UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

"DISEÑO DE UN LABORATORIO FORENSE DIGITAL"

PARA OPTAR AL GRADO DE MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

ING. GUSTAVO PRESMAN

PRESENTADO POR:

ANDRADE, JORGE ROBERTO

MOLINA SIGÜENZA, RICARDO ALBERTO

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América.

Septiembre 2014

Contenido

GLOSARIO

GATEWAY: Una pasarela, puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

MALWARE: Del inglés malicious software, también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

BOT: Palabra que resulta de una aféresis practicada sobre robot— es un programa diseñado para interactuar con otros programas, servicios de Internet o seres humanos de manera semejante a como lo haría una persona.

LOGS: Un log es un registro oficial de eventos durante un rango de tiempo en particular. En seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

HASH: También llamadas funciones picadillo, funciones resumen o funciones de digest. Una función hash H es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. En la informática son usadas para garantizar la integridad de los datos.

HOST: El término host ("anfitrión", en español) es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

CADENA DE CUSTODIA: Se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene como fin no viciar el manejo que de ellos se haga y así detectar posibles alteraciones, sustituciones, contaminaciones o destrucciones.

Desde la ubicación, fijación, recolección, embalaje y traslado de la evidencia en la escena del siniestro, hasta la presentación al debate, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena, es la misma que se está presentando ante el tribunal, o el analizado en el respectivo dictamen pericial.

El propósito de mantener un registro de cadena de custodia es permitir la identificación de acceso y circulación de pruebas digitales potenciales en cualquier punto dado en el tiempo. El registro de cadena de custodia debe contener la siguiente información como mínimo:

1. Un identificador único de evidencia

2. Registrar quien accede a la evidencia con hora y lugar donde se llevó a cabo

3. Registrar quién verifica las pruebas de entrada y salida de la planta de preservación de pruebas y el momento en el que sucede

4. Registrar por qué la prueba se desprotegió (en cualquiera de los casos y su propósito) y la autoridad competente que lo realizo

5. Registrar todo cambio inevitable a la evidencia digital potencial, así como el nombre de la persona responsable y la justificación del cambio.

DoS (Denial of Service): Denegación de Servicios, por sus siglas en inglés, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Ciberterrorismo: También conocido como terrorismo electrónico, es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

INTRODUCCIÓN

Recientemente se ha identificado una necesidad en el ámbito de la Informática Forense en relación con los delitos informáticos que están en una evolución continua a nivel mundial. Hoy en día las tácticas para la suplantación de identidad, ingeniería social, robo de contraseñas, espionaje, ciberterrorismo, fraude, ataques de DoS, entre otros. Están latentes cada vez más, tanto si estos delitos informáticos son a nivel personal o si son ataques a la industria independientemente cual sea su clasificación y si su sector es público o privado.

Bajo este contexto es necesario tener las capacidades, habilidades, herramientas, personal idóneo y el apoyo de la Administración de Justicia para poder demostrar a los delincuentes o atacantes que se tiene la capacidad para responder a todas aquellas acciones fraudulentas.

Es por eso la iniciativa de este proyecto la cual quiere brindar un diseño de un laboratorio digital forense para su incursión tanto a nivel público como privado y que sirva para un mejor tratamiento de la evidencia digital en busca del entendimiento de lo que ocurre o ha ocurrido en hechos bajo inspección de anormalidad.

Este diseño de laboratorio digital forense estará regido bajo las normas, metodologías, regulaciones y estándares internacionales para poder cubrir con las demandas de los diferentes delitos informáticos y poder asegurar el procesamiento de la evidencia digital en cuanto a su identificación, preservación, extracción, análisis, interpretación, documentación y presentación.

Además se pretende crear un precedente que con este tipo de proyectos enfocados en la Informática Forense fortalecer esta especialidad técnico-legal desde la Administración de Justicia hasta el ámbito educacional pasando por la concientización de todos los sectores públicos y privados con el fin de combatir los delitos informáticos formando una base en una sociedad de la información y del conocimiento que se apoyen en los avances tecnológicos emergentes, con el fin de recabar, analizar, custodiar y detallar elementos probatorios basados en sistemas de información que procuren la identificación y reconstrucción de la verdad de los hechos que se investigan.

OBJETIVOS

OBJETIVO GENERAL

Diseñar un laboratorio forense digital utilizando metodologías y estándares internacionales en cuanto a la recolección, investigación, adquisición y preservación de la evidencia digital para poder ser implementado tanto a nivel público como privado.

OBJETIVOS ESPECÍFICOS

1. Definir los conceptos asociados que integran a la evidencia digital forense, los métodos que conducen a la investigación de la evidencia digital, mencionar los tipos de investigación forense a nivel de red, dispositivos móviles, computadoras de escritorio, laptops, entre otros.
2. Explicar el establecimiento y la gestión de un laboratorio forense digital, identificar el alcance de los requerimientos del laboratorio y especificar la localización geográfica del laboratorio forense digital.
3. Desarrollar un plan de negocio para el laboratorio forense digital.
4. Definir el personal a cargo del laboratorio forense digital y considerar los requerimientos para la formación continua del personal a cargo.
5. Explicar las regulaciones y los estándares nacionales e internacionales para mantener un nivel fidedigno y eficiente.

IMPORTANCIA

Actualmente entidades públicas y privadas e incluso la administración de Justicia, se van dando cuenta de que la tecnología es una parte cada vez más importante de nuestra vida laboral, social y personal. Pero también este avance tecnológico es aprovechado por profesionales de la estafa y el engaño cibernético con lo que es imprescindible la figura de detectives tecnológicos, expertos informáticos que asesoren de manera técnica y profesional y que garanticen los derechos, la privacidad de datos y que brinde una protección ante individuos que se amparan ante el anonimato de Internet, estos detectives tecnológicos son conocidos como peritos informáticos.

El perito informático es un nuevo perfil profesional, que surge de las nuevas tecnologías y que está especializado en las Tecnologías de la información y la comunicación (TICs[1]), con una demanda al alza debido al aumento de conflictos, tanto privados como aquellos que deben resolverse mediante juicio, en los que intervienen sistemas informáticos.

El ciberespionaje, las preocupaciones en materia de privacidad y el personal interno malintencionado son noticia y ocupan un lugar destacado en las discusiones sobre seguridad cibernética en la última década.

Debido al exponencial aumento de los delitos a través de equipos electrónicos, se han diseñado técnicas, herramientas y buenas prácticas en la informática forense, orientadas a la colección, preservación, análisis y presentación de la evidencia digital. En ese sentido, los cuerpos y órganos que llevan a cabo las investigaciones en materia judicial, tales como la Fiscalía General de la Republica (FGR), Policía Nacional Civil (PNC) y Corte Suprema de Justicia (CSJ), así como las instituciones encargadas de formar a gestores de la seguridad de la información en el ámbito de la informática forense como universidades podrán optar a este tipo de diseño y de poder implementar laboratorios de informática forense con el objeto de ofrecer solución para la

[1] Se denominan Tecnologías de la Información y las Comunicación TICS al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TICs incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.

identificación, adquisición, análisis y presentación de las evidencias digitales en el contexto de la situación bajo inspección.

La informática forense procura descubrir e interpretar la información en medios informáticos para establecer y detectar pistas sobre ataques informáticos, robo de información, registro de conversaciones, pistas de correos electrónicos, revelación de contraseñas, etcétera. La importancia de la interpretación de la información y el poder mantener la integridad de la evidencia digital o electrónica es sumamente frágil, teniendo en cuenta sus características principales: es volátil, es anónima, es duplicable, es alterable y modificable y eliminable.

La disciplina forense adaptada al ámbito de las nuevas tecnologías hace su aparición como una disciplina auxiliar de la justicia moderna, y surge como respuesta al auge delincuencial para enfrentar los desafíos y técnicas de los intrusos informáticos.

En el momento actual son muchos los casos en los que se obtienen distintos medios de prueba, vitales para el éxito de una investigación como por ejemplo: discos duros, teléfonos móviles, computadoras, servidores, sistemas GPS[2], entre otros.

La importancia de la creación de un diseño de laboratorio digital forense es principalmente para el análisis y la reconstrucción de eventos sobre delitos informáticos, como contraparte la implementación de un laboratorio de informática forense puede tener muchas versiones y alcances, las cuales dependerán del ámbito y necesidades de la organización, aspectos como el presupuesto disponible, personal capacitado, la legislación actual del país, determinarán el diseño de la plataforma y la estructura del laboratorio. De igual forma las organizaciones también deben considerar cuales serían los caminos evolutivos que deberán adoptar una vez diseñado el modelo inicial, toda vez que se puede evolucionar en cantidad de peritos, cantidad y forma de los procedimientos, costo por casos, entre otros.

Realizar este tipo de proyecto relacionado a la problemática existente sobre los delitos informáticos en la actualidad del país, es con el objetivo de repercutir en las instituciones que están ligadas a resolver la creciente ola de incidentes, fraudes y ofensas, con el fin de enviar un mensaje claro a los intrusos. Además inculcar sobre aspectos en la educación superior, incluir carreras donde se pueda adoptar este tipo de especialidades, hay que tener en cuenta que los

[2] El GPS es un sistema de posicionamiento por satélites desarrollado por el Departamento de la Defensa de los E.U., diseñado para apoyar los requerimientos de navegación y posicionamiento precisos con fines militares. En la actualidad es una herramienta importante para aplicaciones de navegación, posicionamientos de puntos en tierra, mar y aire.

delitos informáticos van en aumento, y se deben tener en consideración las nuevas problemáticas tecnológicas como el Big Data y el Internet de Todo (IoE[3]) para poder afrontar estos nuevos retos. A parte concientizar a la administración de Justicia poder introducir leyes que garanticen el cumplimiento de la ley ante delitos informáticos. Por último, la introducción de este tipo de laboratorios sirva para dar a los gestores de la seguridad de la información los conceptos y prácticas esenciales de la investigación de la computación forense y que sean capaces de probar los conocimientos adquiridos mediante la realización de tareas prácticas, sin un laboratorio digital forense con una base sólida en sus instalaciones a nivel de hardware y software no se lograrán los objetivos propuestos en módulos netamente técnicos como por ejemplo: Análisis forense a sistemas operativos Linux, análisis forense a sistemas operativos Windows, análisis forense en dispositivos móviles, evidencia física entre otros. Por lo tanto la implementación de laboratorios adecuados es un reto más en el proceso de formación.

[3] Internet de Todo (Internet of Everything, por sus siglas en inglés) es un concepto que se refiere a la interconexión digital de objetos cotidianos con Internet. Alternativamente, Internet de las cosas es el punto en el tiempo en el que se conectarían a Internet más "cosas u objetos" que personas.

JUSTIFICACIÓN

Hoy en día la Informática Forense no está establecida como la disciplina para esclarecer los actos catalogados como delitos informáticos y existe un gran vacío a nivel institucional del involucramiento en la aplicación de la informática forense para dar solución a todo este tipo de hechos, tanto en el apartado jurídico, penal y educacional. La iniciativa de crear un modelo de diseño de laboratorio digital forense, es proveer tanto en su funcionamiento a nivel de software, hardware, manejo de riesgos, recurso humano y recurso económico para mantener la idoneidad del procedimiento de la evidencia digital y sostener las medidas de seguridad y control de los procesos a nivel legal u organizacional.

La implementación de este tipo de diseño proporcionara al investigador distintas herramientas que le facilitarán la tarea, es preciso tener presente la ingente cantidad de datos a examinar y el reto que supone, más aún en una especialidad relativamente reciente y multidisciplinaria, que carece de un estándar consensuado en cuanto a medios y técnicas.

¿Qué se puede lograr mediante el uso de la Informática Forense y una propuesta de diseño de un laboratorio forense digital?, a continuación se mencionan algunos servicios que pueden llevarse a cabo:

1. Recuperación de archivos ocultos, borrados o dañados
2. Identificación de rutas, modificaciones y autoría de documentos y datos
3. Acceso a información protegida o cifrada, revelado de contraseñas
4. Seguimiento de transferencias de archivos, correos electrónicos, sesiones de chat
5. Comunicaciones vía red (Internet) y VoIP[4]
6. Identificación de origen y destino. Rastreo de archivos en Cloud Computing
7. Posicionamiento e historial de dispositivos dotados de GPS
8. Auditoría de actividad en computadores y dispositivos electrónicos.
9. Pruebas de penetración y certificación de seguridad de redes y sistemas
10. Estudio de virus, troyanos, rootkits, Ingeniería inversa.

[4] Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VozIP, (VoIP por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

Además provee fortalecimiento en la administración de justica en la relación con el delito informático, en los siguientes ámbitos:

1. Concienciación del público
2. Estadísticas y datos sobre delitos informáticos
3. Entrenamiento uniforme y cursos de certificación para investigadores
4. Actualización del marco regulatorio
5. Cooperación con los proveedores de tecnología
6. Estructuración de unidades de lucha contra el delito informático

Las técnicas forenses en el entorno digital, cuentan con un amplio horizonte de aplicación, desde la recuperación de información en soportes informáticos intervenidos, por ejemplo en casos de terrorismo, fraude fiscal, malversación de fondos, espionaje industrial o civil. Hasta la geolocalización y seguimiento del historial de dispositivos GPS, móvil y VoIP, que pueden resultar decisivos en cualquier investigación.

La finalidad de las técnicas forenses aplicadas al medio digital, no es otra que contribuir a detener y judicializar a los culpables de un hecho y contar con las pruebas de cargo apropiadas que resulten en una sentencia condenatoria o en el caso contrario, exculpar a un inocente.

Además, a nivel educacional se reflejaría que se deben actualizar los currículos para preparar gestores de la seguridad de la información como peritos informáticos para hacer frente a un tipo de criminalidad que está relacionado con tecnologías de la información. Y esto aumentaría con un nivel apropiado de profesionales con las habilidades para combatir el problema creciente del delito informático.

El proyecto tiene como objetivo beneficiar a todas las instituciones que estén involucradas directa e indirectamente en la aplicación de la Informática Forense, en primer lugar a las instituciones educativas ya que ellas generarían profesionales competentes en esta ciencia y sus enfoques curriculares cambiarían con el objeto de forjar a comprender los delitos informáticos y profundizar en esta ciencia multidisciplinaria. Luego beneficiar a instituciones como la Fiscalía General de la Republica (FGR) que es la encargada de dar resolución a casos delictivos, a la Policía Nacional Civil (PNC) que velan por guardar la cadena de custodia de la evidencia digital y la Corte Suprema de Justicia (CJS) que se encarga de verificar el cumplimiento de las leyes y dar el veredicto final en este tipo de hechos.

ALCANCES Y LIMITACIONES

ALCANCE

El proyecto de investigación se enfocará en el diseño de un laboratorio forense digital donde se establecerán las condiciones para dar un tratamiento adecuado a los diferentes delitos informáticos aplicando normas, metodologías y estándares en las cuales deberá ser tratada la evidencia digital para poder garantizar su proceso legal.

LIMITACIÓN

La poca incursión de la ciencia de la Informática Forense en El Salvador como por ejemplo en instituciones de gobierno, universidades, empresa privada, entre otros. Debilitará aspectos en la investigación como son los temas de regulaciones, leyes aplicables a delitos informáticos y personal capacitado en el peritaje informático. Aspectos como la falta de inversión en este tipo de programas ocasionaran fragilidad en ciertas bases del diseño ya que afectarán en el recurso del capital humano, instalaciones adecuadas y la adquisición de hardware y software.

RESULTADOS ESPERADOS

Se pretende con este tipo de investigación dar un lineamiento o propuesta para poder implementar un laboratorio forense digital y poder contribuir a una necesidad que existe en esta área de la Informática que atañe a los delitos informáticos en El Salvador. Actualmente en el país no hay centros especializados acordes al análisis de la evidencia digital y en procedimientos ante una diligencia legal, las evidencias recolectadas pierden su validez por tratamientos inadecuados.

A continuación se presenta una lista de los resultados a esperar:

1. Instituciones del sector público o privado tengan una propuesta solida de implementación de un laboratorio forense digital.
2. Contribuir a la formación de peritos informáticos para la recolección de evidencia digital basada en normas de buenas prácticas, procesos y estándares internacionales.
3. Proponer a las universidades que con la implementación de este tipo de laboratorios potenciarían a los gestores de la seguridad de la información ya que los fundamentos teóricos no pueden ser comprendidos si no hay una base práctica.
4. Que este tipo de investigación marque un precedente para futuros proyectos que abonen a la Informática Forense y formalicen a nivel nacional estándares para el estudio de la evidencia digital.
5. Presentar a instituciones del estado, como la Fiscalía General de la Republica (FGR), Policía Nacional Civil (PNC), Corte Suprema de Justicia (CSJ) este tipo de proyectos para que formalicen estos laboratorios y ayude a evitar la impunidad en los delitos informáticos y de esta manera poder velar por los derechos de los ciudadanos y ciudadanas.

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO 1: INVESTIGACIÓN PRELIMINAR

PLANTEAMIENTO DEL PROBLEMA

Debido al gran avance de las tecnologías de la información la tendencia en la creación y almacenaje de datos cada vez está en aumento, y aún más importante esta información sensible está orientada en los diferentes sectores de la industria donde los datos de las organizaciones están manteniendo una gran cantidad de movimientos transaccionales. Esta situación ha venido a desencadenar una infinidad de incidentes de seguridad impactando significativamente en las organizaciones. Hoy en día han aparecido nuevos tipos de ataques catalogándose como delitos informáticos o delincuencia informática, como por ejemplo: adivinación de contraseñas, ataques dirigidos por datos, confianza transitiva, explotación bugs del software, hijacking, ingeniería social, negación de servicios, phishing, reenvió de paquetes, rubberhosse, sniffing, spoofing, tempest, troyanos, etcétera. Estos tipo de ataques están siendo ejecutados por ciberterroristas, desarrolladores de virus, phreakers, script kiddies, crackers, atacantes internos; y cada uno de ellos con diferentes motivaciones como son la venganza, el dinero, el espionaje, el ego, el reto y hoy en día la ideología.

Los usos en los cuales es requerida la informatica forense ademas de los delitos informaticos, se pueden mencionar los siguientes:

- **PROSECUCIÓN CRIMINAL:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil
- **LITIGACIÓN CIVIL:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense
- **INVESTIGACIÓN DE SEGUROS:** La evidencia encontrada en las computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones
- **TEMAS CORPORATIVOS:** Puede recolectarse la información en casos que tratan sobre acoso sexual, robo, apropiación de información confidencial o propietaria, de espionaje industrial.
- **MANTENIMIENTO DE LA LEY:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información
- **SEGURIDAD LÓGICA:** virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico

- Otros

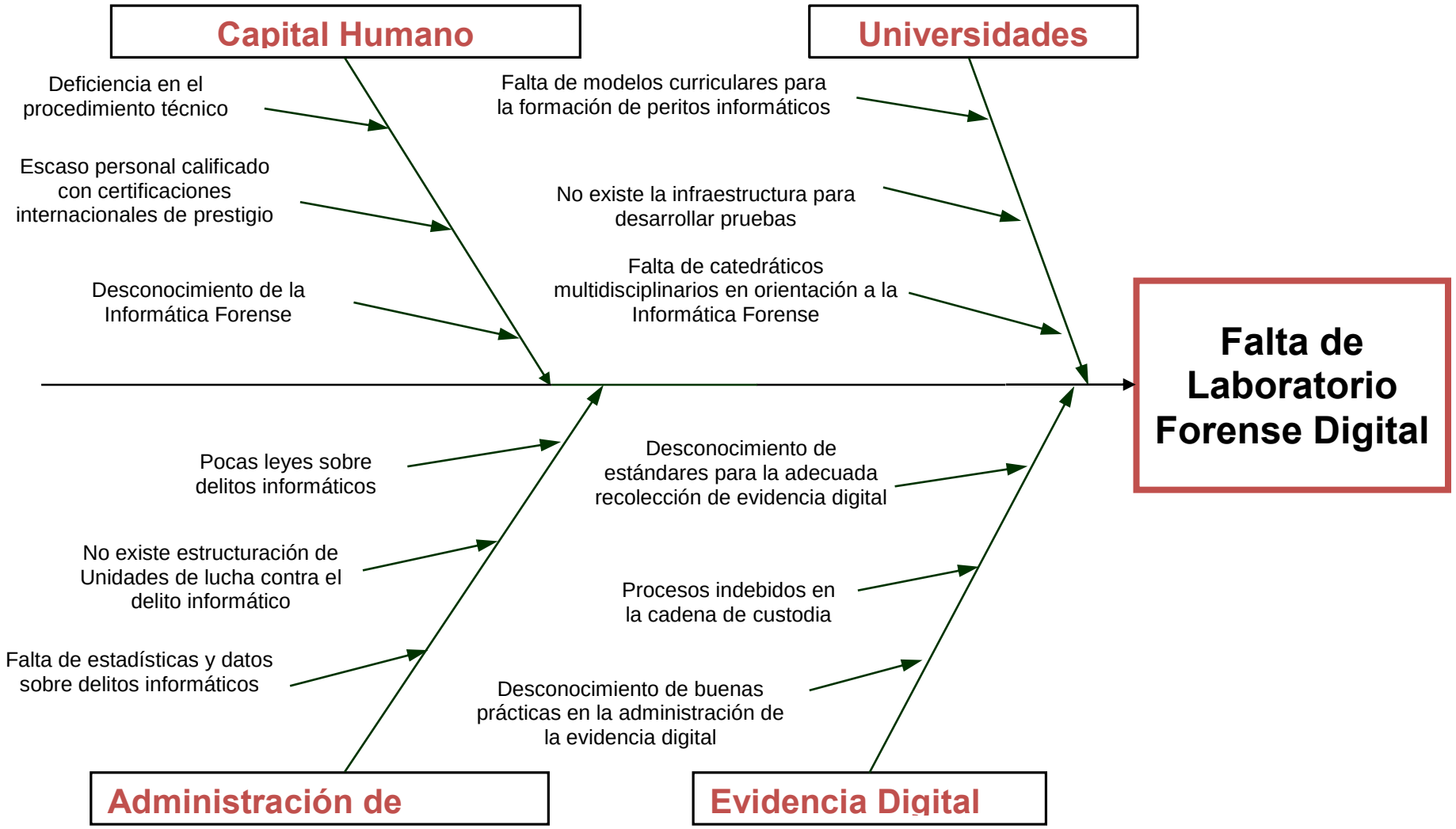
Es importante señalar que la informática forense no solo se aplica a los delitos informáticos, sino también a la investigación de otras conductas disvaliosas o incidentes que pueden ser explicados mediante el análisis de la evidencia digital.

La problemática antes mencionada hace surgir la necesidad de crear un diseño de laboratorio forense digital que cuente con los estándares internacionales, metodologías, infraestructura y personal capacitado para atender los incidentes que involucren medios informáticos. Con la implementación de un laboratorio forense digital se estaría contribuyendo a la formación de profesionales idóneos en el peritaje informático, sumado al hecho que en el país no existen laboratorios de entrenamiento que ayuden a gestar a investigadores de manera óptima para la resolución de casos. Además, el tratamiento de la evidencia digital es preciso extremar las medidas de seguridad y procedimientos ya que alguna imprecisión puede llevar a comprometer el proceso legal u organizacional.

De acuerdo a las tendencias de ataques informáticos a los que se encuentran las pequeñas, medianas y grandes empresas tanto públicas como privadas, la iniciativa de este tipo de proyecto para la implementación de un laboratorio forense digital es para dar respuesta a los diferentes tipos de incidentes y resolver de forma satisfactoria cualquier delito informático, teniendo en consideración el tratamiento adecuado de la evidencia digital en medios informáticos.

DIAGRAMA CAUSA-EFECTO

La representación de la solución a la problemática está reflejada por el siguiente Diagrama de Ishikawa.



