که روی این اسناد حساب می‌کنید واقعا به آنها اطمینان داشته باشید. بعضی از مدارک آنقدر کوچک هستند که داخل یک کیف مدارک قرار گیرند اما بعضی از آنها مانند صفحه نمایش، صفحه کلید، چاپگر و ... خیلی بزرگ هستند.

برای ایمن سازی و دسته بندی مدارکی که حاوی مولفه‌های بزرگ کامپیوتری می‌باشند، می‌توانید ازکیف‌های مدرک بزرگ و یا برچسب‌ها، نوارها و ... استفاده کنید.

هنگامی‌که ازاین موارد برای ایمن سازی مدارک کامپیوتری استفاده می‌کنید مطمئن شوید که اینها برای نگهداری این قطعات کامپیوتری موثر وامن هستند. همیشه نسبت به الکتریسیته ساکن که می‌تواند داده‌های دیجیتال را از بین ببرد دقت کنید. به همین دلیل، مطمئن گردید که کیف‌هایی که برای نگهداری مدارک از آنها استفاده می‌کنید ضد ساکن باشند و همچنین مطمئن شوید که محل نگهداری مدارک با بالشتک‌هایی مناسب سازی شده باشد. چرا که این بالشتک گذاری‌ها از بروز خرابی‌های احتمالی مدارک هنگام جابه جا نمودن آنها از مکانی به مکان دیگر جلوگیری می‌کند.

از آنجاییکه شاید شما هیچ چیزی را برای ایمن سازی مدارک نداشته باشید، شاید