FACTORES DE LA PROBLEMÁTICA

De acuerdo al Diagrama de Ishikawa se han establecido las siguientes causas primarias a la problemática:

a) **Capital Humano:** La Tecnología de la Información (TI) y la industria de la comunicación continua creciendo exponencialmente a lo cual produce nuevas tecnologías, dispositivos, sistemas, entre otros. Este rápido crecimiento impacta significativamente en la necesidad de peritos informáticos competentes que tengan las capacidades, destrezas y conocimientos técnicos-legales para resolver casos en los cuales estén comprometidos dispositivos electrónicos para dar solución a delitos informáticos.

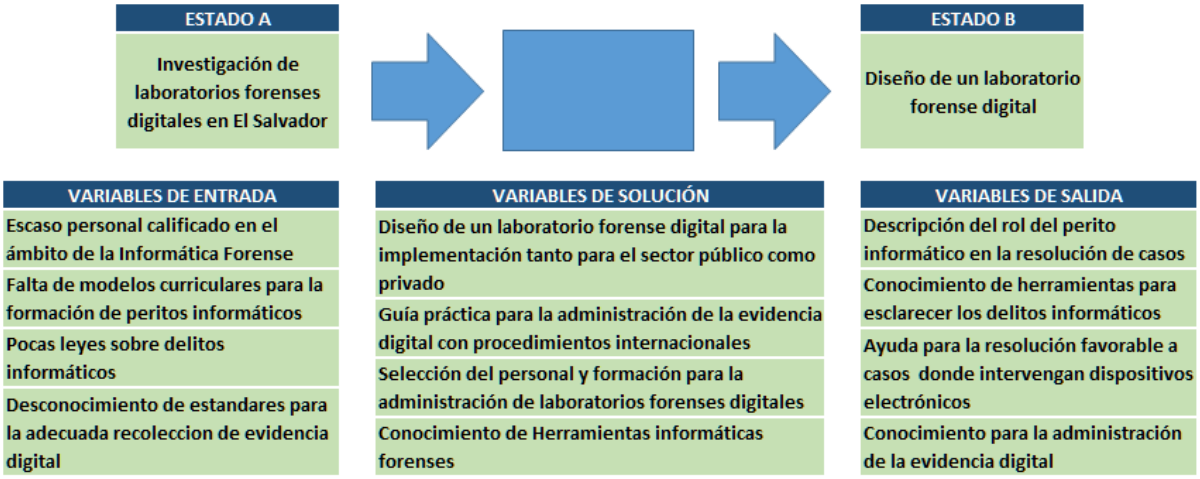
b) **Administración de Justicia:** El fortalecimiento de leyes y habilidades de justicia para enfrentar los desafíos de los delitos informáticos, en elementos y consideraciones que se hacen necesarios para apoyar tanto táctica como operacional este tipo de problemas.

c) **Universidades:** No es clara la formación de un perito informático multidisciplinario por lo que los modelos curriculares de los programas en relación a la seguridad de la información deben ser actualizados para preparar a sus egresados frente a los delitos informáticos en relación a la Informática Forense.

d) **Evidencia Digital:** Guías, conceptos prácticos, procedimientos y buenas prácticas internacionales en la administración de la evidencia digital para apoyar procesos donde la evidencia digital es fundamental para el esclarecimiento de algún hecho en específico.

FORMULACIÓN DEL PROBLEMA

Representación de la formulación del problema en base al siguiente diagrama de sistemas:



ANÁLISIS DEL PROBLEMA

Variable de entrada: No existen laboratorios forenses digitales en El Salvador

- Escaso personal calificado en el ámbito de la Informática Forense
- Falta de modelos curriculares para la formación de peritos informáticos
- Pocas leyes sobre delitos informáticos
- Desconocimiento de estándares para la adecuada recolección de evidencia digital

Variable de salida: Proponer un diseño de un laboratorio forense digital basado en requerimientos, estándares y metodologías internacionales para el tratamiento adecuado de la evidencia digital.

- Descripción del rol del perito informático en la resolución de casos
- Conocimiento de herramientas para esclarecer los delitos informáticos
- Ayuda para la resolución favorable a casos donde intervengan dispositivos electrónicos
- Conocimiento para la administración de la evidencia digital

Variable de solución: Diseño de un laboratorio forense digital para la implementación a nivel público o privado

- Diseño de un laboratorio forense digital para la implementación tanto para el sector público como privado

- Guía práctica para la administración de la evidencia digital con procedimientos internacionales
- Selección del personal y formación para la administración de laboratorios forenses digitales
- Conocimiento de Herramientas informáticas forenses

ENUNCIADO DEL PROBLEMA

¿En qué medida afecta la comprobación de la evidencia digital en un proceso de investigación de delito informático si no hay laboratorios forenses digitales especializados y con estándares de buenas prácticas en la recolección de evidencia digital en El Salvador?

FORMULACIÓN DE HIPÓTESIS

HIPÓTESIS GENERAL:

En qué medida afecta la comprobación de la evidencia digital en una investigación de delito informático si no hay centros de investigación de evidencia digital especializados y con estándares de buenas prácticas en la recolección de evidencia.

HIPÓTESIS ALTERNA:

En la medida que hayan centros de investigación de evidencia digital especializados y con estándares de buenas prácticas, mayores serán las probabilidades de comprobar la fiabilidad en la evidencia digital.

HIPÓTESIS NULA:

En la medida que hayan centros de investigación de evidencia digital especializados y con estándares de buenas prácticas, menores serán las probabilidades de comprobar la fiabilidad en la evidencia digital.

CAPÍTULO 2: INFORMÁTICA FORENSE Y LA SITUACIÓN ACTUAL EN EL SALVADOR

BREVE HISTORIA DE LA INFORMÁTICA FORENSE

Muchas son las definiciones que de informática forense podemos encontrar en gran número de publicaciones, pero todas ellas –de una manera u otra– hacen hincapié en unos puntos esenciales; de una forma simple, podríamos definir la informática forense como un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales.

De la definición vemos que se trata de un proceso, técnico y científico, que debe estar sujeto a una metodología, tendente primero a la recogida y después al análisis de los datos digitales que se pueden extraer de un sistema o conjunto de dispositivos informáticos o electrónicos, y todo ello con el propósito de ser presentados ante un tribunal. El fin último y principal objetivo que se deduce de la palabra forense, es su uso en un procedimiento judicial.

A comienzo de los años 90, el Federal Bureau of Investigation (FBI[5]) por sus siglas en inglés, observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por el ácido desoxirribonucleico (ADN[6]). Para ello, mantuvo reuniones en su ámbito, y a finales de los años 90 se creó la International Organization of Computer Evidence (IOCE[7]) por sus siglas en inglés, con la intención de compartir información sobre las prácticas de informática forense en todo el mundo. (National Institute of Justice)

En marzo del año 1998, el G8[8] –a través del subgrupo de trabajo denominado The High Tech Crime, siglas en inglés de Crimen de Alta Tecnología, conocido como el Grupo de Lyón-Roma[9]– encargó a la IOCE el desarrollo de una serie de principios aplicables a los procedimientos para actuaciones sobre pruebas digitales, así como la armonización de métodos y procedimientos entre las naciones que

[5] Federal Bureau of Investigation. Siglas en Ingles de Ofician Federal de Investigaciones

[6] El ácido desoxirribonucleico, abreviado como ADN, es un ácido nucleico que contiene instrucciones genéticas usadas en el desarrollo y funcionamiento de todos los organismos vivos conocidos y algunos virus, y es responsable de su transmisión hereditaria.

[7] International Organization of Computer Evidence, siglas en Inglés de Organización Internacional de Prueba Informática

[8] Se denomina G8 a un grupo informal de países del mundo cuyo peso político, económico y militar es tenido por relevante a escala global. Está conformado por Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido, Rusia

[9] El Grupo de Lyon Roma, es un grupo de trabajo que se estableció por primera vez bajo la presidencia italiana del G8 en 2001. Se discute y desarrolla cuestiones y estrategias relativas a la seguridad pública en un esfuerzo por combatir el terrorismo y la delincuencia transnacional

garantizasen la fiabilidad en el uso de las pruebas digitales recogidas por un estado para ser utilizadas en tribunales de justicia de otro estado. La IOCE, trabajó en el desarrollo de estos principios a lo largo de dos años. La Scientific Working Group on Digital Evidence (SWGDE[10]), principal portavoz de la IOCE en Estados Unidos, y la Association of Chief Police Officers (ACPO[11]) del Reino Unido, propusieron una serie de puntos que luego englobaron los principios generales que se presentaron en el año 2000 al Grupo de Lyón. (International Organization on Computer Evidence (IOCE))

Cabe mencionar instituciones que hoy en día se están integrando cada vez más al ámbito de la informática forense como The High Technology Crime Investigation Association (HTCIA), que está diseñado para fomentar, promover y facilitar el intercambio de datos, experiencias, ideas y metodologías relacionadas con las investigaciones y la seguridad en las tecnologías avanzadas. HTCIA continúa afianzando su posición como líder en las organizaciones profesionales dedicadas a la prevención, investigación y persecución de los delitos relacionados con las tecnologías avanzadas.

En temas de certificación se encuentra ISFCEA, una entidad privada, fundada en conjunto con una compañía norteamericana dedicada a los temas de computación forense, denominada Key Computer Service, LLC. Esta asociación ofrece la certificación CCE – Certified Computer Examiner, la cual se otorgó por primera vez en el año 2003.

Hasta la fecha, la certificación CCE tiene varios niveles: básico y avanzando o maestro. Las habilidades requeridas para el nivel básico son: (Cano, Jeimy J., 2011)

- Identificación y adquisición de medios magnéticos
- Manejo, etiquetado y almacenamiento de evidencia digital
- La cadena de custodia
- El derecho a la privacidad
- Buen entendimiento de como eliminar, verificar y validad medios de almacenamiento de información, entre otros

La informática forense a nivel mundial es la ciencia dedicada a la recolección, preservación, análisis y presentación de la evidencia digital en casos judiciales, arbitrales o procesos internos disciplinarios.

[10] Scientific Working Group on Digital Evidence, Siglas en Ingles de Grupo Científico de Trabajo sobre la Evidencia Digital
[11] Association of Chief Police Officers, Siglas en Ingles de Asociación de Jefes de Policía

NUEVOS RETOS Y DESAFÍOS DE LA INFORMÁTICA FORENSE

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sean humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro. (Cano, Jeimy J.)

El Informe de Seguridad 2014 de Check Point[12] revela la prevalencia y el crecimiento en las amenazas que asolan las redes empresariales a través de la información obtenida en el transcurso del año 2013. Dicho informe está basado en la investigación colaborativa y el análisis en profundidad de más de 200.000 horas monitorizadas de tráfico de red desde más de 9.000 Gateways con prevención de amenazas, en organizaciones de más de 122 países. (Checkpoint)

De acuerdo al Informe de seguridad 2014 de Check Point:

- El 84% de las organizaciones analizadas descargaron software malicioso
- Cada 60 segundos un host accede a un sitio malintencionado
- Cada 10 minutos un host descarga Malware
- El 33% de los hosts no tienen versiones de software actualizadas
- El 73% de las organizaciones detectaron al menos un bot
- El 77% de los bots están activos por más de 4 semanas
- El 86% de las organizaciones tienen por lo menos una aplicación de alto riesgo
- El 88% de las compañías afirmó haber experimentado al menos un incidente con pérdida potencial de datos
- En 33% de las instituciones financieras analizadas, información de tarjetas de crédito fue enviada fuera de la organización

Verizon[13] en su informe sobre investigaciones de brechas en los datos de 2014, determina que el universo de amenazas puede parecer sin límites, pero el 92% de 100,000 incidentes analizados en los últimos 10 años, pueden ser descritos por solo 9 patrones básicos, los cuales son:

[12] Check Point Software Technologies Ltd. es un proveedor global de soluciones de seguridad IT.

[13] Verizon es una compañía que brinda soluciones de telecomunicaciones y banda ancha

1. Ataques de Intrusiones de Puntos de Venta (POS)[14]
2. Ataques a aplicaciones Web
3. Mal uso de información privilegiada
4. Robo o pérdida física de información
5. Software Criminal (Crimeware)[15]
6. Clonación de Tarjetas (Card Skimmers)[16]
7. Ataques de Denegación de Servicios (DoS)[17]
8. Ciber Espionaje
9. Errores comunes

Estos nueve patrones engloban de forma general un universo de técnicas de ataque que buscan vulnerar los sistemas y equipos de las víctimas.

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina, de acuerdo al Reporte Norton[18] 2013. De acuerdo a al reporte de Seguridad de Norton 2013, en el cuál se han entrevistado más de 13.000 personas en 24 países, para el año 2013, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 113 MM en doce meses, en donde el 83% de los costos financieros directos son el resultado de fraude, reparaciones, robos y pérdidas, en donde el costo promedio por víctima es de USD $298, lo que representa un 50% más que en el 2012. El mismo estudio revela que por cada segundo hay 12 víctimas de un delito informático, lo que da como resultado más de un millón de víctimas de delitos informáticos cada día, a nivel mundial. (Symantec)

El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina, expuesta por Carlos Sarzana en el libro Delitos Informáticos, AD-HOC (SARZANA, 2000). El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o

[14] Intrusiones POS típicas se iniciaron mediante la colocación de malware especialmente diseñado en el punto de venta de cajas que 'raspa' datos de la tarjeta mientras que se mantiene en la memoria temporal. Los datos de las tarjetas se extraen a través de una conexión remota desde las cajas hasta el Control maestro de los Ciber atacantes.

[15] Crimeware es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El término fue creado por Peter Cassidy, Secretario General del Anti-Phishing Working Group para diferenciarlo de otros tipos de software malicioso.

[16] El acto de usar un skimmer para recoger ilegalmente datos de la banda magnética de una tarjeta de crédito, de débito o de cajero automático. Esta información, es copiada en la banda magnética de otra tarjeta en blanco, y es utilizada por un ladrón de identidad para realizar compras o retirar dinero en efectivo en nombre del titular de la cuenta real.

[17] un ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

[18] Norton es un producto de Symantec Corporation, la cual es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática

información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. Por otro lado, el crecimiento sostenido del mercado negro de la información, funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal. Un estudio de RAND Corporation[19] afirma que los mercados negros cibernéticos son una economía de millones de dólares madura y en crecimiento, con una sólida infraestructura y organización social, y que, al igual que cualquier otra economía, seguirá evolucionando y reaccionando a la ley de la oferta y la demanda. (Corporation, RAND)

A pesar de los escenarios anteriores, la criminalística nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio. La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En un mundo donde las ciberamenazas se hallan en constante cambio, las organizaciones deben de comprender la naturaleza de los últimos ataques y cómo sus redes pueden estar potencialmente afectadas.

LA INFORMÁTICA FORENSE DISCIPLINA PARA ESCLARECER LOS DESAFÍOS INFORMÁTICOS

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

[19] RAND Corporation, es una institución sin fines de lucro que ayuda a mejorar la política y la toma de decisiones a través de la investigación y el análisis.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

Existen múltiples definiciones a la fecha sobre el tema forense en informática, según Rodney McKemmish. (Rodney McKemmish) Una Primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: **Computación Forense**, **Forensia Digital** y **Forensia en Redes**, entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

Es importante anotar, que al ser esta especialidad técnica un recurso importante para las ciencias forenses modernas, asumen dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

COMPUTACIÓN FORENSE

Esta expresión podría interpretarse de dos maneras:

a) Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o
b) Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero en conclusión ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

FORENSIA DIGITAL

Trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina

especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

FORENSIA EN REDES

La Forensia en Redes es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece a un profesional que entendiendo las operaciones de las redes de computadoras, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense: (Óscar López, Haver Amaya, Ricardo León)

1. **Prosecución Criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
2. **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. **Investigación de Seguros:** La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
5. **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

La informática forense tiene 3 objetivos, a saber: (Juan David Gutiérrez Giovanni Zuccardi)

1. La compensación de los daños causados por los criminales o intrusos

2. La persecución y procesamiento judicial de los criminales
3. La creación y aplicación de medidas para prevenir casos similares

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Una vez estudiado el informe, el G8 aprobó un conjunto de principios básicos para luego dictar una serie de recomendaciones aplicables a las evidencias digitales: (RFC 3227)

- Todos los principios generales de procedimientos y técnicas forenses deben ser aplicados cuando se manipulen pruebas digitales.
- Cualquier institución con atribuciones en la búsqueda, recolección, y análisis de pruebas debe tener una metodología o unos principios generales definidos con el objetivo de proteger los intereses de todas las partes. Dichos principios han de tener en cuenta las peculiaridades de cada ordenamiento jurídico.
- En la manipulación de pruebas digitales, las acciones que se lleven a cabo no deben alterar dicha prueba. Siempre que sea posible, no se realizará ninguna acción, durante la búsqueda, recolección, o manipulación de las pruebas digitales, que conlleve una alteración de la misma. En caso de que se tenga que actuar de tal forma que se altere la prueba, las acciones deberán ser completamente documentadas.
- Cuando sea necesario que una persona tenga acceso a una prueba digital original, dicha persona debe estar formada para ese propósito. Aunque es ampliamente aceptado que la mejor práctica es realizar una imagen digital de la prueba a analizar, y actuar sobre la copia, puede haber ocasiones, en el curso de una actuación, en que se tenga que acceder a la prueba digital original. Dicha acción, además de seguir el principio anterior, debe realizarse por una persona que esté formada en dicho aspecto.
- Toda actividad relativa a la recogida, acceso, almacenamiento, o transferencia de pruebas digitales debe ser completamente documentada, conservada y disponible para su estudio. Todas las manipulaciones que se lleven a cabo deben ser documentadas de forma total y comprensible, de manera que las acciones que se están registrando puedan ser reproducidas si fuera necesario. Es vital mantener la cadena de custodia.
- Cada persona es responsable de todas las acciones tomadas con respecto a la prueba digital mientras dicha prueba esté a su cargo. Dicha responsabilidad es personal y no corporativa.
- Cualquier institución o grupo, que sea responsable de la recogida, acceso, almacenamiento, o transferencia de una prueba digital, es responsable de cumplir y hacer cumplir estos principios. Las instituciones con atribuciones en la recogida y manipulación de pruebas

digitales, velarán para que estos principios se lleven a cabo, siendo un marco de referencia y trasladándose éstos a los procedimientos de actuación que se desarrollen en dichas instituciones.

Todas las técnicas utilizadas para la recogida y análisis de evidencias digitales, deben estar respaldadas por una buena metodología científica y documentadas en un protocolo de actuación, que recoja tanto los aspectos técnicos de la informática como los aspectos legales que se derivan de su peculiaridad forense. Para asegurar que las pruebas digitales son recogidas, preservadas, examinadas o transferidas de manera que se salvaguarde su integridad, fiabilidad, y precisión, todas las instituciones forenses, cuya función esté relacionada con dichas pruebas digitales, deberán establecer y mantener un sistema de calidad efectivo, sin olvidar tampoco la formación del personal. (Association of Chief Police Officers (ACPO))

INSTITUCIONES A NIVEL INTERNACIONAL QUE DAN SOPORTE A LA INFORMÁTICA FORENSE

La informática forense debido a su naturaleza debe estar respaldada tanto a nivel internacional como a nivel local, esto para garantizar unificación de procedimientos, estrategias y herramientas, todo con el fin de garantizar los elementos esenciales de las evidencias y resguardar la integridad de las mismas. La Asociación Internacional de Especialistas en Investigaciones Computacionales IACIS[20], por sus siglas en inglés y la Red Transnacional de la Alta Tecnología HTCN[21], son dos asociaciones internacionales que han desarrollado programas de certificación forenses en informática, que permiten detallar las habilidades requeridas y las capacidades deseables en los investigadores informáticos.

A continuación se presenta ejemplos de las certificaciones expedidas por cada una de las asociaciones antes mencionadas y una breve explicación de éstas:

IACIS

CREDENCIALES CERTIFICADORAS PARA INVESTIGACIÓN FORENSE EN INFORMÁTICA DE IACIS: La IACIS ofrece la certificación internacional denominada Certificación Externa de Computación Forense

[20] IACIS es una corporación sin fines de lucro de voluntariado internacional compuesto por profesionales de la informática forense dedicada a fomentar y perpetuar la excelencia educativa en el campo de la informática forense.

[21] High Tech Crime Network (HTCN), tiene como misión lograr las certificaciones más valiosos y reconocidos para nuestros miembros, a través de un amplio proceso que verifica la formación y la experiencia del solicitante, mientras que la aplicación de los más altos estándares de requisitos de certificación, la aplicación diligente de nuestras políticas, procedimientos y código de ética.

CFEC[22], la cual se encuentra diseñada para personas que pertenecen al área informática y tiene pocos conocimientos del ámbito legal o del policial.

HTCN

CREDENCIALES CERTIFICADORAS PARA INVESTIGACIÓN FORENSE EN INFORMÁTICA DE HTCN: La HTCN ofrece diversas certificaciones en la línea forense en informática. En particular se menciona la certificación de Investigador Certificado en Delito Informático CCCI[23] nivel básico y avanzado. El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento continuo que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones. Esta certificación es avalada y reconocida en diferentes tribunales y cortes del mundo, dada la seriedad y rigurosidad de proceso de certificación.

Todas las técnicas utilizadas para la recogida y análisis de evidencias digitales, deben estar respaldadas por una buena metodología científica y documentadas en un protocolo de actuación, que recoja tanto los aspectos técnicos de la informática como los aspectos legales que se derivan de su peculiaridad forense. Para asegurar que las pruebas digitales son recogidas, preservadas, examinadas o transferidas de manera que se salvaguarde su integridad, fiabilidad, y precisión, todas las instituciones forenses, cuya función esté relacionada con dichas pruebas digitales, deberán establecer y mantener un sistema de calidad efectivo, sin olvidar tampoco la formación del personal.

En el ámbito profesional también existen otras entidades que aseguran la formación de los peritos informáticos, estas entidades ofrecen certificaciones, reconocidas a nivel mundial por su contenido y la pericia que exigen al participante. Dentro de estas certificaciones de la industria podemos mencionar, más no limitar a las siguientes:

(ISC)²[24]

A principios de la década de 1980, las organizaciones que utilizaban redes informáticas empezaron a comprender que múltiples equipos conectados en diversos lugares eran mucho más vulnerables que un mainframe único. Por ello surgió la necesidad de dotar a estos sistemas de medidas de seguridad de la información, y de formar profesionales cualificados para planificar e implementar los procedimientos y políticas de seguridad. En aquel entonces no existía una titulación específica, ni escuelas que ofrecieran estudios apropiados.

[22] Computer Forensic External Certification
[23] Certified Computer Crime Investigator
[24] El Consorcio internacional de Certificación de Seguridad de Sistemas de Información o (ISC)², es una organización sin ánimo de lucro con sede en Palm Harbor, Florida que educa y certifica a los profesionales de la seguridad de la información.

La necesidad de una certificación profesional para mantener y validar un corpus de conocimiento común, unos valores y una ética para los individuos en la industria se convirtió en una creciente preocupación. Varias sociedades de profesionales de la tecnología informática reconocieron que se necesitaba un programa de certificación que validara la calidad del personal de la seguridad informática.

El (ISC)2 cuenta con la Certified Cyber Forensics Professional (CCFP)[25], esta certificación está dirigida a los profesionales en forense informática con más experimentados y que cuentan con la aptitud y la perspectiva de aplicar efectivamente su experiencia forense informática a una variedad de desafíos.

EC-Council[26]

Dentro de sus programas de formación y certificaciones ofrece una especialización exclusiva para la parte de Forense, es la certificación CHFI[27]. El programa CHFI en su versión 8, certifica individuos en la disciplina de seguridad, específicamente de la informática forense desde una perspectiva independiente del proveedor. La certificación CHFI fortalecerá el conocimiento de la aplicación de la fuerza pública, los administradores de sistemas, oficiales de seguridad, defensa y personal militar, profesionales legales, banqueros, profesionales de la seguridad, y cualquier persona que se preocupa por la integridad de la infraestructura de red.

OFFENSIVE SECURITY[28]

Ofrece una certificación líder en seguridad, es la OSCP[29]. El OSCP es una preparación en donde desafía a los estudiantes a demostrar que tienen una comprensión clara y práctica del proceso de pruebas de penetración y de ciclo de vida a través de un arduo examen de certificación de veinticuatro (24) horas.

Estas certificaciones y entidades, buscan garantizar una formación idónea, apegada a las buenas prácticas y siguiendo los debidos procesos, herramientas y técnicas. (Infosec Institute)

ASPECTOS LEGALES RELACIONADOS A LOS DELITOS INFORMÁTICOS Y AL USO DE LA INFORMÁTICA FORENSE

Entre los desafíos que generan los delitos informáticos, uno de los más importantes es el hecho que este tipo de delitos pueden ser cometidos sin respetar barreras geográficas o jurisdiccionales. En este

[25] Certified Cyber Forensics Professional, siglas en de Certificado de Ciber Forense Profesiona, ofrecida por (ISC)[2]
[26] EC-Council http://www.eccouncil.org/
[27] Computer Hacking Forensic Investigator
[28] Offiensive Security. http://www.offensive-security.com/
[29] Offensive Security Certified Professional

sentido, cualquier delincuente informático puede operar acciones desde un determinado lugar, conectarse a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. La cadena puede tener indeterminadas variables dependiendo de la complejidad del ataque y de los conocimientos del delincuente. Si bien esta situación no sucede en todos los casos, es relativamente sencillo realizar estos ataques en la actualidad para personas con conocimientos en informática. Esto representa para el Derecho un verdadero desafío a vencer.

Manuel Castells (Manuel Castells), en ocasión de un discurso del 2001, y hablando del "caos" positivo que Internet genera en la comunicación, dijo: *"Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España"*. En seguida citó el ejemplo de cuando en 2000 un sitio Web de EE.UU. organizó la venta de votos de personas ausentes, hecho que representaba un delito electoral en ese país. Pero la Web se mudó a Alemania, donde ese hecho ya no podía ser perseguido por las leyes de ese país. En consecuencia, una importante cantidad de grupos de delincuentes informáticos, organizan sus ataques desde lugares con poca o nula legislación en la materia, o bien, en aquellos países que aun teniendo legislación al respecto, no poseen un adecuado sistema para la detección y persecución eficaz de este tipo de delitos.

Un ejemplo de ello fue el caso de un ataque de tipo viral que costó a empresas norteamericanas miles de millones de dólares, el cuál fue atribuido por el FBI a un estudiante en Filipinas al que no se lo pudo acusar de crimen alguno. Rápidamente el gobierno filipino dispuso legislación para combatir el crimen cibernético con el objetivo de evitar futuros inconvenientes. (Phil Williams, Electronic Journal of the U.S. Department of State)

En un contexto de incremento de la ciberdelincuencia organizada a nivel mundial, los llamados "paraísos legales informáticos", son los considerados al momento de ejecución de estas actividades. En palabras del Dr. Marcelo Riquert (Marcelo Alfredo Riquert), habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad.

Debido al alcance global que tienen los delitos informáticos, entidades como la Unión Europea han creado políticas de seguridad tendientes al combate de este tipo de crímenes. De acuerdo al reporte de Tendencias de Seguridad Cibernética en América Latina y El Caribe, América Latina y el Caribe tienen la población de usuarios de Internet de más rápido crecimiento del mundo, con 147 millones de usuarios únicos en el 2013, lo que representó un aumento del 12% respecto del año 2012. (Symantec)

Es debido a estos números, que países como Bolivia, Colombia, Perú, Argentina, Brasil, México, Chile, Costa Rica, entre muchos otros, están trabajando en la creación de leyes que castiguen y persigan los delitos informáticos. Es por ello que algunos de estos países al tener reglamentado este tipo de delitos, cuentan con laboratorios especializados para la recopilación de evidencias, entre los países que muestran adelanto en este sentido podemos mencionar a Bolivia y a Perú. (Symantec)

Bolivia cuenta con el Instituto de Investigaciones Forenses (IDIF), el cual es un órgano dependiente administrativa y financieramente de la Fiscalía General de la República, que está encargado de realizar, con autonomía funcional, todos los estudios científico - técnicos requeridos para la investigación de los delitos o la comprobación de otros hechos por orden judicial. (Ley No. 1970 Nuevo Código de Procedimiento Penal de 25 de marzo de 1999, en su Título II, Capítulo II, Art. 75º.).

Argentina promulga el 4 de junio de 2008 la Ley 26388 de delitos informáticos, de esta manera se une a la lista de los países de Latinoamérica que cuentan con regulación legal sobre aspectos informáticos. A lo largo de su articulado tipifica, entre otros, los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP)
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP)
- Acceso a un sistema o dato informático (artículo 153 bis CP)
- Publicación de una comunicación electrónica (artículo 155 CP)
- Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP)
- Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP)
- Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data)
- Fraude informático (artículo 173, inciso 16 CP)

- Daño o sabotaje informático (artículo 183 y 184, incisos 5º y 6º CP)

Perú en su Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, incorporó los delitos informáticos al Código Penal. (Marcelo Alfredo Riquert)

Cada país ira teniendo poco a poco casos de éxito en la persecución y sanción de los delitos informáticos, y será inevitable el uso de personal idóneo y con infraestructura adecuada para la manipulación de pruebas de delitos.

¿QUÉ ES LA EVIDENCIA DIGITAL?

A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo checksums[30], hash MD5, SHA-1[31], SHA-256, estas últimas son más ampliamente recomendadas, SHA-1 produce una salida resumen de 160 bits de un mensaje que puede tener un tamaño máximo de 2^{64} bits mientras que SHA-256 produce una salida resumen de 256 bits de un mensaje de 2^{64} bits. (Brian Deering)

Cuando ha sucedido un incidente, generalmente, las personas involucradas en el crimen intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital.

La evidencia digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada idéntica como si fuera la original. Esto se hace comúnmente para no manejar los originales

[30] Una suma de verificación, (también llamada suma de chequeo o checksum), en telecomunicación e informática, es una función hash que tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.

[31] El SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST).

y evitar el riesgo de dañarlos. Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.

Las funciones criptográficas hash son un elemento fundamental en la criptografía moderna y juegan un papel importante en los procesos de evidencia digital.

Una función hash, o función resumen, toma un mensaje como entrada y produce una salida que llamamos código hash, o resultado hash, o valor hash, o simplemente hash. La idea básica de las funciones criptográficas hash es que los valores hash obtenidos con ellas sirven como una imagen representativa y compactada de una cadena de entrada, y pueden usarse como un posible identificador único de esa cadena de entrada: ese valor hash obtenido del mensaje de entrada suele llamarse resumen del mensaje o huella digital del mensaje.

Una de las propiedades deseables de las funciones de hash criptográficas es que sea computacionalmente imposible que se produzca una colisión. El valor de una función hash puede ser usado para certificar que un texto dado (o cualquier otro dato) no ha sido modificado, publicando el valor firmado de la función de hash si no es factible que se produzca una colisión. En este contexto, factible se refiere a cualquier método capaz de producirla más rápido que un ataque de cumpleaños de fuerza bruta[32].

La seguridad proporcionada por un algoritmo hash es sumamente dependiente de su capacidad de producir un único valor para un conjunto de datos dados. Cuando una función hash produce el mismo valor para dos conjuntos de datos distintos, entonces se dice que se ha producido una colisión. Una colisión aumenta la posibilidad de que un atacante pueda elaborar computacionalmente conjuntos de datos que proporcionen acceso a información segura o para alterar ficheros de datos informáticos de tal forma que no cambiara el valor hash resultante y así eludir la detección. Una función hash fuerte es aquella que es resistente a este tipo de ataques computacionales mientras que una función hash débil es aquella donde existe una creencia casi certera de que se pueden producir colisiones. Finalmente, una función hash quebrantada es aquella que se conoce métodos computacionales para producir colisiones.

La evidencia de digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo. Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros

[32] Un ataque de cumpleaños (o, en inglés, birthday attack) es un tipo de ataque criptográfico que se basa en la matemática detrás de la paradoja del cumpleaños, haciendo uso de una situación de compromiso espacio-tiempo informática.

sitios. Cuando se habla de "eliminar la fuente de la evidencia" significa neutralizar el sistema o la técnica utilizada por el sistema para dejar los rastros, al controlar esta técnica o proceso no existirá la evidencia y, por tanto, no habrá trazas que seguir en una investigación. También se puede referir a las técnicas anti forenses, que son métodos para limitar la identificación, recolección y validación de datos electrónicos (A la fecha, las técnicas anti forenses no cuentan con un marco de referencia compartido para su estudio o análisis). Si el atacante no puede materializar algún método para la eliminación de la evidencia, puede optar por esconder la evidencia o falsificarla. En la primera, la evidencia se dispersa en el medio que la contiene, se oculta en el mismo, o en el sistema donde se encuentra, limitando los hallazgos del investigador en su proceso. En la segunda, crea o invalida la evidencia residente en el sistema para eliminar las conclusiones y análisis que adelante el investigador. (Cano, Jeimy J., 2011)

Eoghan Casey (Casey Eoghan) en su libro, "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet", define la evidencia de digital como "*cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor*".

CLASIFICACIÓN DE LA EVIDENCIA DIGITAL

Jeimy Cano en su libro Evidencia Digital: Contexto, situación e implicaciones nacionales, clasifica la evidencia digital que contiene texto en 3 categorías: (Evidencia Digital: Contexto, situación e implicaciones nacionales)

1. Registros generados por computador: Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

2. Registros no generados sino simplemente almacenados por o en computadores: Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.

3. Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: Los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

CRITERIOS DE ADMISIBILIDAD

En legislaciones modernas existen cuatro criterios que se deben tener en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial. (Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis)

Autenticidad: Una evidencia digital será autentica siempre y cuando se cumplan dos elementos:

1. Demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos
2. La evidencia digital debe mostrar que los medios originales no han sido modificados, es decir, que la los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma.

A diferencia de los medios no digitales, en los digitales se presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales contrarios a los no digitales, en las que aplica que la autenticidad de las pruebas aportadas no será refutada. Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos. (Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis)

Confiabilidad: Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son "creíbles y verificables". Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.

Una prueba digital es confiable si el "sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba". La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización del registro de las acciones de los usuarios del sistema y que posea con un registro centralizado e íntegro de los mismos registros.

Suficiencia o completitud de las pruebas: Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada.

Apogeo y respeto por las leyes y reglas del poder judicial: Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico. (Evidencia Digital: Contexto, situación e implicaciones nacionales)

RELACIÓN ENTRE LA EVIDENCIA DIGITAL Y LA COMPUTACIÓN FORENSE

La informática forense es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada. Para conseguir sus objetivos, la informática forense desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales.

Todo hecho en el que un sistema informático esté involucrado, tanto si es el fin o un medio, puede ser objeto de estudio y análisis, y por ello, puede llevarse a juicio como medio probatorio.

La evidencia digital es cualquier documento, fichero, registro, dato, etc. Contenido en un soporte informático, susceptible de tratamiento digital, entre algunos ejemplos se pueden mencionar, pero no están limitados a:

- Documentos de Ofimática (Word, Excel, Open Office, etc.)
- Comunicaciones digitales (E-mails, SMSs, Mensajería, etc.)
- Imágenes digitales (Fotos, videos, etc.)
- Bases de Datos
- Ficheros de Registro de Actividad (LOGS)

Uno de los pilares más importantes de la informática forense es el valor que se le puede dar a las evidencias informáticas para aportar en los procesos judiciales, esto significa, su validez jurídica. (López, Javier Pagés)

EL ROL DEL INVESTIGADOR

Los investigadores estarán implicados en la identificación, recolección, consolidación y preservación de la evidencia digital. Además deberán seguir una serie de procedimientos y normativas, esto guiará la función del rol que desempeñaran en sus actividades. Como guía para el proceso de la evidencia digital se encuentra la norma ISO/EIC 27037:2012 "Guía para la Identificación, recolección, adquisición y preservación de evidencia digital."

La norma proporciona orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de la evidencia digital. Entre otros fines, pretende ayudar a las organizaciones en sus procedimientos de tratamiento de circunstancias excepcionales que involucran datos gestionados en ellas de forma que se pueda facilitar el intercambio de evidencias digitales potenciales y su presentación como prueba en juicio o arbitraje.

Define dos roles de especialistas en la gestión de las evidencias electrónicas: (27037, ISO/IEC, 2012)

DIGITAL EVIDENCE FIRST RESPONDERS (DEFR)[33]

Experto en primera intervención de evidencias electrónicas, Individuo autorizado, entrenado y calificado para actuar en la escena del hecho con capacidad de recolección y adquisición de evidencia digital.

DIGITAL EVIDENCE SPECIALISTS (DES)[34]

Experto en gestión de evidencias electrónicas, posee las mismas capacidades que un DEFR sumado a capacidades de Análisis.

Los DEFR y DES deberán documentar todas sus acciones, las que se regirán por los siguientes principios:

- Minimizar el manejo de la evidencia digital original
- Documentar cualquier acción que implique un cambio irreversible
- Adherirse a las regulaciones y leyes locales
- No extralimitarse en sus funciones

Dentro de los procedimientos que deberán realizar están:

[33] Equipo de Respuesta de Evidencia Digital
[34] Especialista de Evidencia Digital

1. **Identificación:** Es el reconocimiento de donde se halla la evidencia digital, sea esta física o lógica.
2. **Recolección:** Frecuentemente el DEFR deberá tomar la decisión de recolectar la evidencia y trasladarla al laboratorio para su adquisición, en función del tiempo y los recursos informáticos disponibles en la escena del hecho, sustentado por el mandato judicial. En cualquier caso, deberá documentar su decisión fundamentándola y estará preparado para defenderla en una corte.
3. **Adquisición:** Es el proceso de copia forense que el DEFR o DES realizará obteniendo una copia binaria exacta del contenido lógico o físico de los objetos involucrados en la investigación. La norma establece que la copia debe ser verificada con un "método de verificación probado" evitando expresarse sobre la utilización de algún Hash[35] en particular.
4. **Preservación:** La evidencia digital deberá ser preservada para asegurar su integridad durante todo el proceso. Esto incluye el embalaje, que en algunos casos tiene requerimientos especiales.

LOS PROCEDIMIENTOS DE LA EVIDENCIA DIGITAL

Los procedimientos de recolección y análisis de evidencia digital generalmente se encuentran sustentados en herramientas de software, procedimientos internacionalmente aceptados y experiencia del investigador. Mientras mayor sea la capacidad de las herramientas para identificar, recolectar, asegurar y analizar la evidencia en medios electrónicos, mejores resultados y controles se pueden mantener, dado que la intervención humana en el proceso ha sido mínima. Sin embargo, no podemos perder de vista que el software no es infalible y requiere un proceso de depuración y pruebas que exige una revisión por parte de la comunidad científica, identificación y valoración de sus errores, resultados de uso en casos anteriores, entre otras, que permitan aumentar la confiabilidad y la respetabilidad de los resultados.

Todas las técnicas utilizadas para la recogida y análisis de evidencias digitales, deben estar respaldadas por una buena metodología científica y documentadas en un protocolo de actuación, que recoja tanto los aspectos técnicos de la informática como los aspectos legales que se derivan de su peculiaridad forense. Para asegurar que las pruebas digitales son recogidas, preservadas, examinadas o transferidas de manera que se salvaguarde su integridad, fiabilidad, y precisión, todas las instituciones

[35] Función Hash, también llamadas funciones picadillo, funciones resumen o funciones de digest.

forenses, cuya función esté relacionada con dichas pruebas digitales, deberán establecer y mantener un sistema de calidad efectivo, sin olvidar tampoco la formación del personal. (RFC 3227)

HERRAMIENTAS PARA LOS PROCEDIMIENTOS EN LA RECOLECCIÓN DE LA EVIDENCIA

Hoy en día el acceso a herramientas informáticas que permiten la investigación de delitos con la menor intervención posible, permiten garantizar la integridad de las evidencias recolectadas.

Una de las herramientas, posiblemente la más utilizada en la actualidad para la informática forense es EnCase, esta herramienta tiene entre sus características lo siguiente:

- Copiando comprimido de discos fuentes
- Búsqueda y análisis de múltiples partes de archivos adquiridos
- Diferente capacidad de almacenamiento
- Varios campos de ordenamiento, incluyendo estampillas de tiempo
- Análisis compuesto del documento
- Búsqueda automática y análisis de archivos de tipo ZIP y attachments de e-mail
- Firmas de archivos, identificación y análisis
- Análisis electrónico del rastro de intervención
- Soporte de múltiples sistemas de archivo
- Vista de archivos y otros datos en el espacio unallocated
- Integración de reportes
- Visualizador integrado de imágenes con galería

En Case es una herramienta de paga, es decir es necesario comprar una licencia para poder disponer de su potencia, sin embargo existen otras herramientas y procedimientos que pueden ser utilizadas para la recolección y procesamiento de la evidencia digital.

Es importante considerar que la constante evolución de las aplicaciones y plataformas informáticas impactan directamente en las herramientas por lo que las herramientas que se listan a continuación a modo de ejemplo está construido en base a las aplicaciones actuales y necesariamente evolucionará con el tiempo.

Las herramientas usadas en el análisis forense las podemos dividir de acuerdo a su función, las cuales son: (Listado de Herramientas Forenses)

HERRAMIENTAS DE ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA

Set de utilidades que permite la adquisición de la Memoria de Acceso Aleatorio (RAM[36]) para posteriormente hacer un análisis con ella. En este conjunto de herramientas podemos encontrar:

- **pd Proccess Dumper**: Convierte un proceso de la memoria a fichero
- **FTK Imager (Forensic Tool Kit Imager):** Permite entre otras cosas adquirir la memoria
- **DumpIt**: Realiza volcados de memoria a fichero
- **Responder CE:** Captura la memoria y permite analizarla
- **Volatility**: Analiza procesos y extrae información útil para el analista. Permite el análisis forense de RAM
- **RedLine**: Captura la memoria y permite analizarla. Dispone de entorno gráfico
- **Memorize:** Captura la memoria RAM (Windows y OSX)

HERRAMIENTAS DE MONTAJE DE DISCOS

Utilidades para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla. En este conjunto de herramientas podemos encontrar:

- **ImDisk**: Controlador de disco virtual
- **OSFMount**: Permite montar imágenes de discos locales en Windows asignando una letra de unidad
- **raw2vmdk**: Utilidad en java que permite convertir raw/dd a .vmdk
- **vhdtool**: Convertidor de formato raw/dd a .vhd permitiendo el montaje desde el administrador de discos de Windows
- **LiveView**: Utilidad en java que crea una máquina virtual de VMware partiendo de una imagen de disco
- **MountImagePro**: Permite montar imágenes de discos locales en Windows asignando una letra de unidad

CARVING[37] Y HERRAMIENTAS DE DISCO

Recuperación de datos perdidos, borrados, búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes y/o vídeos. Recuperación de particiones y tratamiento de estructuras de discos. En este conjunto de herramientas podemos encontrar:

[36] RAM acrónimo de Random Access Memory (Memoria de Acceso Aleatorio)
[37] Carving, es el proceso de montaje de archivos de computadoras a partir de fragmentos, en ausencia de los metadatos del sistema de archivos.

- **Foremost** es una herramienta forense para recuperar archivos basándose en sus cabeceras, y estructuras internas, en al área forense se le llama File carving o data carving

UTILIDADES PARA EL SISTEMA DE FICHEROS

Conjunto de herramientas para el análisis de datos y ficheros esenciales en la búsqueda de un incidente. En este conjunto de herramientas podemos encontrar:

- **AnalyzeMFT**: Utilidad en python que permite extraer la MFT[38]
- **MFT Extractor**: Otra utilidad para la extracción de la MFT
- **INDXParse**: Herramienta para los índices y fichero
- **MFT Tools**: (mft2csv, LogFileParser, etc.) Conjunto de utilidades para el acceso a la MFT
- **MFT_Parser**: Extrae y analiza la MFT
- **Prefetch Parser**: Extrae y analiza el directorio prefetch
- **Winprefectchview**: Extrae y analiza el directorio prefetch
- **Fileassassin**: Desbloquea ficheros bloqueados por los programas

HERRAMIENTAS DE ANÁLISIS DE MALWARE

- **PDFStreamDumper:** Esta es una herramienta gratuita para el análisis de PDFs maliciosos
- **SWF Mastah**: Programa en Python que extrae stream SWF de ficheros PDF
- **Proccess explorer**: Muestra información de los procesos
- **Captura BAT**: Permite la monitorización de la actividad del sistema o de un ejecutable
- **Regshot**: Crea snapshots del registro pudiendo comparar los cambios entre ellos
- **Bintext**: Extrae el formato ASCII de un ejecutable o fichero
- **LordPE**: Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados
- **Firebug**: Análisis de aplicaciones web
- **IDA Pro**: Depurador de aplicaciones
- **OllyDbg**: Desensamblador y depurador de aplicaciones o procesos

[38] Tabla Maestra de Archivos (MFT). Hay al menos una entrada en la MFT para cada archivo en un volumen NTFS, incluyendo la MFT sí mismo.

- **Jsunpack-n**: Emula la funcionalidad del navegador al visitar una URL. Su propósito es la detección de exploits
- **OfficeMalScanner**: Es una herramienta forense cuyo objeto es buscar programas o ficheros maliciosos en Office
- **Radare**: Framework para el uso de ingeniería inversa
- **FileInsight**: Framework para el uso de ingeniería inversa
- **Volatility**: Framework con los plugins malfind2 y apihooks
- **shellcode2exe**: Conversor de shellcodes en binarios

FRAMEWORKS

Conjunto estandarizado de conceptos, prácticas y criterios en base al análisis forense de un caso.

- **PTK**: Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado
- **Log2timeline**: Es un marco para la creación automática de una súper línea de tiempo
- **Plaso**: Evolución de Log2timeline. Framework para la creación automática de una súper línea de tiempo
- **OSForensics**: Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado
- **DFF**: Framework con entorno gráfico para el análisis
- **Autopsy**: Herramienta libre que existe para el análisis de evidencia digital

ANÁLISIS DEL REGISTRO DE WINDOWS

Permite obtener datos del registro como usuarios, permisos, ficheros ejecutados, información del sistema, direcciones IP, información de aplicaciones.

- **RegRipper**: Es una aplicación para la extracción, la correlación, y mostrar la información del registro
- **WRR**: Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro
- **Shellbag Forensics**: Análisis de los shellbag de Windows
- **Registry Decoder**: Extrae y realiza correlación de datos del registro aun estando encendida la máquina

HERRAMIENTAS DE RED

Todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

- **WireShark**: Herramienta para la captura y análisis de paquetes de red
- **NetworkMiner**: Herramienta forense para el descubrimiento de información de red
- **Netwitness Investigator**: Herramienta forense
- **Network Appliance Forensic Toolkit**: Conjunto de utilidades para la adquisición y análisis de la red
- **Xplico:** Extrae todo el contenido de datos de red (archivo pcap o adquisición en tiempo real). Es capaz de extraer todos los correos electrónicos que llevan los protocolos POP y SMTP, y todo el contenido realizado por el protocolo HTTP
- **Snort**: Detector de intrusos. Permite la captura de paquetes y su análisis
- **Splunk**: Es el motor para los datos y logs que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube
- **AlientVault**: Al igual que Splunk recolecta los datos y logs aplicándoles una capa de inteligencia para la detección de anomalías, intrusiones o fallos en la política de seguridad.

RECUPERACIÓN DE CONTRASEÑAS

Recuperación de contraseñas en Windows, por fuerza bruta, en formularios, en navegadores.

- **Ntpwedit**: Es un editor de contraseña para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory
- **Ntpasswd**: Es un editor de contraseña para los sistemas basados en Windows, permite iniciar la utilidad desde un CD-LIVE
- **pwdump7**: Vuelca los hash. Se ejecuta mediante la extracción de los binarios SAM
- **SAMInside / OphCrack / L0phtcrack**: Hacen un volcado de los hash. Incluyen diccionarios para ataques por fuerza bruta

DISPOSITIVOS MÓVILES

Utilidades y herramientas para la recuperación de datos y análisis forense de dispositivos móviles.

Para iPhone

- **iPhoneBrowser**: Accede al sistema de ficheros del iphone desde entorno gráfico
- **iPhone Analyzer**: Explora la estructura de archivos interna del iphone
- **iPhoneBackupExtractor**: Extrae ficheros de una copia de seguridad realizada anteriormente
- **iPhone Backup Browser**: Extrae ficheros de una copia de seguridad realizada anteriormente
- **iPhone-Dataprotection**: Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad
- **iPBA2**: Accede al sistema de ficheros del iphone desde entorno gráfico
- **sPyphone**: Explora la estructura de archivos interna

Para BlackBerry

- **Blackberry Desktop Manager:** Software de gestión de datos y backups
- **Phoneminer**: Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad
- **Blackberry Backup Extractor**: Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad
- **MagicBerry**: Puede leer, convertir y extraer la base de datos IPD

Para Android

- **android-locdump**: Permite obtener la geolocalización
- **androguard**: Permite obtener, modificar y desensamblar formatos DEX/ODEX/APK/AXML/ARSC
- **Viaforensics**: Framework de utilidades para el análisis forense
- **Osaf**: Framework de utilidades para el análisis forense

LIVE CD FORENSE

Es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí su nombre), que puede ejecutarse directamente en una computadora. Normalmente, un Live CD viene acompañado de un conjunto de aplicaciones, algunos Live CD incluyen una herramienta que permite instalarlos en el disco duro. Otra característica es que por lo general no se efectúan cambios en el ordenador utilizado.

Para usar un Live CD es necesario obtener uno (muchos de ellos distribuyen libremente una imagen ISO que puede bajarse de Internet y grabarse en disco) y configurar la computadora para que arranque desde la unidad lectora, reiniciando luego la computadora con el disco en la lectora, con lo que el Live CD se iniciará automáticamente.

Un Live CD Forense, es un CD con las herramientas de Respuesta ante Incidentes y Análisis Forense compiladas de forma que no realicen modificaciones en el sistema. En un análisis forense una vez confirmado el incidente, se realiza el análisis post-mortem. Los Forensic Live CDs son ampliamente utilizados durante las investigaciones forenses informáticos. Estos CD son aplicaciones encapsuladas en un Sistema Operativo anfitrión que por lo general se carga de dos posibles formas, uno, instalándose directamente en el equipo como un Sistema Operativo más. La segunda opción es la que le da su nombre, ya que esta opción no requiere su instalación, se inicia desde un CD o una memoria USB desde la secuencia de arranque del equipo. Estos Live CD contienen aplicaciones que permiten realizar análisis al equipo en estudio, algunas de las distribuciones que se pueden encontrar son:

- Helix
- CAINE
- ForLEX
- EnCase
- DEFT Linux
- Kali Linux
- Phlak

En contraste con el análisis forense tradicional, en la Informática Forense las investigaciones deben llevarse a cabo en prácticamente cualquier situación o dispositivos físico, no sólo en un entorno controlado de laboratorio. Esto nos lleva a considerar las acciones a tomar en un entorno de investigación, en donde debemos ser cuidadosos de los procesos y determinar efectivamente la cadena de custodia para evitar la contaminación de la escena de un crimen, una vez recopilada toda la evidencia y siguiendo todos los procedimientos adecuados para garantizar la integridad de los datos recabados entramos a un entorno de trabajo, el Análisis Forense debe realizarse en una red aislada, con equipos preparados para tal fin en donde aplicamos los procesos de búsqueda específica por medio de las herramientas adecuadas según la investigación y fin de la evidencia.

SITUACIÓN ACTUAL DE LA INFORMATICA FORENSE EN EL SALVADOR

En la actualidad el acceso a nuevas aplicaciones, fuentes de información y recursos han ampliado la cantidad de individuos que buscan hacer algún daño sustancial por medio de equipos informáticos, este desarrollo tecnológico es usado por muchos para cometer delitos como: Clonación de tarjetas,

piratería, fraude, extorsión, difamación, acoso, pornografía infantil, y un largo etc. algunos de estos delitos no tipificados en la legislación salvadoreña, pero lo que impide el accionar de las instituciones judiciales es que las leyes actuales no incluyen las herramientas para llevarlos a cabo, como es el caso de la informática y el uso de dispositivos electrónicos.

La Policía Nacional Civil se ve limitada en los procesos de investigación de delitos informáticos, porque no cuenta con suficiente personal capacitado en el uso de herramientas informáticas y metodologías de recolección de evidencia digital.

La Fiscalía General de la República y la Corte Suprema de Justicia presentan debilidades, ya que no tienen leyes en las cuales se puedan amparar para juzgar a individuos detenidos y procesados por cometer delitos informáticos.

Las instituciones encargadas de preparar profesionales en informática no han abordado el tema de la informática forense, esto debido a la falta de personal capacitado para impartir los conocimientos sobre dicha temática.

Los casos que se mencionan a continuación son un fiel ejemplo que en El Salvador los delitos informáticos han dejado de ser un mito y se han vuelto una realidad.

CASO #1

El periódico digital lapagina.com (http://www.lapagina.com.sv) presento un reportaje titulado:
POLICÍA Y FISCALÍA ENFRENTAN PROFUNDAS DEBILIDADES ANTE "CIBER DELITOS"
(http://www.lapagina.com.sv/ampliar.php?id=58659)
Este reportaje habla sobre la explosión de las redes sociales y el uso de internet en el país, y como esto ha abierto la puerta a numerosos delitos que van desde pornografía infantil hasta extorsiones, robos de información confidencial e identidad y muestras de violencia extrema. Delitos que prosperan en un marco jurídico y una investigación policial con grandes debilidades.

Un "fenómeno" nuevo

Al respecto, en El Salvador, los investigadores de la Policía Nacional Civil (PNC) coinciden que parte del gran problema es la poca conciencia de nuestra sociedad en el uso correcto de internet.
"Se supone que sabemos usar internet pero no somos conscientes de los riesgos que eso tiene, no sabemos que al pegarnos a la web yo dejo una IP como una huella digital y que si yo no sigo normas de seguridad me pongo en riesgo", dijo el jefe de la unidad de Delitos Especializados de la PNC, Romeo Américo Pereira. Quien reconfirmó además que en nuestro país "la web se utiliza para violencia, para hackear páginas y para robo de identidad", entre otros delitos.

Un proceso muy complejo

De acuerdo a la PNC, la investigación inicia cuando la persona pone una denuncia a la Fiscalía General de la República (FGR) sobre una página, perfil o muro de una red social o página web que presenten mensajes textuales o/y visuales de violencia o que podrían tipificarse como delito, como los ya mencionados. Luego la fiscalía tiene que direccionar a la PNC para que ésta comience a indagar quien le brinda servicio de internet a la persona que puso la denuncia.

A partir de eso la PNC debe indagar con el proveedor cuál es el IP del equipo de donde se subieron esos archivos (pornografía, violencia, amenaza, acoso, etc.), "pero para llegar a donde deliberadamente subieron esos archivos o enviaron esos mensajes, que puede ser en cualquier parte del mundo, antes hay que llegar al proveedor de servicio", explicó Pereira, de la Unidad de Delitos Especializados.

"En el escenario más fácil usted debe pedirle al proveedor algunos datos de la IP, luego pedirle a Facebook a quién está asignada determinada cuenta, qué IP se pegó o respaldó la conexión a esa cuenta en el día, hora, minutos y segundos exactos", sostiene.

Luego la PNC esperará la respuesta de la red social que también debe hacer una indagación para darle a las autoridades la IP que respaldó la conexión, y si es en el país (en este caso El Salvador) se podría proceder a un allanamiento y hasta confiscar el equipo y realizarle un análisis informático forense.

Limitantes jurídicas

Una de las mayores limitaciones que tiene la policía para actuar son los vacíos de Ley, ya que ni el Código Procesal Penal, ni el Código Penal contemplan específicamente este tipo de delitos por medios electrónicos.

"La parte más delicada es la jurídica porque El Salvador pese a los esfuerzos que la Policía ha hecho en querer incorporar desde el 2000 a nuestra legislación algunos artículos y especificaciones y aclaraciones que a nuestro juicio ayudarían para una mejor investigación y abordaje del delito, no hay una buena base jurídica", sostiene el representante de la unidad de delitos especializados de la PNC.

La ley no obliga a las empresas servidoras de Internet a guardar un respaldo del registro de IP de todos los que se van conectando en el servicio web a los servidores de ellos, añade.

Y la otra limitante -señalan- es que la FGR no tiene una unidad específica para investigar delitos informáticos, por lo que sólo son procesados como delitos los ya tipificados, pero no tienen que ver específicamente con medios informáticos. (Periódico La Página)

CASO #2

ANALIZAN PROPUESTA DE LEY CONTRA DELITOS CIBERNÉTICOS

Los delitos en donde se ven involucrados dispositivos electrónicos ya no pueden seguir ignorándose, es por ello que se deben **analizar propuestas de ley contra los delitos cibernéticos**, tal como lo propone Transparencia Activa en el siguiente enlace.
http://www.transparenciaactiva.gob.sv/analizan-propuesta-de-ley-contra-delitos-ciberneticos/

El ministro de Seguridad, David Munguía Payés, reveló a Transparencia Activa que presentaron a Casa Presidencial una propuesta de ley contra el delito cibernético para su análisis y posterior envío a la Asamblea Legislativa.
"Hay mucha gente que se aprovecha del anonimato. Esos delitos provocativos decantan en violaciones, agresiones o acosos; también desprestigian a personas con calumnias, desde el anonimato hacen fraudes a bancos, instituciones financieras, etc.", explicó el funcionario.
La ley contra delitos cibernéticos o informáticos daría herramientas legales para procesar a quienes sin escrúpulos usan internet y las redes sociales para dañar a terceros. De momento, dichos delitos en la mayoría de los casos quedan impunes por la falta de una legislación especial.
En El Salvador, se reportan casos de mujeres que denuncian acoso a través de redes sociales como Facebook. Fátima Ortiz, directora ejecutiva del Consejo contra la Trata de Personas, revela que "muchos crean cuentas exprés para buscar víctimas para prostitución infantil, por ejemplo".
"Es de mucha importancia que el país cuente con una ley para castigar delitos informáticos, ya que estos son muy comunes, porque estos ciberdelincuentes están enterados que no hay nada y nadie los castigue ni les prohíba sus acciones", opina Erika Candray. (Transparencia Activa)

CASO #3

EL SALVADOR NECESITA QUE SE APRUEBEN LEYES EFICIENTES

Estos análisis surgen de la necesidad de que **El Salvador necesita que se aprueben leyes eficientes,** así lo expresa el movimiento Medio Lleno en el siguiente enlace.
http://mediolleno.com.sv/editorial/el-salvador-necesita-que-se-aprueben-leyes-eficientes
Los diputados iniciaron el estudio de una ley que permita la penalización de delitos cibernéticos, pero aún hay muchos puntos que requieren aclararse y tratamiento para que la normativa sea viable.

En El Salvador hay un sinfín de leyes aprobadas por el Órgano Legislativo, las cuales deberían estar en función de la efectividad, evolución y desarrollo de las prácticas democráticas, políticas y económicas del país. Los diputados han dado el aval a leyes de gran importancia para la sociedad, como la Ley de Acceso a la Información Pública, la Ley del Impuesto Sobre la Renta, la del IVA, el Código Electoral, la Constitución de la República, entre otras más o menos importantes que las mencionadas y que son vitales para el funcionamiento del país.

No obstante, también han aprobado normativas que son pocos o nada viables porque carecen del conocimiento de los ciudadanos o estos desconocen en qué les pueden beneficiar y cómo pueden hacer para denunciar las violaciones a dichas leyes. Tal es el caso de normativas como la Ley Especial contra el Tabaco, la Ley Orgánica de Administración Financiera del Estado, Ley de los Servicios Privados de Seguridad, Ley de la Superintendencia de Obligaciones Mercantiles y la que se indicó en el inicio de este texto: Ley Especial de Protección contra los Delitos informáticos. (Movimiento Medio Lleno)

CASO #4

Ante este tipo de hechos y análisis de propuestas hay personas que proponen soluciones basadas en las leyes existentes, tal es el caso de la **PIEZA REFORMA CÓDIGO PENAL DELITOS INFORMÁTICOS,** dicha pieza de correspondencia que fue ingresada a la Asamblea Legislativa por el partido Cambio Democrático puede ser leída desde el siguiente enlace:

http://www.cambiodemocraticosv.org/documentos/PiezaReformaCodigoPenalDelitosInformaticosVersion3.pdf

La problemática antes mencionada hace surgir la necesidad de aplicar la informática forense, como medio que ayude a esclarecer hechos delictivos informáticos.

INSTITUCIONES INVOLUCRADAS EN EL ESCLARECIMIENTO DE DELITOS INFORMÁTICOS.

Surge la inquietud de conocer cómo, cuándo, quienes y donde se aplica la informática forense; ya que en el país se tiene un alto índice de delitos informáticos entre los que están: clonación de tarjetas de crédito, pornografía infantil, robo de información confidencial, piratería de software, robo de base de datos, robo de identidad, financiamiento del crimen, es por ello que se hace necesario realizar el estudio de la situación actual de la informática forense como medio de recolección y análisis de evidencia digital que ayude al esclarecimiento de estos delitos.

Con el crecimiento de delitos informáticos que se han dado en El Salvador, se hace más ardua la tarea para las instituciones judiciales y policiales, las cuales trabajan en conjunto con la finalidad de lograr el esclarecimiento de dichos delitos, se hace necesario por parte de estas instituciones la utilización de la tecnología informática para revolver este tipo de delitos, sin embargo, en nuestro país aún no se cuenta con una legislación que ampare el uso de esta tecnología como en otros países donde si está establecido en el código penal, leyes sobre la legalidad de la aplicación de la tecnología informática en procesos judiciales.

En todo proceso de investigación y penalización de delitos, deben existir instituciones involucradas en la recolección, manipulación, interpretación y presentación de evidencias.

En la resolución de un caso delictivo, La Fiscalía General de la República es la encargada de la parte acusatoria y de la búsqueda de pruebas incriminatorias, La Policía Nacional Civil forma parte en estos procesos judiciales como el ente encargado de guardar la cadena de custodia, La Corte Suprema de Justicia se encarga de verificar el cumplimiento de las leyes y dar el veredicto final en la resolución de un caso por medio del juez, el rol específico de cada uno de estos actores es el siguiente:

LA FISCALÍA GENERAL DE LA REPÚBLICA (FGR)

La Fiscalía General es el Órgano del Estado, integrante del Ministerio Público, el cual tiene sus fundamentos en la Constitución de la República, establecidos en el artículo 193. Siendo este artículo de la Constitución el fundamento de la Fiscalía General, ésta es la institución determinada por el estado para actuar con una función requirente "acusar", se l e ha dado a ésta una facultad acusatoria donde existe un derecho de perseguir una actuación que constituya un hecho delictivo, donde esta institución buscará la verdad material y real de los hechos, debiendo dirigir la investigación del delito junto con la policía teniendo presente un conjunto de principios que se deben tener en cuenta en todo acto que esta institución realiza.

Dentro de sus funciones están:

- Defender los Intereses del Estado y de la Sociedad.
- Dirigir la investigación del delito con la colaboración de la Policía Nacional Civil, y en particular de los hechos criminales que han de someterse a la jurisdicción penal.

LA POLICÍA NACIONAL CIVIL

Es la encargada ante todo de evitar que la escena de un crimen sea contaminada por personas sin autorización, trabaja en conjunto con la Fiscalía en la investigación del delito, pero no puede tomar decisiones por ella misma, ya que únicamente se dedica a seguir las órdenes indicadas por la Fiscalía. En un caso de homicidio, la policía copia el acta del reconocimiento médico – forense, llevándolo a las oficinas de la institución, siendo este el primer paso para comenzar a buscar posibles sospechosos.

Los detectives policiales investigan a los posibles móviles, descubren a los criminales y tienen autoridad para detener a los sospechosos si las investigaciones indican que hay responsables.

La forma de proceder de esta institución ante delitos informáticos es similar a la de otros delitos, ya que cuando en la escena del crimen está involucrado un dispositivo electrónico computacional como

posible móvil, se acordona el lugar impidiendo cualquier tipo de intrusión, esta forma de accionar permite que la obtención de evidencias digitales sea recolectada de forma correcta haciendo uso de la aplicación de la informática forense.

CORTE SUPREMA DE JUSTICIA

Esta institución es la que provee los jueces para los tribunales de justicia en donde se vaya a resolver un determinado hecho delictivo. El juez es un ente independiente de las partes procesales pues es la autoridad competente que decidirá la situación jurídica del imputado, se debe basar en el principio de independencia e imparcialidad, pues el dirigirá el proceso, valorará los elementos de prueba y es el que decidirá si el imputado es inocente o culpable.

INSTITUCIONES DE EDUCACION SUPERIOR

El desarrollo de modelos de formación y la falta de preparación académica en la gestión de profesionales en la seguridad de la información hace que una de las ciencias; como es la ciencia de la informática forense este por debajo de los niveles de preparación profesional tanto a nivel práctico y teórico. Dando como resultado una ciencia incapaz de sobresalir ante los temas del delito informático que envuelven a la sociedad salvadoreña, ya que debido al alto índice de delitos informáticos en la actualidad se debe dar una mejor respuesta a los retos de seguridad pero para contrarrestar estos problemas se debe gestionar al capital humano por medio de las capacitaciones y un buen currículo que abone todas las problemáticas actuales.

CAPÍTULO 3: UNA INTRODUCCIÓN A LA CIENCIA FORENSE DIGITAL Y LOS TIPOS DE INVESTIGACIÓN DE LA INFORMÁTICA FORENSE

INTRODUCCIÓN

La cantidad de información digital almacenada en dispositivos electrónicos es cada vez mayor y existe una diversidad de equipos electrónicos que cumplen con esta función, por ejemplo: (Stephenson, 2014) computadoras de escritorios, laptops, Smartphone, PDA (asistente digital personal), discos duros externos y un sinfín de equipos electrónicos que están en el mercado globalizado. La cantidad de información digital creada o replicada en el 2012 que corresponde a 1 millón de terabytes será duplicada a 1 billón de terabytes en 2020. Todos estos datos se componen de correos electrónicos, videos, música, fotografías, videos de vigilancia, transacciones financieras, llamadas telefónicas y actividades de sistemas computacionales.[39]

[39] Gants, J., & Reinsel, D. (2012, December). Big data, bigger digital shadows, and biggest growth in the far east. Consultado en http://www.emc.com/leadership/digital-universe/2014iview/index.htm

Hoy en día los delitos informáticos están incrementando a niveles que están siendo difíciles de contrarrestar ya que las técnicas que se están utilizando están al mismo margen de las nuevas tendencias tecnológicas. Como resultado a esta problemática la Ciencia Forense Digital es la encargada de investigar los dispositivos digitales en los cuales se pueda encontrar una evidencia digital y por medio de ella esclarecer algún hecho en particular, ya sea civil, criminal u organizacional. La Forensia Digital es una disciplina que aplica los conceptos, estrategias y procedimientos informáticos especializados, con el fin de apoyar el esclarecimiento de los hechos de eventos que se pueden catalogar como incidentes, fraudes o usos indebidos en el contexto organizacional, personal o judicial.

UN POCO DE HISTORIA

La Forensia Digital emergió como una disciplina científica inicialmente desarrollada para La Aplicación de la Ley Federal de los Estados Unidos a mediados de 1980. El desarrollo de esta disciplina fue cambiando debido a la incursión de las computadoras personales (PC) dentro de las organizaciones y donde se fueron generando los primeros incidentes que al final se irían catalogando como delitos informáticos. Como parte de su evolución fue el hecho de que ya no solo estaba en el ámbito de una computadora personal sino que envolvía a las telecomunicaciones, seguridad, networking, aplicación de ley y el sistema criminal de justicia. Es así como la Forensia Digital para algunos autores se ha transformado en un estado de transición entre el arte a la ciencia en el cual se desarrollan altas destrezas técnicas multidisciplinarias para la resolución de casos. Algunos conceptos de Forensia Digital la definen como: "Cualquier información de valor probatorio que se almacena o trasmite en forma binaria" una definición un tanto genérica y con una corta cobertura.

Autores como Barbin D. and Patzakis J., la definen como: "Informática Forense es la colección, preservación, análisis y presentación de la evidencia digital relacionada ante una corte".[40]

Otro autor como Mark Pollit la define como: "El análisis forense digital es la aplicación de la ciencia y la ingeniería para un problema legal de la evidencia digital. Se trata de una síntesis de la ciencia y la ley".[41]

El US- CERT define Forensia Digital como: "La disciplina que combina elementos de derecho y ciencias digitales para recopilar y analizar los datos procedentes de los sistemas digitales, redes, comunicaciones inalámbricas y dispositivos de almacenamiento en una forma que sea admisible como prueba es un tribunal de justicia"

[40] Barbin D. and Patzakis J., article titled "Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program."
[41] Special Agent Mark Pollitt, FBI –quoted in Forensic Computing: A Practitioner's Guide, (Sammes & Jenkinson)

Todas las definiciones anteriores hacen que la Informática Forense o Forensia Digital se involucre tanto la parte de la ciencia como aspectos de la ley transformándola en una herramienta integral para la investigación de la evidencia digital la cual es obtenida a través de la aplicación de la investigación digital y técnicas de análisis a dispositivos digitales y asociada a dispositivos periféricos en los cuales los datos están preservados en forma electrónica.

PRINCIPIOS DE LA EVIDENCIA DIGITAL

La evidencia digital se puede requerir en una serie de escenarios distintos, cada uno de los cuales tiene un equilibrio diferente por ejemplo; la calidad de la evidencia, oportunidad de análisis, restauración del servicio y el costo de la recolección de la evidencia digital. Por lo tanto, se les exige a las organizaciones a tener un proceso de priorización que identifica las necesidades y balances de la calidad de la evidencia, su puntualidad y el servicio de restauración. Un proceso de priorización implica llevar a cabo una evaluación del material disponible para determinar el posible valor probatorio y el orden en que se debe recolectar la evidencia digital potencial, adquirido o conservado. La priorización se lleva a cabo para minimizar el riesgo de la evidencia digital potencial de ser dañada y maximizar el valor probatorio de la evidencia digital potencial recolectada.

En la mayoría de las jurisdicciones y organizaciones, la evidencia digital se rige por tres principios fundamentales: la pertinencia, confiabilidad y suficiencia. Estos tres principios son importantes para todas las investigaciones, no sólo para que la evidencia digital pueda ser admisible en una corte. La evidencia digital es relevante cuando se va a probar o refutar un elemento del caso particular que se investiga. La definición detallada de "confiable" varía entre las jurisdicciones, el significado general del principio, "es que se pretende garantizar la evidencia digital". No siempre es necesario recolectar todos los datos o realizar una copia completa de la evidencia digital. En muchas jurisdicciones, el concepto de suficiencia significa que se necesita recoger la evidencia digital potencial para permitir que los elementos de la materia puedan ser adecuadamente examinados o investigados. La comprensión de este concepto es importante para priorizar el esfuerzo adecuadamente cuando el tiempo o el costo es una preocupación.

Los principios establecidos para la evidencia digital, de acuerdo a la norma ISO/IEC 27037:2012, son definidos de la siguiente manera:

- **RELEVANCIA:** Debería ser posible intentar demostrar que el material adquirido es relevante para la investigación - es decir, que contiene información de valor para ayudar a la investigación del incidente en particular y que hay una buena razón por el cual se ha adquirido.

A través de la auditoría y la justificación, se debe ser capaz de describir los procedimientos utilizados y explicar cómo se tomó la decisión de adquirir cada prueba.

- **FIABILIDAD:** Todos los procesos utilizados en el manejo de la evidencia digital potencial debe ser auditable y reproducible, los resultados de la aplicación de tales procesos deben ser reproducibles.
- **SUFICIENCIA:** Se debería tener en cuenta que la evidencia se debe recopilar de una manera suficiente, para poder permitir llevar a cabo una investigación adecuada. A través de la auditoría y la justificación dar una indicación de la cantidad total de evidencia recolectada, del porque se consideró y los procedimientos utilizados para decidir cuánto y qué evidencia a adquirir.

Además la Association of Chief Police Officers (ACPO) del Reino Unido ha definido Guías de Buenas Prácticas para la Evidencia Electrónica Basada en Computadoras, estos principios se han aceptado a nivel mundial para la Forensia Digital, estos principios son los siguientes: (Andy Jones & Craig Valli, 2009)

1. **Principio 1:** Ninguna acción tomada por las fuerzas del orden o de sus agentes deberá cambiar los datos almacenados de un dispositivo digital o medio de almacenamiento que posteriormente pueden ser invocados ante los tribunales.
2. **Principio 2:** En los casos en que una persona considere necesario acceder a los datos originales almacenados en un dispositivo digital o en medios de almacenamiento, esa persona deberá ser competente para hacerlo y ser capaz de dar pruebas que aclaren la importancia y las implicaciones de sus acciones.
3. **Principio 3:** Una pista de auditoría u otro registro de todos los procesos que se aplican a las pruebas electrónicas por computadora deberán ser creados y preservados. Una tercera parte independiente debe ser capaz de examinar esos mismos procesos y lograr el mismo resultado.
4. **Principio 4:** La persona a cargo de la investigación (el oficial de caso) tiene la responsabilidad general de garantizar que la ley y estos principios se respetan.

Con el fin de cumplir con los principios de la evidencia digital, siempre que sea posible, una imagen deberá ser realizada a partir del dispositivo origen, como también copias de archivos parciales o selectivos, serán siempre una alternativa en las circunstancias en las que se encuentre el investigador, así como el cuidado que deberá tener el investigador para asegurar que todas las pruebas pertinentes adopten el mismo enfoque, protegiendo la evidencia digital de la contaminación y su destrucción preservando la cadena de custodia. Cabe recordar que cualquier fallo que se de en los procedimientos de la recolección de la evidencia digital esta podría ser excluida o limitada por algún tribunal. Esta

adopción de normas estará regida en ambientes organizacionales, civiles y judiciales manteniendo estos principios igualmente confiables y que nunca deberán ser olvidados por el investigador.

Los dispositivos de almacenamiento de dato en los cuales podrían haber fuentes de evidencia para la investigación forense se pueden mencionar los siguientes: CDs, DVDs, discos duros externos, routers, modems, floppy disks, memory sticks, USBs, cámaras digitales, dongles, wireless network cards y otros dispositivos de almacenamiento externo o dispositivos de procesamiento que podrían estar conectados por medio de cable, Bluetooth, WiFi o infrarrojo.

PROCEDIMIENTOS

Para la aplicación de los cuatro principios del tratamiento de la evidencia digital es esencial que en la investigación se desarrollen procedimientos orientados a satisfacer el buen manejo de la evidencia digital y que principalmente no se incumplan con estos principios, se deben considerar los procedimientos previos a la investigación, entre estos se deben tener en cuenta los siguientes: (Andy Jones & Craig Valli, 2009)

- **REGISTRAR TODAS LAS ACCIONES:** Todas las acciones llevadas a cabo en la investigación deben ser registrados. Esto proporciona un registro de todas las acciones llevadas a cabo en todas las etapas de las investigaciones y sirve para varios propósitos. Además de demostrar un récord que todas las acciones necesarias fueron tomadas y llevadas a cabo de la manera correcta, esto también se puede utilizar como una lista de verificación para los investigadores para asegurarse de que no han perdido nada. (Marcella, y otros, 2002)
- **GRABAR LA ESCENA:** Antes de que cualquiera de los equipos en la escena se altere, deben tomarse fotografías o videos de la escena, incluyendo todas las conexiones relacionadas con el equipo. Una vez que las fotografías iniciales de la escena se han hecho, puede ser necesario mover el equipo ligeramente para dar acceso a la parte trasera del equipo y sus conexiones. Si el equipo fotográfico o de vídeo no está disponible, se debe hacer un diagrama para registrar la información; Sin embargo, en estos días, esto debería ser la excepción. Esto volverá a formar parte de la prueba, sino que también proporcionará información vital si se hace necesario reconstruir el equipo en el laboratorio. No hay nada peor que la eliminación de un gran número de cables y dispositivos, almacenarlos y transportarlos, siguiendo los procedimientos adecuados, sólo para descubrir que no se pueden poner de nuevo juntos en la forma en que se configuró originalmente porque no se tiene la información necesaria.
- **GRABAR LA INFORMACIÓN EN PANTALLA:** Si el sistema está encendido, es importante registrar la información visible. Si todos los archivos están abiertos, deben ser guardados, preferiblemente a un dispositivo externo y grabar la acción.

- **CABLEADO Y SOCKETS ETIQUETADOS:** Una vez que las conexiones han sido fotografiadas, todos los cables deben estar etiquetados, ya que se separan, y debe quedar indicado que dispositivo fue removido de su socket. Esto ayuda a la reconstrucción del sistema si es necesario.
- **COMPROBACIÓN DE CONTRASEÑAS:** Durante el examen inicial de la escena y la actividad posterior de grabar y desmontar el sistema para transportarlo, el investigador siempre debe recordar que no es inusual que las personas graben contraseñas y las almacenen en las proximidades del dispositivo digital. Si se encuentra alguna contraseña, deben ser registradas para su uso posterior en el proceso.

Los RFC «Request For Comments» son documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer por ejemplo una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento, y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad.

Estos son los puntos más importantes relacionados con dicho proceso: (RFC 3227)

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

FASES DE UNA INVESTIGACIÓN FORENSE DIGITAL

Los procedimientos para el tratamiento de la evidencia digital se deben realizarse en cuatro diferentes etapas, sugeridas por la norma ISO/IEC/ 27037: (27037, ISO/IEC, 2012)

ETAPA 1 - IDENTIFICACION:

La evidencia digital se representa en forma física y lógica. La forma física incluye la representación de los datos dentro de un dispositivo tangible. La forma lógica de la evidencia digital se refiere a la representación virtual de datos dentro de un dispositivo.

El proceso de identificación consiste en la búsqueda del reconocimiento y documentación del dispositivo digital. El proceso de identificación debe reconocer los dispositivos de almacenamiento y de procesamiento digital que puedan contener evidencia digital correspondiente al incidente. Este proceso también incluye una actividad para dar prioridad a la recopilación de pruebas basada en su volatilidad. La volatilidad de los datos se debe identificar para asegurar el orden correcto de los procesos de recaudación y de adquisición para minimizar el daño a la evidencia digital y obtener la mejor evidencia. Además, el proceso debe identificar la posibilidad de pruebas digitales potencial ocultas. Los investigadores deben ser conscientes de que no todos los medios de almacenamiento digital pueden ser fácilmente identificados y localizados, por ejemplo el cloud computing, NAS y SAN, estas tecnologías son componentes virtuales para el proceso de identificación.

Los investigadores deberán proceder sistemáticamente a una búsqueda minuciosa para los artículos que pueden contener evidencia digital. Los diferentes tipos de dispositivos digitales que pueden contener evidencia digital pueden ser fácilmente pasados por alto (por ejemplo, debido a su tamaño pequeño), disfrazados o mezclados entre otro material irrelevante.

ETAPA 2 – RECOLECCIÓN:

Una vez identificados los dispositivos digitales que pueden contener evidencia digital potencial, los investigadores deben decidir si se recoge o adquiere durante el siguiente proceso. Hay una serie de factores de decisión para esto, la decisión debe basarse en las circunstancias.

La recolección es un proceso en el manejo de la evidencia digital donde los dispositivos que pueden contener evidencia digital potencial son removidos de su ubicación original a un laboratorio u otro entorno controlado para la posterior adquisición y análisis. Los artefactos que contengan evidencia digital potencial pueden estar en uno de dos estados: cuando el sistema está encendido o cuando el sistema está apagado. Se requieren diferentes enfoques y herramientas, dependiendo del estado del dispositivo. Procedimientos locales pueden aplicarse a los enfoques y las herramientas que se utilizan para el proceso de recolección.

Este proceso incluye la documentación de todo el enfoque, así como el empaquetado de todos los dispositivos antes de su transporte. Es importante para los investigadores recoger cualquier material que pueda relacionarse con la información digital potencial (por ejemplo, papeles con contraseñas anotadas, soportes y conectores de alimentación de los dispositivos del sistema incorporado). La evidencia digital puede perderse o dañarse si no se aplica un cuidado razonable. Los investigadores deberían adoptar el mejor método de recolección posible en función de la situación, el costo y el tiempo, así como documentar la decisión de utilizar un método en particular.

NOTA 1: La eliminación de medios de almacenamiento digital no siempre es recomendable y el investigador debe estar seguro de que son competentes para remover soportes de almacenamiento y reconocer cuándo es apropiado y permitido hacerlo.

NOTA 2: Los detalles de los dispositivos digitales no recogidos deben documentarse con la justificación de su exclusión, de conformidad con los requisitos de competencia aplicables.

ETAPA 3 - ADQUISICIÓN

El proceso de adquisición implica producir una copia de la evidencia digital (por ejemplo: la copia de un disco duro completo, una partición o archivos seleccionados), la documentación de los métodos utilizados y las actividades realizadas. El investigador deberá adoptar un método de adquisición adecuada basada en la situación, el costo y el tiempo, y documentar la decisión de utilizar un método particular o herramienta adecuada.

Los métodos utilizados para adquirir evidencia digital deben ser claramente documentados en detalle, en lo que sea prácticamente posible, debe ser reproducible o verificable por un investigador competente. Los investigadores deben adquirir la evidencia digital de la manera menos intrusiva con el fin de evitar la introducción de cambios en lo posible. Al llevar a cabo este proceso, el investigador debe considerar el método más apropiado para su uso. Si los resultados del proceso son inevitables a los datos digitales, las actividades realizadas deberán ser documentadas para explicar los cambios en los datos.

El método de adquisición utilizado deberá presentar una copia de la evidencia digital de la evidencia digital potencial o dispositivo digital que pueda contener evidencia digital potencial. Tanto la fuente original y la copia de la evidencia digital deberán ser verificadas con una función de verificación probada (demostrando precisión en ese punto en el tiempo) que sea aceptable para la persona que va a utilizar la evidencia. La fuente original y cada copia de la evidencia digital deben producir la misma salida de la función de verificación.

En circunstancias en las que no se puede llevar a cabo el proceso de verificación, por ejemplo, cuando la adquisición es a un sistema en funcionamiento, cuando la copia original contiene sectores de error o el período de tiempo de adquisición es limitado. En tales casos, el investigador deberá utilizar el mejor método posible disponible y ser capaz de justificar y defender la selección del método. Si la imagen no se puede verificar, entonces esto necesita ser documentado y justificado. Si es necesario, el método de adquisición utilizado deberá ser capaz de obtener el espacio asignado y no asignado.

NOTA 1: Cuando el proceso de verificación no se puede realizar en la fuente completa debido a errores en la fuente, la verificación utilizara las partes de la fuente que se puedan leer con fiabilidad y que puedes ser utilizadas.

Puede haber casos en los que no es factible o permisible crear una copia de la evidencia digital de una fuente de evidencias, como cuando la fuente es demasiado grande. En estos casos, un investigador puede realizar una adquisición lógica, que se enfoca en tipos de datos, directorios o lugares específicos. En general, esto se lleva a cabo a nivel de archivo y partición. Durante la adquisición lógica, los archivos activos y archivos no basados en el espacio asignado en los medios de almacenamiento digital pueden ser copiados; archivos eliminados en el espacio no asignado no pueden ser copiados, dependiendo del método utilizado. Otros casos en los que este método puede ser útil es cuando son sistemas críticos involucrados y que no pueden ser apagados.

NOTA 2: Algunas jurisdicciones pueden requerir un tratamiento especial de los datos; por ejemplo, sellar los datos en presencia del propietario. El sellado debe hacerse de conformidad con las normativas locales (legislativas y de procedimiento).

ETAPA 4 - PRESERVACIÓN

La evidencia digital potencial deberá preservarse para asegurar su utilidad en la investigación. Es importante proteger la integridad de las pruebas. El proceso de conservación implica la protección de la manipulación o la expoliación de la evidencia digital y los dispositivos digitales potenciales que pueden contener evidencia digital potencial. El proceso de conservación deberá ser aprobado y deberá mantenerse durante todo el proceso de manipulación de la evidencia digital, a partir de la identificación de los dispositivos digitales que contienen evidencia digital potencial.

En el mejor de los casos, no debería haber ningún despojo de los propios datos o los metadatos asociados con ella (por ejemplo, fecha y sello de tiempo). El investigador deberá ser capaz de demostrar que la evidencia no ha sido modificada desde que se recogió o fue adquirida, y deberá proporcionar los fundamentos y acciones documentadas si se hicieron cambios inevitables.

NOTA: En algunos casos, la confidencialidad de las pruebas digitales es un requisito; ya sea un requisito de negocio o un requisito legal (por ejemplo, la privacidad). La evidencia digital potencial debe conservarse de manera que garantice la confidencialidad de los datos.

ERRORES COMUNES

Una serie de errores comunes puede ocurrir durante las investigaciones. (Andy Jones & Craig Valli, 2009)

- La primera y la más frecuente de ellas es la falta de mantenimiento de la documentación adecuada. La creación y el mantenimiento de la documentación es tan tedioso y exigente, por lo que este es uno de los errores más comunes.
- Otra es la modificación accidental de los datos mediante la apertura de los archivos de la evidencia original. Simplemente la apertura de un archivo al examinar los contenidos da como resultado las marcas de tiempo en el archivo que se está examinando. Esto puede dificultar la investigación posterior y el resultado de las pruebas es que se queden inutilizables.
- Otra es la destrucción de evidencia potencial como resultado de la instalación de software en los medios de comunicación en la evidencia. La escritura de software en la memoria del dispositivo digital o en el disco duro puede causar distorsión en la evidencia que se encuentre alojada allí, porque no se encuentra protegida, y se sobrescribe en ella.
- Otro error común es no controlar adecuadamente el acceso a la evidencia digital y mantener la cadena de custodia. Cuando esto ocurre, es casi imposible demostrar que la evidencia no ha sido comprometida.

Si bien estos errores podrían parecer evitables, hay momentos en algunas investigaciones por ejemplo en las que es necesario abrir un archivo de la evidencia original antes de que sea copiada o de instalar algún software con el fin de recuperar la evidencia original. Esto ocurre especialmente en las investigaciones sobre grandes sistemas de red en las que no pueden ser fácilmente aislados o apagados estos sistemas. Cuando sea necesario llevar a cabo este tipo de acciones, es esencial que se registren, junto con la razón que se tomó para realizar dichas accione.

Un fracaso para el investigador es no poder saber cuándo se han alcanzado los límites de su conocimiento y el momento de pedir ayuda. En el área del análisis forense digital, el tema es ahora tan amplio y complejo que no es posible que una persona tenga el nivel necesario de conocimientos en todas sus áreas pertinentes. Una vez que el investigador es superado en su área de conocimiento, cualquier evidencia que se recupere será de valor cuestionable y puede ser impugnada en los tribunales.

CADENA DE CUSTODIA

En las investigaciones se debe ser capaz de dar cuenta de todos los datos y los dispositivos adquiridos en el momento que se encuentra dentro de la custodia. El registro de cadena de custodia es un documento de identificación de la cronología del movimiento y la manipulación de la evidencia digital potencial. Se debe establecer la colección o el proceso de adquisición, esto suele llevarse a cabo mediante el trazado de la historia del elemento desde el momento en que fue identificada, recolectada o adquirida por el equipo de investigación hasta el presente estado y ubicación.

El registro de la cadena de custodia es un documento o serie de documentos relacionados que detalla la cadena de custodia y registros de quien fue el responsable del manejo de la evidencia digital potencial, ya sea en forma de datos digitales o en otros formatos (como las notas de papel). El propósito de mantener un registro de cadena de custodia es permitir la identificación de acceso y circulación de pruebas digitales potenciales en cualquier punto dado en el tiempo. El registro de cadena de custodia en sí puede comprender más de un documento, por ejemplo, para potenciales pruebas digitales debería ser un documento contemporáneo que guarde la adquisición de datos digitales a un dispositivo en particular, el movimiento de ese dispositivo de grabación y la documentación de extractos posteriores o copias de potencial evidencia digital para su análisis u otros propósitos.

De acuerdo a la norma ISO/IEC 27037:2012, el registro de cadena de custodia debe contener como mínimo la siguiente información:

- Identificador único de evidencias;
- Quien accede a la evidencia, la hora y el lugar donde se llevó a cabo;
- Quién verifica las pruebas de entrada y salida de la planta de preservación de pruebas y en el momento que sucedió;
- Por qué la prueba se desprotegió (en cualquiera de los casos y su propósito) y la autoridad competente que lo realizo, y
- Todo cambio inevitable a la evidencia digital potencial, así como el nombre de la persona responsable del mismo y la justificación de la introducción del cambio.

La cadena de custodia debe mantenerse durante toda la duración de las pruebas y conservarse durante un cierto período de tiempo después de finalizar la vida útil de la evidencia - este período de tiempo se puede ajustar de acuerdo a las jurisdicciones locales de la colección y la aplicación de las pruebas. Debería de ser establecido desde el momento que es adquirida la evidencia digital y la evidencia digital potencial no deberían de ser comprometidos.

NOTA: Algunas jurisdicciones pueden tener requisitos especiales con respecto a la cadena de custodia. Esto es facultad de los códigos procesales o códigos de procedimiento.

La cadena de custodia es un término legal que se refiere a la capacidad de garantizar la identidad y la integridad de la evidencia desde el momento en que se recoge a través del tiempo, los resultados del análisis se reportan y posteriormente se desechan. La cadena de custodia garantiza responsabilidad continua, lo cual es importante porque, si no se mantiene correctamente, una evidencia no puede ser admisible en la corte. (Andy Jones & Craig Valli, 2009)

La cadena de custodia consiste en un registro cronológico de las personas que han tenido la custodia de la evidencia desde su colección. Cada persona en la cadena de custodia es responsable de todos los aspectos del cuidado de la evidencia mientras está bajo su control. Debido a la naturaleza sensible de las pruebas, es una práctica normal designar a una persona en calidad de custodio de la evidencia, a asumir la responsabilidad de la evidencia cuando no esté en uso del investigador o de una de las otras personas autorizadas que participan en la investigación.

En el pasado, las pruebas documentales se limitan a los documentos en papel, donde aplicaba la regla del mejor resultado de la evidencia para luego producir el documento original. Sin embargo, con la rápida transición a la era de la información, los documentos ahora son raramente escritos a mano o producidos en una máquina de escribir, hoy en día se crean usando software de procesamiento de texto en ordenadores personales. Cada vez más, estos documentos ya no se imprimen y no se envían por correo regular o por fax al destinatario, ahora se envían directamente desde el ordenador.

Las copias de los archivos digitales se consideran como el documento electrónico original (siempre que sea posible se deben producir copias de la evidencia digital, utilizando criptografía hash).

FUENTES POTENCIALES DE EVIDENCIA

En el pasado, en los primeros días de la computación, las únicas fuentes viables de evidencia digital en un dispositivo digital se consideraron en el disco duro y disquetes. La memoria volátil se limitaba en tamaño y no existía el concepto de evidencia potencial que hoy en estos días se está recuperando evidencia en ella. En los dispositivos digitales modernos, existe una amplia gama de fuentes potenciales de pruebas electrónicas. Las fuentes potenciales de evidencia digital en equipos electrónicos que el investigador debe tener en cuenta son: (Andy Jones & Craig Valli, 2009)

- Discos duros externos e internos
- Disqueteras
- CDs/DVDs
- Pen drives (Dongles[42])
- Modems
- Routers
- Teléfonos móviles
- Tapes
- Jaz/Zip Cartridges

[42] Dongles: En informática, una mochila, llave, candado o seguro electrónico (dongle en inglés) es un pequeño dispositivo de hardware que se puede integrar a un programa y se conecta a un ordenador, normalmente, para autenticar un fragmento de software

- Cámaras
- MP3 Players
- Dispositivos de red
- Dispositivos Bluetooth
- Dispositivos infrarrojos
- Dispositivos WiFi

Esta lista tiene por objeto indicar el alcance que debe tener en cuenta el investigador y no es tan exhaustiva. Lo que también hay que tener en cuenta es que los procedimientos forenses estándar se deben seguir en las pruebas forenses digitales al mismo tiempo que se está recolectando y preservando la evidencia digital. Es muy posible que el elemento de una evidencia convincente se encuentre en la huella digital en el teclado en lugar del dispositivo digital, o podría ser la contraseña escrita en un pedazo de papel que se ha quedado adjunta al computador que de acceso al investigador la evidencia de mayor peso. El análisis forense digital está constituido de herramientas y técnicas que se pueden aplicar a cualquier investigación, y la forma en que se maneja debe asegurarse de que se integren en las otras partes de la investigación y estar en línea con los estándares apropiados, así como las políticas de la organización y procedimientos. Por ejemplo, si las huellas dactilares deben tomar desde un disquete, en qué momento deberían ser tomadas y qué se debe utilizar para tomarlas. Una unidad de disco es altamente sensible al polvo y a otros objetos, particularmente cuando el polvo en cuestión es un óxido de metal, es posible que la recuperación de los datos desde el disco flexible y la toma de prueba de las huellas dactilares latentes no se coordinaran siguiendo los estándares establecidos, alguna o todas las demás evidencias potenciales podría perderse.

EL EXAMINADOR FORENSE DIGITAL

El papel del examinador forense digital es localizar los datos que existen en un sistema informático y todos los dispositivos asociados. Esto puede requerir que se recupere información eliminada o borrada, dañada, cifrada, o recuperar las contraseñas para poder acceder al contenido de los archivos. El investigador debe ser consciente de que cualquier información que se descubra durante el análisis puede ser utilizada por cualquiera de los lados durante el litigio, ya sea civil o penal. Esto plantea dos cuestiones distintas: el papel del investigador forense y la cantidad de tiempo dedicado a una investigación. (Andy Jones & Craig Valli, 2009)

La tarea del investigador forense digital es descubrir los hechos. Si bien se ha iniciado la investigación como el resultado de una sospecha de que ha ocurrido algo, siempre el investigador debe recordar que su función es la de determinar los hechos relacionados con el incidente.

Es normal que cuando la información obtenida es suficiente para demostrar un delito, todos los datos que no han sido utilizados por el investigador permanecen intactos. Esta es un caso de la utilización de los recursos, si las pruebas han sido suficientes para demostrar alguna anomalía, no sería sensato ni económico investigar más a fondo sobre el enfoque de la utilización de recursos, pero el problema con este enfoque es que puede dejar evidencias ocultas, o más crímenes pueden permanecer sin descubrirse, o incluso información que pueda resultar sospechosa no puede ser demostrada.

El análisis forense digital es importante para las organizaciones, ya que tiene la ventaja de ahorrar presupuestos. Cada vez los departamentos de TI (y en particular el departamento de seguridad de TI) realizan presupuestos para proteger a los sistemas con tecnologías tales como firewalls, software antivirus, sistemas de detección de intrusos (IDS) o los sistemas de protección de intrusos (IPS) con el fin de detectar actividades maliciosas. Estas inversiones sólo pueden ser razonables si la información correcta se recoge y se almacena de manera válida a efectos legales, ya que de ser necesario en algún momento se puede acceder a la información la cual no ha sido alterada o contaminada de alguna manera y se puede utilizar para cualquier acción civil o penal contra el responsable de algún delito que se haya cometido.

TIPOS DE DATOS

Se encuentran y se colectan dos tipos de datos básicos durante una investigación forense digital. El primer tipo de dato, es el dato persistente. Un ejemplo de estos datos, son los datos almacenados en un disco duro o un CD/DVD el cual persiste (o se conserva), esto significa que cuando los dispositivos digitales se apagan o se encienden los datos permanecen en él. (Andy Jones & Craig Valli, 2009)

El segundo tipo se refiere a los datos volátiles, se trata de los datos que existan en la memoria, o en la transmisión, que muy probablemente se perderán cuando el dispositivo digital se apague. Los lugares más comunes para los datos volátiles se encuentran en los registros de los dispositivos, la memoria caché y la memoria de acceso aleatorio (RAM).

Además de los datos en la memoria, se encuentra el tráfico en la red que generalmente tiene dos usos. La primera, relativa a la seguridad, implica el seguimiento de una red para el tráfico anómalo y la identificación de intrusiones. Un atacante podría ser capaz de borrar todos los archivos de registro en un servidor comprometido, por lo que la evidencia basada en la red puede ser la única evidencia disponible para el análisis forense. La segunda forma de análisis forense de redes se refiere al cumplimiento de la ley. En este caso, el análisis de tráfico de red capturado puede incluir tareas como volver a montar los archivos transferidos, en busca de palabras clave y analizar la comunicación humana, tales como correos electrónicos o chats.

Es importante que el investigador entienda estos dos tipos de datos y poder valorar el dato más importante para poder preservarlo con el fin de capturar la evidencia necesaria de la actividad, ya que cada uno de ellos puede ser necesario durante una investigación.

Como ejemplo, en una investigación sobre un ataque informático a un computador. La decisión puede ser necesaria en cuanto si se debe capturar la memoria volátil, donde la evidencia de las acciones más recientes del perpetrador puede ser capturada, o simplemente capturar los datos persistentes. El riesgo es que en el intento de capturar la memoria volátil, los datos persistentes pueden perderse debido a que el equipo seguirá funcionamiento durante más tiempo y el atacante puede utilizar la oportunidad de eliminar pruebas durante ese tiempo.

LA PREPARACIÓN FORENSE

Uno de los factores que cualquier persona responsable en la gestión o la administración de sistemas informáticos o redes debe tener en cuenta, es que los procedimientos necesarios para restablecer las operaciones normales dentro de la organización durante un incidente, la recopilación y recuperación de pruebas sea más fácil. Estas medidas están siendo cada vez referidas al investigador forense digital y de acuerdo con Rowlingson[43], hay un proceso de diez pasos que pueden ser utilizados por cualquier organización para garantizar que, en caso de un incidente, serán capaces y estar preparados para la recolección y el almacenamiento de la información que se requiere para una investigación exitosa. Rowlingson describe los pasos como:

1. **LA DEFINICIÓN DE LOS ESCENARIOS DE NEGOCIO QUE REQUIEREN EVIDENCIA DIGITAL:** Nunca será posible predecir todos los escenarios que se puedan presentar, pero los que son considerados como los más probables, o aquellos que causarían a la organización la mayor preocupación, se pueden identificar. Hay diferentes tipos de organizaciones sensibles a diferentes escenarios dependiendo del tipo de sistemas utilizados y la forma en que se utilizan. La definición de estos escenarios se definen como:

- UNA REDUCCIÓN EN EL IMPACTO DE UN DELITO INFORMÁTICO. Se ha pensado en los factores que afecten la probabilidad de un incidente y el impacto del incidente de este tipo en la organización, esta consiente la organización en sus puntos vulnerables y las medidas que se pueden tomar para reducir al mínimo la probabilidad y el nivel de impacto de un incidente.
- LOS REQUISITOS LEGALES. Mediante la comprensión de los requisitos legales en la recolección, el almacenamiento, la manipulación, y la divulgación de la información, será posible organizar la recolección y almacenamiento con el fin de retener sólo la información

[43] Rowlingson. R, "A ten-Step Process for Forensic Readiness," International Journal of Digital Evidence, Winter 2004, Volume 2, Issue3.

que es más probable que se requiera y almacene de manera que todos los requisitos legales puedan cumplirse sin interrupción indebida en el funcionamiento de la organización.

- LA PRODUCCIÓN DE PRUEBAS. Puede que sea necesario que para demostrar el cumplimiento de una serie de requisitos reglamentarios o legales o de presentar pruebas para su uso en cualquier penal o disciplinaria interna o externa de los casos civiles, cada uno de estos casos pueden requerir almacenar diferentes tipos de información, si se han considerado una serie de escenarios, la datos correspondientes pueden ser identificados y almacenados para cumplir con estos requisitos.

2. **IDENTIFICAR LAS FUENTES DISPONIBLES Y LOS DIFERENTES TIPOS DE POSIBLES PRUEBAS:** La realización de este proceso ayuda a cualquier investigación a identificar las posibles fuentes de información. La identificación de la fuentes de información pueden ayudar a resaltar las deficiencias en la información que se recolecta y almacena actualmente y permitirá realizar cambios en el tipo de información recolectada, así mismo ayudara a colocar sensores para su monitoreo. Los procedimientos creados como parte de esta actividad asegurará el nivel y el tipo de información recolectada y el nivel de utilización para cualquier investigación.
    - En este proceso, algunos de los aspectos a tener en cuenta incluyen el formato de los datos, el período de tiempo que se almacenan, los lugares de almacenamiento, el control de los datos y quién tiene acceso a ellos. Otras fuentes de información que pueden ser requeridos y que pueden ponerse a disposición en una investigación y que forman parte de las restricciones legales o reglamentarias son: La Ley de Protección de Datos, acuerdo de Basilea II, Sarbanes Oxley, la legislación de derechos humanos, entre otros.

3. **DETERMINAR EL REQUISITO DE RECOLECCIÓN DE PRUEBAS:** Al considerar el problema previamente con el personal que tendrán que llevar a cabo las investigaciones, como por ejemplo: el administrador de sistemas y el equipo legal deberían determinar en la manera posible el tipo y la cantidad de información que pueden y debes ser recolectados. Cuando los escenarios han sido identificados y las posibles fuentes de información han sido aislados, será posible determinar los requisitos de recopilación de pruebas.
    - Los temas que deben abordarse al determinar los requisitos de la recopilación de la evidencia, es cómo la evidencia puede recolectarse sin interferir indebidamente en los procesos de trabajo de la organización, la gestión del coste de la recolección y el almacenamiento de información en proporción a un incidente, la legalidad de la

recolección de la información necesaria y si habrá suficiente información disponible para permitir una investigación exitosa.

- Una vez que se han considerado estos factores, será posible para la organización entender la inversión económica del almacenamiento de los datos necesarios y la recopilación de pruebas, esto ayudara a determinar si los datos identificados se recolectan por razones específicas o por otros motivos. Si toda la información requerida no está siendo recolectada, entonces una decisión de la alta gerencia debe de hacerse sobre la inversión económica de la recolección y almacenamiento de la información adicional.

4. **ESTABLECER LA CAPACIDAD PARA RECOPILAR Y ALMACENAR DE FORMA SEGURA EVIDENCIA DE FORMA QUE SEA LEGALMENTE ADMISIBLE:** Esto incluye la planificación para garantizar que las herramientas y las instalaciones están establecidas adecuadamente para asegurarse de que la información se recopila y almacena de forma adecuada y que el personal esta adecuadamente capacitado, conscientes de las necesidades, y cuentan con la experiencia práctica en este tipo de procedimientos, por lo que cualquier evidencia recolectada y almacenada será admisible en cualquier procedimiento disciplinario legal o interno.
   - Los temas que necesitan ser considerados en este apartado incluyen, si la información ha sido recolectada de una manera que es jurídicamente correcta y se ha almacenado de una manera que se hace admisible en cualquier corte. Hay que prestar atención a la forma en que se recopilan los datos. Por ejemplo, la organización tiene el derecho de supervisar y recoger el correo electrónico institucional (tienen políticas de uso de Internet y sobre el uso del correo electrónico dentro la organización). También se debe tener en cuenta los procedimientos de almacenamiento y que miembros del personal tendrán acceso a los registros almacenados.

5. **ESTABLECER UNA POLÍTICA PARA EL ALMACENAMIENTO SEGURO Y LA MANIPULACIÓN DE PRUEBAS POTENCIALES Y ASEGURARSE DE QUE SE ENSAYA CORRECTAMENTE Y REGULARMENTE:** Es sólo mediante la planificación previa el correcto almacenamiento y la manipulación de la información para poder asegurar que la prueba será útil en un determinado momento.
   - Se debe asegurar de que las auditorías y otros registros y cualquier otra información relevante se almacenarán de tal manera que no pueden ser alterados o modificados, y que tales registros se almacenan por el propietario de forma físicamente segura.

6. **ASEGURAR QUE EL MONITOREO DE LOS SISTEMAS Y EL TRÁFICO EN LAS REDES SE DIRIJA TANTO A DETECTAR COMO A IMPEDIR INCIDENTES DE GRAVEDAD**: Este paso debe formar parte de los procesos normales de seguridad y los procedimientos implementados para proteger los sistemas informáticos, pero el aporte del investigador puede proporcionar un punto de vista diferente, mejorando las defensas de los sistemas de monitoreo.
   - El monitoreo se guiará por una serie de factores indicativos de los diferentes tipos de actividad. Por ejemplo, la actividad de fraude puede estar indicada por patrones en los datos financieros. La fuga de los derechos de propiedad intelectual de la organización puede ser revelada mediante la comprobación de la información contenida en los mensajes de correos electrónicos y datos adjuntos en los registros de los archivos en medios extraíbles o en las impresiones de documentos. El abuso de los privilegios en un sistema informático puede ser indicado por los permisos de autoridad que contenga un determinado usuario, en los derechos de acceso, acceso a los archivos y áreas del sistema. Mediante el análisis el investigador deberá buscar el control adecuado para poder controlar toda la información inútil, ya que la recuperación de cualquier información significativa de grandes volúmenes de datos almacenados será difícil y costoso.

7. **ESPECIFICAR LAS CONDICIONES EN QUE UN INCIDENTE DEBE ESCALARSE EN UNA INVESTIGACIÓN FORMAL COMPLETA:** Al considerar esto con antelación, es posible pensar en los escenarios de forma racional y poder obtener el aporte necesario de todas las partes que se verán afectadas o involucrados. Se deben de considerar las problemáticas con mucho análisis en lugar de tener que tomar decisiones apresuradamente durante un incidente.
   - Se debe asegura de que las políticas en la gestión de incidentes contienen suficientes detalles para las condiciones en que se escalarían los diferentes incidentes e incluir detalles de los personas que deben ser informadas/involucrados en los escenarios identificados.

8. **CAPACITAR A TODO EL PERSONAL PERTINENTE EN LA SENSIBILIZACIÓN DE INCIDENTES:** De esta manera, todo el personal que estará involucrado sabrá su papel en el proceso del análisis de pruebas digitales y tendrán un entendimiento de los requisitos legales para la recolección y almacenamiento de pruebas. Se debe recordar que no será posible capacitar al personal y asegurar que tienen una conciencia del papel que desempeñarán en el momento del incidente, para entonces, será demasiado tarde.

9. **DOCUMENTAR Y DESCRIBIR EL IMPACTO DEL INCIDENTE BASADO EN LA EVIDENCIA DIGITAL**: Al documentar un caso, se deberá proporcionar un reporte del incidente con el fin de procesar todos los detalles para tenerlo en cuenta futuras investigaciones. También dará a las personas involucradas en la gestión de incidentes la oportunidad de considerar los diferentes impactos y permitirá que se analicen nuevas decisiones y medidas a tomar en cuenta.

10. **ASEGURAR DE QUE HAYA UNA REVISIÓN LEGAL DE LOS PROCEDIMIENTOS DESARROLLADOS:** Esto facilitará cualquier acción tomada en respuesta a un incidente. Al obtener una opinión legal de las políticas y procedimientos que se han establecidos para asegurarse de que se están realizando legalmente, la organización puede tener la confianza en que el medidas implementadas son eficaces y correctas.

- El asesoramiento jurídico que se debe buscar debe comprender todas las posibles responsabilidades que pueda resultar de un incidente, las restricciones legales o reglamentarias que deben ser tomados en cuenta, los métodos a seguir cuando haya personal involucrado y cualquiera otro detalle que se debe considerar cuando se realice la revisión legal.

ASPECTOS LEGALES DE LA EVIDENCIA DIGITAL

Cualquier persona responsable de la gestión de la seguridad informática debe estar consciente de las consecuencias jurídicas de la actividad forense digital. Los profesionales de seguridad deben tener en cuenta las políticas, reglamentos, normas y poner en práctica las acciones técnicas en el contexto de las leyes existentes. Por ejemplo, debe tener la autorización correspondiente antes de iniciar el seguimiento y la recopilación de información relacionada con una intrusión informática. También deberá ser conocedor que hay consecuencias legales para el uso de una variedad de herramientas de supervisión de la seguridad informática. (Andy Jones & Craig Valli, 2009)

La ciencia forense digital es una disciplina relativamente joven en la comunidad jurídica y la cuestión se complica más por el rápido cambio tecnológico y las nuevas formas de realizar delitos informáticos. Como resultado de la problemática anterior, muchas de las leyes que se utilizan para perseguir los delitos relacionados con la informática están obsoletas o son leyes que nunca fueron destinadas a ser utilizadas para el entorno digital. Por ejemplo en el Reino Unido, no hace mucho tiempo, phreakers (personas que obtienen las llamadas telefónicas gratuitas) fueron procesados por el robo de la electricidad la única ley en el momento por la cual podían ser procesados. En el Reino Unido, la Ley de Abusos Informáticos de 1990 fue presentada como la primera ley para tratar específicamente los delitos informáticos, pero se encontró muy rápidamente que era difícil enjuiciar bajo esta legislación.

Desde entonces se ha ido actualizado, y la más reciente es el Acta de 2006 de la Policía y la Justicia que procesa delitos informáticos.

Por ejemplo en los EE.UU., una de las mejores fuentes de información en materia de delincuencia informática es el Departamento de Justicia del Delito Cibernético. El sitio ofrece una excelente lista de casos judiciales recientes que se relacionan con la delincuencia informática, también ofrece guías sobre cómo introducir la evidencia digital en la corte y las normas pertinente.

TIPOS DE INVESTIGACIÓN DE LA INFORMÁTICA FORENSE

La ejecución de una investigación forense digital y el tipo de investigaciones que puedan llevarse a cabo, por ejemplo, en un solo equipo, una red o un dispositivo móvil. La razón para la cobertura de estos temas es poner en relieve la variedad de tipos de investigación que el laboratorio puede involucrar y en función de ello las decisiones necesarias a tomar. Estas decisiones son particularmente importantes en las primeras etapas de una investigación, todo con el fin de asegurar que los datos sean capturados de forma correcta y apropiada.

Si la investigación forense digital no se gestiona desde el principio, no se podrán lograr los objetivos, habrá un desperdicio de recursos y esfuerzo. Es esencial que el gerente del laboratorio ponga en marcha los procesos, procedimientos y herramientas necesarias para apoyar al personal y de que estos se encuentren debidamente entrenados y capacitados con la finalidad de ser eficientes y efectivos en la manipulación y recolección de las evidencias.

RAZONES PARA LA REALIZACIÓN DE UNA INVESTIGACIÓN FORENSE DIGITAL

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sean humanas, procedimentales o tecnológicas sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos.

Las razones para llevar a cabo una investigación forense digital serán amplias y dependerán, en parte, por el tipo de organización a la cual pertenece. El tipo de investigación que se requiere para llevar a cabo un análisis por las entidades de justicia e investigación, como la Policía Nacional Civil (PNC) o la Fiscalía General de la Republica (FGR), normalmente se centrará en toda la gama de causas penales. Esto, en sí mismo, tiene una considerable diversidad y debido a que cada vez, más dispositivos electrónicos se han incorporado en muchos aspectos de nuestra vida cotidiana, ya no se limita a la categoría de "Crímenes basados en computadoras". Un ejemplo de esto se pone de relieve en el Reporte Norton 2013 (Symantec), que afirma que de 13,022 personas, el 41 por ciento de los adultos

conectados a la red han sufrido ataques tales como malware, virus, estafas fraudes y robo y que existen 378 millones de víctimas por año.

De acuerdo al reporte Tendencias de Seguridad Cibernética en América Latina y El Caribe (Symantec), las experiencias recientes de los países de la región en cuanto a los delitos informáticos, confirman que los gobiernos no pueden ocuparse por sí solos de garantizar la seguridad del dominio cibernético.

Un laboratorio forense digital puede ser parte también de una entidad corporativa o un laboratorio comercial, el ámbito de aplicación bien puede extender para incluir la recuperación de datos o para apoyar a los proveedores de servicios legales para el descubrimiento civil, donde el foco de trabajo estará en la extracción de información relevante para apoyar las acciones legales. Otras áreas en las que un laboratorio corporativo pueda ser utilizado es en el apoyo para el personal de auditoría de TI y personal de seguridad, en donde se utilizan como parte de una respuesta a un incidente independiente y/o recuperación de desastres, o la utilización por el personal de recursos humanos para la investigación penal y civil por incidentes en su lugar de trabajo.

EL PAPEL DE LA COMPUTADORA EN UN DELITO

<<El cadáver se halla a un lado de la cama. Un armario, una mesa y una silla completan el mobiliario de tan adusta dependencia. Mientras los investigadores indagan sobre la tormentosa vida conyugal de la víctima, los especialistas de la policía científica continúan con su labor, examinando la escena, tomando fotografías y realizando un reportaje video gráfico. Un arma de fuego corta asoma tras el cuerpo de la víctima, y al otro lado de la habitación, sobre una puerta, se adivina la oquedad dejada por un proyectil, el cual, no ha sido encontrado... todavía. ¿Suicidio? ¿Asesinato? Encima de la mesa hay un ordenador portátil y un teléfono móvil. Todas las evidencias papiloscópicas[44], biológicas y balísticas se recogen aplicando las técnicas adecuadas, pero. ¿Qué hacer con el ordenador?, ¿Qué hacer con el teléfono móvil?>>

<<Oculto tras el anonimato, en su oscuro despacho, solamente iluminado por la tenue luz del atardecer, consulta sus mensajes electrónicos privados y profesionales, y ¿por qué no? los de algunos de sus compañeros de trabajo también. ¿Qué clientes tienen? ¿Alguna relación amorosa inconfesable? ¿Algún problema económico? ¿Algún escándalo político? En fin, algún dato que pueda ser tenido en cuenta profesionalmente o como chismorreo. Sobresaltado por la aparición en la puerta del director y

[44] Es la disciplina técnica, parte esencial de la Criminalística, basada en principios científicos debidamente comprobados que tienen por objeto establecer a través del estudio de los calcos, impresiones, estampas o improntas de las crestas papilares, sean estas digitales (tercera falange digital), palmares (obrantes en la cara interna de las manos) y/o plantares (cara interna de los pies), con la finalidad de establecer en forma categórica e indudable la Identidad Física Humana.

una comitiva, trata de cerrar las ventanas que estaba consultando, demasiado tarde, lo han descubierto. Pero ¿Qué hacer con el ordenador?, ¿Cuáles son los pasos a seguir?>> [45]

En cualquier incidente, la computadora podría haber jugado su parte en una de las siguientes tres maneras: (Andy Jones & Craig Valli, 2009)

- La primera es donde la computadora es la víctima de un crimen. Esto es normalmente donde es el blanco de la piratería, virus, caballos de Troya o incidentes de tipo de denegación de servicio.
- La segunda es que el equipo ha sido utilizado como una herramienta en la comisión de un delito; por ejemplo, el envío de amenazas de chantaje. Este tipo de papel cubrirá casi todos los ámbitos de la delincuencia, incluyendo el fraude, la pedofilia, la piratería, el espionaje industrial, delitos contra la propiedad intelectual, y el almacenamiento de la información relativa a cualquier número de otros tipos de delitos. La razón de esto se debe al rol que las computadoras y las redes juegan en las comunicaciones modernas y su creciente integración en todos los aspectos de la vida personal y de negocios.
- La tercera forma en que un ordenador se puede conectar a un delito es de una manera incidental, en las que puede contener la información que se relaciona con delitos como el tráfico de drogas que su dueño está involucrado.

TIPOS DE DISPOSITIVOS Y SISTEMAS QUE PUEDEN REQUERIR DE INVESTIGACIÓN

La gama de dispositivos computarizados que pueden ser fuentes potenciales de información y pruebas y ser considerados para las investigaciones forenses es inmensa. En los hogares de las personas y en algunas oficinas pequeñas, se encuentra el ordenador personal y el enrutador que lo conecta con el mundo exterior, probablemente una consola de juegos, un receptor de televisión por satélite que puede tener la capacidad de Internet y el correo electrónico, el sistema de alarma y sistemas de control para la lavadora y controles ambientales, y cada vez más, otros "productos de línea blanca", en los vehículos automotores, el sistema de gestión del motor y el sistema de navegación por GPS,

[45] Extraído de la publicación: LA INFORMÁTICA FORENSE: EL RASTRO DIGITAL DEL CRIMEN, escrito por Francisca Rodríguez Más y Alfredo Doménech Rosado. Disponible en: http://www.derechoycambiosocial.com/revista025/informatica_forense.pdf

que puede incluir una facilidad de comunicaciones inalámbrica o Bluetooth. En la oficina, habrá sistemas de redes de ordenadores y sistemas de control de acceso y sistemas de alarma.

Para el usuario individual, es el ordenador portátil y los dispositivos móviles, como los Smartphone[46] y/o las Tablets[47]. Estas últimas pueden ser una extraña elección de palabras para describir lo que, hasta la fecha, se ha referido como el "teléfono móvil", pero ese término ya no describe realmente los dispositivos que todos llevamos regularmente con nosotros. Los dispositivos de hoy cada vez más parecen un ordenador en miniatura, es más, poseen capacidades superiores en relación de algunas computadoras. Además de realizar llamadas telefónicas, contiene una libreta de direcciones y un diario, se puede navegar por Internet, enviar correos electrónicos, y actuar como un dispositivo de SMS[48].

Los tipos de información que pueden contener pruebas se encuentran en uno de los tres grupos: Datos Activos, Archivo de Datos, y Datos latentes. (Andy Jones & Craig Valli, 2009)

- **DATOS ACTIVOS:** son la información que se puede ver en el dispositivo, tales como archivos de datos, los programas y los archivos del sistema operativo. Este es el tipo más fácil de datos para recoger.

  DATOS INACTIVOS
- **ARCHIVO DE DATOS:** son los datos que se han hecho copias de seguridad. Esto se puede almacenar, por ejemplo, en los DVDs, CDs, disquetes, cintas de copia de seguridad y discos duros.
- **DATOS LATENTES:** es la clase de información que puede requerir herramientas especializadas para recuperar e incluye información que se ha eliminado o han sido parcialmente sobrescrita.

TEMAS A CONSIDERAR CUANDO SE TRATA DE UN SOLO EQUIPO

La investigación en un solo equipo es probablemente el tipo más fácil de realizar, sin embargo, el nivel de dificultad está creciendo debido a que los ordenadores se vuelven más poderosos y el tamaño de almacenamiento aumenta así como también los medios de comunicación y las formas en que se

[46] Término dado a teléfonos celulares con capacidades avanzadas
[47] Término dado a dispositivos electrónicos de mano con capacidades de ordenadores portátiles
[48] El servicio de mensajes cortos o SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (también conocidos como mensajes de texto) entre teléfonos móviles

conectan a las redes y esto hace que se vuelvan menos evidentes (WiFi[49], WiMax[50] y Bluetooth[51]). Cuando se trata de un único dispositivo los elementos a ser considerados son:

- La Computadora personal (de escritorio y/o portátil)
- Los dispositivos periféricos
- Soporte de almacenamiento
- Material asociado

En la cláusula 7.1.1.1: Documentación y búsqueda física en la escena del incidente, de la Norma ISO/IEC 27037:2012, "las computadoras se consideran como dispositivos independientes digitales que reciben, procesan y almacenan datos". (27037, ISO/IEC, 2012) Estos dispositivos no están conectados a una red, pero si pueden estar conectados a dispositivos periféricos, tales como impresoras, cámaras web, reproductores MP3[52], sistemas GPS, dispositivos RFID [53]entre otros.

Un dispositivo digital que tiene una interfaz de red, pero no está conectado en el momento de la recolección o adquisición, debe ser considerado (a los efectos de esta norma internacional) como un equipo independiente. Dónde se encuentra un ordenador con una interfaz de red, pero no hay conexión obvia, las actividades deben llevarse a cabo para identificar los dispositivos a los que pudo haber sido vinculado en el pasado reciente.

Por lo general, las escenas de incidentes contendrán varios tipos de medios de almacenamiento digital, estos medios de almacenamiento digital se utilizan para guardar datos de los dispositivos digitales y varían en la capacidad de memoria; ejemplos de medios de almacenamiento digital incluyen pero no se limitan a los discos duros externos portátiles, unidades flash, CD, DVD, discos Blue-Ray[54], disquetes, cintas magnéticas y tarjetas de memoria.

[49] WiFi, es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
[50] Wimax, siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 50 km.
[51] Bluetooth, es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.
[52] MP3, es un formato de compresión de audio digital patentado que usa un algoritmo con pérdida para conseguir un menor tamaño de archivo. Es un formato de audio común usado para música tanto en ordenadores como en reproductores de audio portátil.
[53] RFID (siglas de Radio Frequency Identification, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.
[54] Blue-Ray, es un formato de disco óptico de nueva generación desarrollado por la BDA (siglas en inglés de Blu-ray Disc Association), empleado para vídeo de alta definición y con una capacidad de almacenamiento de datos de alta densidad mayor que la del DVD.

Antes de realizar cualquier adquisición o colección, es necesario que el investigador consideré los aspectos de seguridad de la potencial evidencia digital. Se debe tener cuidado de asegurar de que un dispositivo aparentemente independiente no se ha conectado recientemente a una red y debe considerarse la posibilidad de tratarlo como un dispositivo de red para asegurarse de que otras partes de la red se manejan correctamente. El investigador debe tener en cuenta lo siguiente:

- Se debe documentar el tipo y la marca de los dispositivos digitales utilizados, e identificar todos los dispositivos informáticos y periféricos que pueden necesitar ser adquiridos o recogidos durante esta etapa inicial. Los números de serie, números de licencia y otras marcas de identificación (incluyendo daño físico) deben, en lo posible ser documentados.

- En la etapa de identificación, el estado de los equipos y dispositivos periféricos debe permanecer como está. Si los ordenadores o los dispositivos periféricos están apagados, no encenderlos. Si los ordenadores o los dispositivos periféricos están encendidos, no debe apagarse, ya que de otro modo podrían estropear la evidencia digital potencial.

- Si los equipos están encendidos, el investigador debe fotografiar o hacer un documento por escrito de lo que se muestra en las pantallas. Cualquier documento escrito debe incluir una descripción de lo que es realmente visible (por ejemplo, las posiciones de las ventanas aproximadas, títulos y contenidos).

- Un dispositivo que cuente con baterías que pueden correr el riesgo de descargarse, deberá ser cargada de energía para asegurar que la información no se pierda. El investigador forense necesita identificar y recolectar los cables y cargadores de baterías durante esta fase.

- El investigador también debe considerar el uso de un detector de señal inalámbrica para detectar e identificar las señales inalámbricas de los dispositivos inalámbricos que pueden estar ocultos. Puede haber casos en que un detector de señal inalámbrica no sea utilizado, debido a las limitaciones de costos y tiempo y el investigador debe documentar esto.

TEMAS A CONSIDERAR CUANDO SE TRATA DE UN ORDENADOR EN RED Y/O DISPOSITIVOS MÓVILES

La función del forense de red es la captura, registro y análisis de los eventos que suceden en la red con el fin de descubrir pruebas y poder determinar el origen de un incidente o problema relacionado

con la misma. El forense de red se ocupa principalmente de la información relacionada con las redes en diferentes áreas, tales como:

- La topología de red
- La configuración de la red
- El tráfico de red
- Los dispositivos de hardware que forman la red

Según Simson Garfinkel55, el autor de varios libros y artículos sobre la seguridad de la información, el análisis forense de la red se puede dividir en dos áreas principales:

1. Captura del tráfico que pasa a través de un cierto punto en la red para su posterior análisis. Esto normalmente requiere grandes volúmenes de capacidad de almacenamiento.
2. Cada paquete que pasa a través del nodo se somete a un nivel limitado de análisis mientras está en la memoria del dispositivo. Sólo la información que se considera relevante es guardada para futuros análisis. Este enfoque requiere menos almacenamiento, pero más un uso más intensivo del procesador y puede requerir un procesador más rápido para mantenerse al día con los volúmenes de tráfico.

Ambos enfoques normalmente requieren una importante capacidad de almacenamiento de datos y el primer enfoque puede también dar lugar a posibles problemas de privacidad, ya que "los datos del usuario final" puede ser inadvertidamente capturados y almacenados, y pueden estar en contravención con la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA)56, ya que podría ser considerado como espionaje o divulgación de contenido interceptado, esto si no se obtiene el permiso del usuario.

En el contexto de la cláusula 7.2: Dispositivos de red, de la norma ISO/IEC 27037:2012, los dispositivos de red se consideran como ordenadores u otros dispositivos digitales que están conectados a una red, ya sea por medio de cables o de forma inalámbrica. Estos dispositivos de red pueden incluir los mainframes, servidores, computadoras de escritorio, puntos de acceso, switches, hubs, routers, dispositivos móviles, PDAs, dispositivos Bluetooth, sistemas de circuito cerrado de televisión y muchos más.

55 Simson L. Garfinkel es profesor asociado en la Escuela Naval de Posgrado en Monterey, California. Sus intereses de investigación incluyen análisis forense digital; privacidad; seguridad utilizable, y el terrorismo.

56 Electronic Communications Act. Ley de privacidad de las Comunicaciones Electrónicas de 1986 (ECPA) fue promulgada por el Congreso de Estados Unidos para ampliar las restricciones del gobierno sobre escuchas telefónicas de llamadas telefónicas e incluye las transmisiones de datos electrónicos por ordenador. Añadido nuevas disposiciones que prohíben el almacenamiento de las comunicaciones electrónicas, es decir, la Ley de comunicaciones almacenado (SCA)

Se debe tener en consideración que si los dispositivos digitales están conectados en red, es difícil determinar dónde se almacena la evidencia digital potencial que se busca, los datos podrían estar ubicados en cualquier lugar de la red.

La identificación de dispositivos digitales incluye componentes tales como marcas de fábrica, números de serie y adaptadores de corriente. El investigador debe considerar los siguientes aspectos al momento de la identificación: (27037, ISO/IEC, 2012)

- **CARACTERÍSTICAS DEL DISPOSITIVO:** la marca y el fabricante de los dispositivos digitales a veces pueden ser identificados por sus características observables, particularmente si existen elementos de diseño únicos.
- **INTERFAZ DEL APARATO:** El conector de alimentación es a menudo específico a un fabricante y es ayuda confiable para la identificación.
- **ETIQUETA DE DISPOSITIVO:** Al apagar los dispositivos móviles, la información obtenida desde el interior de la cavidad de la batería puede ser reveladora, sobre todo cuando se combina con una base de datos adecuada. Por ejemplo, el IMEI[57] es un número de 15 dígitos que indica el fabricante, el tipo de modelo y el país de aprobación de los dispositivos GSM[58]; el ESN[59] es un identificador único de 32 bits documentado en un chip seguro en un teléfono móvil por el fabricante - los primeros 8-14 bits identifican al fabricante y los bits restantes identifican el número de serie asignado.
- **BÚSQUEDA INVERSA:** En el caso de los teléfonos móviles, si el número telefónico del móvil se conoce, una búsqueda inversa se puede utilizar para identificar el operador de red.

Debido al pequeño tamaño de los dispositivos móviles, el investigador tiene que tener un cuidado especial al identificar todos los tipos de dispositivos móviles que puedan ser relevantes para el caso. El investigador necesita asegurar la escena del incidente y asegurarse de que no se extraen dispositivos móviles o cualquier otro elemento de la escena. Los dispositivos digitales que pueden contener evidencia digital deben protegerse del acceso no autorizado

[57] IMEI, (del inglés International Mobile Equipment Identity, Identidad Internacional de Equipo Móvil) es un código USSD pre-grabado en los teléfonos móviles GSM. Este código identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta.

[58] GSM, sistema global para las comunicaciones móviles (del inglés Global System for Mobile communications, GSM, y originariamente del francés groupe spécial mobile) es un sistema estándar, libre de regalías, de telefonía móvil digital.

[59] ESN (Electronic Serial Number), Número de Serie Electrónico, es un número de identificación permanente que se utiliza para reconocer los dispositivos móviles que acceden a determinadas redes de telecomunicaciones. El ESN es asignado y encajado en un dispositivo de comunicaciones inalámbricas por el fabricante del dispositivo.

En algunas circunstancias, puede ser apropiado dejar los dispositivos de red conectados de modo que su actividad puede ser supervisada y documentado con la autoridad apropiada. Cuando esto no es necesario, los dispositivos deben ser recogidos como se describe a continuación:

- El investigador debe aislar el dispositivo de red cuando se asegure que no hay datos relevantes que puedan ser reemplazados por esta acción y no se produzca un mal funcionamiento en los sistemas primarios o funcionales (tales como en la gestión de las instalaciones del sistema de un hospital, controles de acceso o de plantas de producción, etc.). Esto puede hacerse desconectando los equipos de red de la red telefónica o la red de datos o deshabilitar la conexión con el punto de acceso inalámbrico.
- Antes de desconectar las redes cableadas, el investigador debe rastrear las conexiones con los dispositivos digitales y etiquetar los puertos para futuras reconstrucciones de toda la red. Un dispositivo puede tener más de un método de comunicación. Por ejemplo, un equipo puede ser cableado LAN, un módem inalámbrico y tarjetas de telefonía móvil; también se puede conectar a la red a través de Wi-Fi, conexiones Bluetooth o conexiones de red de telefonía móvil. El investigador debe tratar de identificar todos los métodos de comunicación y llevar a cabo actividades apropiadas para proteger contra la destrucción de la evidencia digital potencial.
- Se debe tener en cuenta que la desconexión de la energía eléctrica de los dispositivos conectados en red puede destruir datos volátiles tales como los procesos en ejecución, conexiones de red y los datos almacenados en la memoria. El sistema operativo del host puede ser poco fiable y reportar información falsa. El investigador debe capturar esta información usando métodos comprobados de confianza antes de desconectar la energía de los dispositivos. Una vez que el investigador se ha asegurado de que no se pierde la evidencia digital, las conexiones de los dispositivos digitales pueden ser removidas.
- La recolección tiene prioridad sobre la adquisición y se sabe que el dispositivo contiene una memoria volátil, el dispositivo debe estar conectado continuamente a una fuente de alimentación.
- Si el móvil está apagado, deberá ser empaquetado con cuidado; esto es para evitar el uso accidental o deliberado de las teclas o botones. Como medida de precaución, el investigador también debe considerar el uso de jaulas Faraday [60]o cajas blindadas o bolsas de transporte bloqueadoras de señal.

[60] Una jaula de Faraday es una caja metálica que protege de los campos eléctricos estáticos. Este fenómeno, descubierto por Michael Faraday, tiene una aplicación importante en aviones o en la protección de equipos electrónicos delicados, tales como discos duros o repetidores de radio y televisión situados en cumbres de montañas y expuestos a las perturbaciones electromagnéticas causadas por las tormentas puede ser un dispositivo activo o pasivo.

- Bajo algunas circunstancias, los dispositivos móviles deben estar apagados con el fin evitar que los datos se cambien. Esto puede ocurrir a través de comandos entrantes y salientes o que pueden causar la destrucción de la evidencia digital potencial.

Posteriormente, cada uno de los dispositivos digitales debe tratarse como si fuera un dispositivo independiente hasta que sea examinado. Durante los exámenes, se debe considerar como un dispositivo de red.

TEMAS A CONSIDERAR CUANDO SE TRATA DE DISPOSITIVOS DE MANO

Cuando se trabaja con un dispositivo de mano o portátil, existe una serie de consideraciones adicionales que deben considerarse para garantizar que cualquier evidencia que contienen sea capturada de una manera que la haga utilizable en cualquier acción penal o civil. El término "dispositivo portátil" se utiliza para describir una gama de dispositivos que continúa expandiéndose, incluye organizadores electrónicos, asistentes digitales personales (PDA), teléfonos móviles (celulares) y cada vez más dispositivos, ya que se reducen sus tamaños.

Además de los tipos de dispositivos que se detallan anteriormente, una serie de otros dispositivos electrónicos entran en el grupo de mano, los que pudieran presentarse durante las búsquedas, estos pueden contener elementos de prueba pertinentes para la investigación; estos tipos de dispositivos incluyen buscapersonas, cámaras digitales y reproductores MP3 y MP4[61].

Los organizadores electrónicos y PDAs van desde dispositivos muy pequeños y muy baratos que pueden contener cualquier cosa; desde un par de entradas telefónicas hasta dispositivos caros que tienen tanto poder de procesamiento y de almacenamiento como el de una PC de escritorio. Estos dispositivos funcionan en una gama de sistemas operativos, como Linux, Windows, Palm OS.

Los teléfonos móviles (celulares) van desde dispositivos capaces de realizar llamadas telefónicas y el almacenamiento de una pequeña lista de números telefónicos hasta los dispositivos 3G[62].

A pesar de la amplia gama de hardware y sistemas operativos, todos los dispositivos de mano ofrecen un nivel similar de funcionalidad.

[61] MP4, MPEG-4 Parte 14 son archivos AAC, que tienen la extensión .mp4

[62] 3G, es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles).

En algunos de los dispositivos, la memoria es volátil y se mantiene activa por la batería. Si esto no funciona o se deja de cumplir íntegramente, toda la información contenida en el dispositivo se puede perder. Sin embargo, incluso si esto pasa puede ser posible recuperar datos de la memoria flash.

Otros dispositivos tienen dos juegos de baterías. La batería principal se utiliza para ejecutar el dispositivo cuando está activada, mientras que una batería de reserva mantiene la información en la memoria, siempre y cuando la batería principal falla o se descargue por completo. Cuando se deba confiscar dispositivos de mano, se debe tener el asesoramiento de especialistas en la primera etapa, esto con el fin de poder determinar la forma más adecuada de manejar y almacenar el dispositivo.

Con los dispositivos de mano, una consideración especial que se debe tener es el aislamiento del dispositivo de la red, esto con el fin de evitar que los datos almacenados en ella, puedan ser alterados o eliminados como resultado de la conexión a una red.

La información almacenada en un dispositivo de mano es probable que se encuentre en la memoria volátil, por lo que una de las acciones primarias es hacer procedimientos en el lugar del hallazgo, con el fin de garantizar que la evidencia almacenada en la memoria principal sufra el menor cambio posible. Todos los cambios que se producen deben tener lugar con el conocimiento de lo que está pasando internamente en el dispositivo.

INVESTIGACIÓN EN CALIENTE[63]

Este término describe la recopilación de posibles pruebas en tiempo real, mientras que los ordenadores y los servidores se están ejecutando. El uso de la investigación en caliente podría proporcionar la oportunidad de reunir pruebas que de otro modo se perdería y puede dar la oportunidad de identificar a los grupos de personas que se están comunicando y pueden estar trabajando juntos. El potencial para capturar esta información ha dado lugar a un cambio hacia la forensia digital en caliente, tanto en el gobierno y el sector privado. Los tipos de información que puede ser recopilada incluye los procesos en ejecución, mensajes de correo electrónico recientes, sitios Web visitados recientemente y salas de chat.

La investigación en caliente trata sobre la extracción y el examen de los datos forenses volátiles que se perderían si el dispositivo llegara a ser apagado. No es una disciplina forense "pura", en la definición formal, ya que el uso de la investigación en caliente tendrá un impacto menor sobre el estado operativo subyacente del dispositivo. Esta es una de esas excepciones a los principios básicos forenses

[63] La investigación en caliente también conocida como investigación en Vivo; se caracteriza porque se realiza en un equipo que se encuentra activo y funcionando

digitales, donde los cambios se deben realizar con el fin de recuperar la información, la clave es que el impacto de las acciones emprendidas sea conocido y que esas acciones estén totalmente documentadas.

Hay una serie de factores que se deben considerar para realizar el análisis forense en caliente, estas van desde la captura y recuperación de la información de sistemas que se consideran críticos para el negocio y que no puede ser apagado pero que se debe tener acceso a los sistemas de archivos cifrados mientras están todavía accesibles. Esos sistemas definidos como críticos para el negocio se verán afectados por el tipo de análisis a realizar sino fuera en caliente.

Otro motivo para la realización de análisis forense en caliente incluye la recuperación de información de los sistemas donde un corte de corriente en el sistema pueda crear una responsabilidad legal para el investigador o un costo comercial inaceptable. Estos pueden aumentar como resultado de las operaciones, la pérdida no intencionada de datos, o daño de equipo, o cuando la evidencia debe ser obtenida de la manera menos intrusiva.

Este tipo de análisis debido a su naturaleza deben ser aprobados por los administradores de los sistemas, quienes son los que asumen los riesgos derivados del análisis o en el caso de una acción legal, la cual está respaldada por una orden judicial, es esta la que ordena la ejecución del análisis en caliente.

Los datos en un sistema tienen diferentes niveles de volatilidad. Todos los datos en una memoria principal son volátiles, ya que son datos del sistema en vivo. Normalmente, los datos de la memoria, el espacio de intercambio, procesos de red, y los sistemas que ejecutan procesos son los más volátiles y se perderán si se reinicia el sistema. Siempre que recoja los datos, es conveniente recoger los datos más volátiles primero y luego proceder a lo que es el menos volátil. El orden de la volatilidad (tal como se define en el RFC 3227[64]) es:

1. Memoria
2. Intercambio de archivos
3. Proceso de Red
4. Sistemas de proceso
5. Archivo de información del Sistema

[64] Reference for Comments 3227 (Referencia de Comentarios 3227) – Directrices para la recopilación de evidencias y su almacenamiento

RAZONES PARA REALIZAR UNA INVESTIGACIÓN

Varias razones existen para llevar a cabo una investigación forense digital y éstos dependerán, en parte, en el tipo de organización a la cual pertenece. Los tipos más comunes de investigación incluyen:

- Las investigaciones penales
- Investigaciones de litigio civil
- Descubrimiento de datos
- La recuperación de datos

INVESTIGACIONES PENALES

Las investigaciones penales, históricamente, son consideradas competencia de las entidades de aplicación de la ley tales como la Fiscalía General de la Republica (FGR) y la Policía Nacional Civil (PNC). Si bien esto es comprensible, es incorrecto, y estos temas se están convirtiendo cada vez más importantes. Todas las investigaciones, sea cual sea la motivación inicial para instigar a ella, deben ser tratadas de la misma manera.

Si los procesos y los procedimientos correctos no se han utilizado desde el principio, cualquier información recogida puede estar contaminada e inutilizable. Los ejemplos de los tipos de actividades comúnmente consideradas de causa penal incluyen:

- La piratería
- El fraude
- Distribución de virus
- El acoso
- El chantaje
- Estafa por medios informáticos
- Pornografía infantil en medios tecnológicos

LAS INVESTIGACIONES DE LITIGACIÓN CIVIL

El tipo de actividad que normalmente cae en la categoría de investigación de litigio civil incluye investigaciones disciplinarias internas para reunir pruebas de uso indebido del sistema y el abuso, o el comportamiento inadecuado que dará lugar a procedimientos disciplinarios internos y potencialmente el despido de un miembro del personal. Incluso en este tipo de investigación, siempre debe tomarse en cuenta que si se discute el caso, puede ir a un tribunal y una vez más, los procesos y procedimientos utilizados deben mantenerse apegados a la misma norma que se aplica a cualquier investigación criminal.

DESCUBRIMIENTO DE DATOS (E-DISCOVERY)

Descubrimiento electrónico de datos (e-discovery) se ha vuelto cada vez más importante y forma parte de los procesos de descubrimiento civil. Estudios recientes han indicado que más del 90 por ciento de todos los documentos elaborados desde 1999 han sido creados en un formato digital.

Elementos del proceso de e-discovery incluyen la preservación de las pruebas electrónicas, la creación de un repositorio de todos los archivos digitales, y un sistema de recuperación de documentos en base a los términos de búsqueda definidos. El alcance de la actividad normalmente cubierta por e-discovery incluye el correo electrónico y los documentos almacenados en equipos individuales y los servidores de red, así como otros dispositivos.

Muchos abogados siguen sin llevar a cabo el descubrimiento electrónico debido a las preocupaciones sobre el costo, el tiempo que se necesita, y la complejidad de este tipo de empresas, y por lo tanto no logran apreciar que en comparación con el descubrimiento de información no digital, e-discovery es mucho más costo-efectiva. Con la digitalización de todos los aspectos del negocio, que ha tenido lugar durante la última década más o menos, en la actualidad es un increíble volumen de pruebas electrónicas disponible que se puede recoger, conservar, documentar, y autenticar. Los tipos de casos en los que la evidencia generada por computadora es típicamente relevante incluyen:

- Difamación
- Robo de propiedad intelectual
- Acoso sexual en el lugar de trabajo
- Fraude
- Incumplimiento de contrato.
- Demandas por lesiones personales
- Disputas salariales

RECUPERACIÓN DE DATOS

Muchas veces los datos se pierden por una variedad de razones; las unidades de disco a veces fallan, ya sea como resultado de fallas mecánicas o electrónicas o debido a la corrupción de los datos. Los datos también se pueden perder como resultado de los usuarios, siendo malicioso o cometiendo errores.

Las tareas de recuperación de datos pueden incluir la recuperación de datos que se perdieron como resultado de:

- Problemas de lógica, como tablas de partición dañados o destruidos, los sectores de arranque, o tablas de asignación de archivos (FAT[65])
- Los problemas mecánicos, tales como unidades de disco duro que no funcionan debido a los accidentes en los cabezales, donde las cabezas de lectura/escritura del disco se han atascado en una posición o han hecho contacto con la superficie de un disco o falla al volver a acelerarse porque, por ejemplo, el lubricante en el husillo[66] se ha endurecido.
- Actividades maliciosas o errores por parte de los usuarios, tales como la eliminación de datos, el formateo de los discos o la eliminación de las particiones.
- Software malicioso como virus y/o caballos de Troya.
- Contraseñas olvidadas
- Daño físico a los discos, como resultado de acontecimientos externos, como golpes, incendios e inundaciones

Las tareas de recuperación de datos implican la recuperación de todos los datos que han sido identificados como necesarios y relevantes. Esto puede ser todo o simplemente una pequeña parte de los datos disponibles sobre los medios de comunicación.

En estos casos la cadena de custodia debe seguir los pasos establecidos en los procedimientos de recolección, tales como Registrar todas las acciones, Grabar la escena, Grabar la información en pantalla, Etiquetar los puntos de red y cables, Comprobación de contraseñas (Referirse al Capítulo 3, sección Procedimientos)

EL SERVICIO TRIAGE FORENSICS[67]

El Triage o muestreo forense Ha sido diseñado para ser usado en aquellas ocasiones en las que es necesario obtener un procesamiento rápido inicial cuando hay un gran volumen de información a procesar, este servicio permite recolectar de una forma directa, sin generación de imagen forense y manteniendo la integridad de la información obtenida; elementos específicos como imágenes o gráficos, archivos con palabras específicas en su nombre o en su contendido, archivos por tipo y toda información siempre y cuando esté perfectamente definida.

ALCANCES:

[65] FAT, Tabla de asignación de archivos, comúnmente conocido como FAT (del inglés file allocation table), es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me

[66] Un husillo es un tipo de tornillo largo también llamado, tornillo sin fin, utilizado para accionar los elementos de apriete de las cabezas lectoras de discos duros.

[67] Triage Forensic se traduce como muestreo Forense

El Triage Forensics se realizará en un equipo de cómputo con el propósito de obtener la información específica siguiendo las mejores prácticas del cómputo forense manteniendo la integridad de la información obtenida. El Triage Forensics se enfoca en la obtención de:

- Información de la navegación por Internet
- Información del software instalado
- Información del sistema
- Actividad de los usuarios
- Datos a partir de patrones, nombres de archivos, hashes o palabras contenidas en el mismo

EJEMPLOS DE USO:

- Cuando existen múltiples computadoras a analizar para identificar cuál de ellas contiene información relevante para un caso de investigación, se realiza el Triage Forensics para identificar aquellas que posteriormente se les realizará una imagen forense.
- Cuando es necesario preservar evidencia digital específica (archivos o imágenes) contenidas en una computadora.
- Cuando se busca obtener información valiosa en la memoria volátil (como contraseñas) de un equipo encendido.

El Triage Forensic no elimina el análisis tradicional sino que lo complementa ya que este permite identificar de forma rápida un gran número de evidencias, las cuales podrían ser de interés para posteriormente ser procesadas formalmente, sirve como un análisis previo en donde se determina los elementos a tratar primero.

RESUMEN

En este capítulo se ofreció una introducción al análisis forense digital y del por qué es necesario, su definición fue cubierta, así como su relación con la ciencia y la ley, se ha introducido una serie de temas que deben ser considerados en la gestión o en la implementación de sistemas de información enfocados al análisis forense digital.

Además se han discutido los motivos para efectuar una investigación forense digital y el tipo de investigaciones que puedan llevarse a cabo. La razón de cubrir estos temas es poner en relieve la variedad de tipos de investigación que en un laboratorio digital pueden involucrarse y el número de decisiones necesarias que se deben tomar a consideración por parte del investigador forense, estas decisiones son particularmente importantes en las primeras etapas de una investigación para asegurarse de que los datos correctos se capturan y se recolectan de la forma apropiada.

Si la investigación forense digital no se gestiona desde el principio, el esfuerzo, recursos y el objetivo no se puede lograr. Es esencial que el administrador del laboratorio ponga en marcha las herramientas, procesos y procedimientos necesarios para una buena investigación forense, y asegurarse que el personal a cargo esté debidamente entrenado y capacitado para realizar una investigación efectiva.

DISEÑO DE LABORATORIO FORENSE DIGITAL

CAPÍTULO 4: EL ESTABLECIMIENTO Y LA GESTIÓN DEL LABORATORIO FORENSE DIGITAL

INTRODUCCIÓN

Esta sección describe cómo establecer y gestionar un laboratorio forense digital, la creación y gestión del laboratorio debe satisfacer las necesidades actuales y futuras de las organizaciones cada vez más dependientes de la tecnología tanto a nivel público como privado, es algo que se debe idear y planificar considerablemente, ya que las consecuencias financieras y los recursos son significativos. Una de las primeras variantes en una planificación a considerar son las consecuencias financieras y los recursos a utilizar, es por ello que se debe tener en cuenta para la gestión de este tipo de áreas, si los recursos de este departamento serán completamente dedicados al área o si será posible colaborar y compartir recursos con otras áreas que contengan los requisitos y las mismas capacidades que soportaran el laboratorio forense digital.

La capacidad y recursos a compartir pueden ser un tanto deseables y esenciales según el tipo de organización, por ejemplo la unidad de análisis forense digital en una institución como La Fiscalía General de la Republica (FGR) o en la Policía Nacional Civil (PNC) en donde el desarrollo de la investigación necesita el apoyo calificado en todos los niveles. Este tipo de visión cambiaría significativamente en el sector privado, pero se debe tener el objetivo de ofrecer el mismo valor que corresponde al área de análisis forense digital en cualquier organización. Para la creación de esta unidad es fundamental el ámbito que tendrá en la organización, así como el desarrollo de un plan de negocios que involucre el área de análisis forense digital.

Por ejemplo en el Reino Unido, la Asociación de Jefes de Policía (ACPO), un grupo que representa a todos los cuerpos de la policía local, creó "*el Asesoramiento y Guía de Buenas Prácticas para los gerentes de las Unidades de Delitos Informáticos Hi-Tech*"[68]. Este documento fue publicado en 2005 y fue desarrollado para dar orientación y asesoramiento sobre cuestiones relacionadas con la creación de un laboratorio forense digital para una organización policial, el documento proporciona una buena base que se fundamenta en años de experiencia en aplicación a la ley, en la creación y gestión de los

[68] In the United Kingdom, the Association of Chief Police Officers (ACPO), a group that represents all of the local police forces, created the Advice and Good Practice Guide for Managers of Hi-Tech/ Computer Crime Units. http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf

laboratorios forenses digitales y que han sido aprobados por organizaciones mundiales. Como resultado, proporciona una guía de temas que se deben abordar en la creación de un laboratorio relacionado a cualquier sector organizacional. Las principales consideraciones que se deben de tener en cuenta antes de llevar acabo un laboratorio forense digital son:

- El impacto
- La probabilidad de éxito
- El costo de la inversión para este tipo de unidades.

Siempre hay que tener en cuenta que, si el laboratorio no está configurado correctamente desde un inicio, o se gestiona mal después de su creación, es probable que cualquier material procesado en el laboratorio no cumpla con las regulaciones pertinentes y buenas prácticas establecidas, y de esta forma el resultado de una investigación estaría contaminada o viciada. Esto significa que podría ser susceptible de ser impugnada en un procedimiento penal o civil, ya que se basan en la evidencia producida de un laboratorio mal gestionado.

ESTABLECIMIENTO DEL LABORATORIO

La creación de un laboratorio forense digital no es un tema trivial, dependerá de una serie de factores y restringido por una serie de normas y reglas. Como se mencionó anteriormente, el costo inicial de la creación de un laboratorio forense digital y el costo de mantenerlo es probable que sea relativamente alto, especialmente cuando se está introduciendo como una nueva función dentro de una organización. El primer problema que deberá ser superado (suponiendo que el laboratorio no se está estableciendo como el resultado de un requisito interno o externo) será convencer a la dirección de la organización que la inversión es necesaria y deseable, esto de acuerdo a las necesidades de las capacidades forenses dentro de la organización.

Los parámetros que puedan ayudar a convencer a la alta gerencia son las exigencias de los cambios normativos y la proliferación de tecnologías que hacen que la creación de la unidad del laboratorio forense digital sea un requisito o una decisión empresarial sensata. Otro factor que apoyaría la iniciativa será el desarrollo de un modelo financiero que pueda demostrar que la creación de un laboratorio forense digital será proporcionar un retorno de la inversión (ROI)[69]. Esto podría lograrse mediante la demostración de que el trabajo que se lleve a cabo en el laboratorio hará un costo neutral en términos de la reducción del costo de la organización que lleva a cabo su actividad principal. Esto

[69] El retorno sobre la inversión (RSI o ROI, por sus siglas en inglés) es una razón financiera que compara el beneficio o la utilidad obtenida en relación a la inversión realizada, es decir, representa una herramienta para analizar el rendimiento que la empresa tiene desde el punto de vista financiero.

puede ser a través de la reducción de pérdidas, seguro más bajos, siendo capaz de demostrar el cumplimiento de los reglamentos, o ser el resultado de incrementar el valor de alguna otra función o servicio dentro de la organización. Otra forma en la cual un retorno de la inversión puede ser recuperado es mediante la demostración de que los servicios o instalaciones del laboratorio pueden ser utilizados por terceros.

El mensaje principal es que antes de iniciar la identificación de los equipos y de sus necesidades, se debe establecer principalmente la gestión del laboratorio, los principales requisitos y el alcance de las tareas que el laboratorio llevará a cabo.

El primer paso para el desarrollo de la creación del laboratorio será identificar las respuestas a una serie de preguntas. El tipo de preguntas que deben ser contestadas son las siguientes: (Andy Jones & Craig Valli, 2009)

- ¿Qué tipos de actividades se realizaran en laboratorio forense digital?
- ¿Por qué se necesitan?
- ¿A qué tipo de cliente ira orientado?
- ¿Cuál son las problemáticas que se tienen actualmente?
- ¿Cuál será el alcance del trabajo a realizar en el laboratorio?
- ¿Cuál es el presupuesto requerido?
- ¿Cuál es el presupuesto disponible?
- ¿Cuál será el volumen de casos a procesar?
- ¿Sera discriminado por especialidad?

Sin respuestas específicas a estas preguntas y otras que estarán dadas por el tipo de organización a la que se brinde el servicio, la función del laboratorio no alcanzara su verdadero potencial.

Por ejemplo para responder a la primera de estas preguntas sobre el tipo de actividad que se realizará en el laboratorio forense digital, se deben tener claro los siguientes requisitos:

- El laboratorio será utilizado por entidades como la Policía Nacional Civil (PNC) que supongan un delito penal y deberá ser investigado
- Será utilizado por los proveedores de servicios legales para la investigación civil
- Sera utilizado dentro de una organización para el personal de seguridad de TI para investigar casos penales y civiles
- Va a ser utilizado por otros investigadores corporativos como el Departamento de Talento Humano para la investigación en la selección del personal

- Va a desempeñar un papel de consultoría externa para investigadores privados o para consultores de seguridad informática externos en respuesta a incidentes

Puede ser que el laboratorio se utilice en más de una de estas áreas y es sólo con la claridad de la comprensión de producir un modelo de negocio coherente para el desarrollo de las prácticas de laboratorio forense digital.

EL ROL DEL LABORATORIO FORENSE DIGITAL

Si el laboratorio es rentable y logra su potencial, se debe tomar una serie de pasos antes de que comience la operación. Una de las primeras acciones que se necesitan llevar a cabo es el desarrollo de los términos de referencia[70]. Esto, en mayor parte, se deriva de la lógica utilizada del tipo de organización y delineará la base de clientes que soportará el laboratorio, así como las funciones de la administración y las personas asignadas al laboratorio, se debe identificar (por escrito) las descripciones de puestos y responsabilidades individuales. Los términos de referencia también ofrecerán una orientación sobre el alcance de las actividades que el laboratorio forense digital llevará a cabo.

Una vez que se han desarrollado los términos de referencia para el laboratorio, se deberán identificar las funciones, deberes y responsabilidades de los miembros del laboratorio. Algunos ejemplos de los derechos que deben ser considerados en los roles respectivos de todos los miembros del laboratorio se detallan en organizaciones profesionales, como la Sociedad Americana de Directores de Laboratorios Crimen (ASCLD)[71] y, en el Reino Unido, la ACPO[72] la Guía de Buenas Prácticas.

EL PRESUPUESTO

El primer elemento del presupuesto que se requiere para establecer el laboratorio será lo que la mayoría de las organizaciones llaman costo de capital[73], este es el gasto que incluye el costo de la compra de los equipos, software, la obtención y renovación del establecimiento. Estos son los costes requeridos para obtener la infraestructura, el equipo y ponerlo en un estado de operación.

[70] Los Términos de referencia contienen las especificaciones técnicas, objetivos y estructura de cómo ejecutar un determinado estudio, trabajo, proyecto, comité, conferencia, negociación, etc.
[71] American Society of Crime Laboratory Directors, www.ascld.org
[72] Association of Chief Police Officers (ACPO), http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
[73] El coste del capital es el rendimiento mínimo que debe ofrecer una inversión para que merezca la pena realizarla desde el punto de vista de los actuales poseedores de una empresa.

El segundo elemento del costo será para gastos como gastos de alquiler, mantenimiento del establecimiento, el sueldo del personal y su formación, los gastos en curso como el mantenimiento, modernización, renovación de equipos y licencias de software.

El presupuesto dependerá de la fortaleza del modelo de negocio que se ha presentado, así como la prioridad y la cantidad que la organización puede permitirse. Si la cantidad asignada por la organización no es tan alta como la que exige el modelo de negocio, será necesario revisar el alcance de las tareas del laboratorio y modificar el nivel de capacidad del servicio que puede ofrecer, para revaluar el presupuesto y plantearlo a la alta gerencia de manera más persuasiva o para encontrar una fuente alternativa de ingresos para apoyar el laboratorio.

Cuando se hayan explorado todas las problemáticas y tener respuestas para cada una de ellas, entonces se podrá comenzar a preparar la creación del laboratorio forense digital. Una serie de consideraciones, como el tamaño y el tipo de laboratorio, dependerá de las respuestas que se han obtenido en la investigación del modelo del negocio.

ADMINISTRACIÓN DEL LABORATORIO FORENSE DIGITAL – LA CONSIDERACIÓN DEL PERSONAL

Es probable que la persona que realice la planificación de negocios sea el primer director del laboratorio forense digital o estará muy involucrado en la selección del gerente del laboratorio. Una vez que el gerente ha sido identificado, esta persona será fundamental para el desarrollo de las funciones necesarias y cumplir con las tareas del laboratorio, además estará involucrada de la selección del personal que asistirá en las actividades del laboratorio.

Dependiendo del tamaño del laboratorio y de la finalidad por el cual fue creado, se requerirá una serie de habilidades para realizar las funciones acordes a las necesidades del laboratorio, las funciones estarán dadas como resultado de la identificación de requisitos del laboratorio establecido en la etapa de planificación. Algunas de las habilidades requeridas serán prioridad en la fase de la selección del personal y del reclutamiento, pero otras habilidades se brindarán en la fase de capacitación del personal para evolucionar la experiencia práctica. Es esencial que en esta primera etapa de la planificación de las funciones y sus responsabilidades sean documentadas desde un principio, ya que guiará la selección del personal y asegurara que las personas seleccionadas tendrán una comprensión clara de su rol dentro el laboratorio.

CONSIDERACIÓN DEL PERSONAL – LOS NIVELES DEL PERSONAL Y SUS ROLES

Dependiendo del tamaño y el propósito del laboratorio a ser creado, algunas funciones que puedan necesitar a tenerse en cuenta son las siguientes:

ADMINISTRADOR DEL LABORATORIO

Un papel clave en el laboratorio, el director del laboratorio será responsable de todos los aspectos de la gestión del laboratorio, esto incluirá todos los asuntos relacionados con el personal, como el reclutamiento, entrenamiento, tutoría, consejería, orientación ética[74], recompensas, y las retenciones. También será responsable de la planificación financiera, la contabilidad, la gestión y adquisición del equipo y del software, la asignación de tareas, el cumplimiento de las normas y el costo-efectividad de la práctica del laboratorio. Un buen gerente del laboratorio tendrá un enorme impacto en la eficacia del laboratorio y deberá ser seleccionado con cuidado.

OFICIAL DE RECEPCIÓN

El oficial de recepción es efectivamente el líder de laboratorio y será reconocido como el "punto de contacto" dentro de ella, siendo la persona responsable en la gestión de la interfaz con los clientes. Esta es la persona que va a tratar, en un principio, con los investigadores y quién decidirá qué tareas són aceptadas en el laboratorio. Esta persona también será responsable en la interfaz con cualquier representación fuera de la organización (por ejemplo, un experto de la defensa o representante legal), que puede requerir el acceso al laboratorio, al personal, o los elementos específicos de las pruebas. Para asegurarse de que se toma un enfoque coherente cuando se trata de personas externas al laboratorio, es esencial que siempre que sea posible, sólo una persona lleve a cabo esta función de coordinación, el oficial de recepción tendrá que tener un buen conocimiento del proceso de investigación y ser capaz de traducir las solicitudes de los investigadores en tareas realistas para el laboratorio, de este modo, el oficial de recepción tendrá que tener buenas habilidades interpersonales así como de comunicación.

OFICIAL DE PRIORIDADES

El oficial de prioridades es la persona que será responsable de decidir si las tareas son aceptadas en el laboratorio, o no lo son, para definir la asignación de las prioridades en los casos que deben ser tratados. Al igual que el oficial de recepción, el papel del oficial de prioridades requiere un carácter

[74] La enseñanza de la ética en esta ciencia; la informática forense, es poder inculcar el deseo y la voluntad de ser ético en los estudiantes y profesionales como parte de algo natural y de interrelación para poder contribuir con las buenas prácticas de profesionales responsables y éticos.

robusto, con buenas habilidades interpersonales y un buen conocimiento tanto del proceso de investigación como el rol del investigador.

OFICIAL DE COPIA DE IMÁGENES

Este rol describe a cualquier persona que sea responsable de la creación de la copia (imagen) de los medios de comunicación incautados y asegurar que las imágenes se crean de manera válida a efectos legales. Dependiendo del tamaño del laboratorio y la diversidad de las tareas, esta función puede ser realizada por una sola persona o varias, cada una de las cuales pueden especializarse en un producto de plataforma o software específico. Será preciso que el oficial de las copias de imágenes este bien capacitado, tener experiencia en la obtención de imágenes de los medios de comunicación, deba tener un buen conocimiento de la legislación y puntos de contacto tanto en el país de origen como en otros países en los que puede ser localizada algún tipo de evidencia.

EL ANALISTA

Esta es la persona que será responsable del análisis del material disponible y de garantizar que cualquier resultado que se presente este en forma clara y comprensible y que puede ser reproducido por cualquier persona que necesite hacerlo. Durante el curso del análisis, tratará de encontrar información útil o pruebas que se relacionen con la investigación actual, también deberá descubrir información que se relacione con otros incidentes o delitos no conocidos en el momento en el que fue incautado el material a investigar. El analista con formación y experiencia, debe ser capaz de informar a la gerencia y a los clientes sobre el progreso del análisis. El analista requerirá un conocimiento en profundidad tanto de hardware como de software, deberá tener buena capacidad de análisis, así como buenas habilidades de comunicación oral y escrita.

Dependiendo del tamaño y el alcance de las tareas del laboratorio, una o más de estas funciones se puede combinar, y no sería inusual que el director del laboratorio actuara también como el oficial de recepción, el oficial de prioridades, el oficial de copia de imágenes o también de llevar a cabo el rol del analista.

Es necesario comprender que para tener éxito, uno de los temas importantes que se tratará será el de la selección del personal para el laboratorio forense. Se necesitara tener una idea clara de la finalidad y la función del laboratorio y los roles que se han identificado para ser capaz de seleccionar el personal adecuado con la combinación adecuada de habilidades y las experiencias necesarias. Una vez establecido el laboratorio y se ha seleccionado al personal, se tendrán que tener una serie de competencias que reúna los siguientes aspectos:

- Comprensión de los procesos legales

- Una amplia gama de conocimientos a nivel de hardware y software, incluyendo teléfonos móviles, PDAs, ordenadores, redes, sistemas de comunicación, entre otros
- Buena comunicación tanto oral como escrita
- Buena administración

Además de las competencias anteriores se requerirán otras habilidades, no mencionados en este momento, lo que se ha pretendido es dar una idea de la gama de habilidades requeridas en un laboratorio forense digital.

La clave en este apartado es de realizar un reclutamiento y selección de personal adecuado, ya que es importante y vale la pena invertir esfuerzos en conseguir la mezcla correcta de personal idóneo. Además de la recopilación y el desarrollo de las habilidades correctas, el personal debe trabajar y funcionar como equipo ya que a menudo se trabajarán en ambientes difíciles de alta presión. También vale la pena tener en cuenta desde un principio, las medidas que se pondrán en marcha para motivar y retener al personal, dada que la inversión es importante, el nivel de esfuerzo, la financiación en el reclutamiento, la educación y formación de habilidades, por el hecho que hay una escasez general de experiencia y personal cualificado disponible en el mercado laboral, por lo que estos profesionales en cualquier momento cumplirán también funciones diversas fuera de su campo de destrezas.

ASIGNACIÓN DE TAREAS

Con el fin de garantizar el mejor uso de los recursos disponibles y asegurarse de que las cargas de trabajo del personal dentro del laboratorio se distribuyen de manera uniforme, es importante que los niveles individuales de experiencia se desarrollen continuamente. Esto ayudará a asegurar que existe suficiente personal capacitado, lo que permitirá que en ausencias, las tareas sean realizadas con normalidad. El entorno forense digital puede ser estresante y para asegurar que el laboratorio está funcionando de manera eficiente y que el personal se utiliza de manera eficaz en las tareas correspondientes, se debe asegurar que se tiene en cuenta la asignación justa y apropiada de funciones dentro del laboratorio.

FORMACIÓN Y EXPERIENCIA

Una vez que las tareas a desarrollar en el laboratorio se han definido, se decide el software y el hardware que se utilizará para realizar el examen forense en las pruebas incautadas. Será esencial garantizar que el personal este recibiendo formación adecuada y tener suficiente experiencia en el uso de todas las herramientas tanto a nivel de hardware como software. Nunca se debe poner al personal en la posición de tener que defender los resultados de la investigación o dar fe de los hechos si no han recibido una formación adecuada sobre el uso del software y mucho menos si no posee la

experiencia adecuada. Se recomienda adoptar certificaciones o acreditaciones profesionales reconocidas a nivel mundial en actividades relacionadas a la investigación de la evidencia digital.

Se debe tomar en cuenta que al establecer los presupuestos, el hecho de que la formación es un ciclo continúo y no un único evento. Para que el laboratorio tenga credibilidad y pueda satisfacer las demandas que se pondrán en él, el personal tiene que operar con eficacia y en continuo desarrollo de sus habilidades, para ello, deben tener acceso a un programa permanente de capacitación que tenga en cuenta los cambios en las tecnologías y de la evolución de las herramientas disponibles. Esto será costoso de implementar y mantener, deberá ser apoyado porque cualquier falla en el mantenimiento de las capacitaciones del personal dará lugar a un personal descalificado que no estará adecuadamente capacitado para poder llevar a cabo las tareas necesarias, y en última instancia llevará al fracaso de las actividades y roles que posea el laboratorio.

LA PRODUCTIVIDAD DEL PERSONAL Y EL LABORATORIO

En el desarrollo del inicio del modelo de negocio para la creación del laboratorio forense digital, se han realizado conjeturas en relación con los tipos de investigaciones que se realizarán y el volumen de trabajo previsto. La decisión con respecto a la dotación de personal para el laboratorio se basa en estas conjeturas y una evaluación de la carga de trabajo que cada miembro del personal será capaz de manejar. Si bien esto es una parte esencial de la planificación inicial y la justificación de los niveles de dotación de personal, la realidad es que, una vez que el laboratorio está en pleno funcionamiento, todas estas conjeturas será necesarias volverlas a examinar a la luz de la experiencia adquirida. El tipo de investigación es casi seguro que cambiará a medida que los clientes empiezan a comprender mejor la capacidad del laboratorio, y la carga de trabajo es casi seguro que aumentará por la misma razón. Asimismo, se debe considerar la posibilidad de que el laboratorio podría ser más rentable si también está apoyando a otros tipos de análisis o investigaciones, y no sólo los relacionados con delitos de alta tecnología. La carga de trabajo que el personal puede absorber también cambiará a medida que la experiencia del personal aumente, así como la familiaridad con las herramientas y el uso de equipos.

La productividad tanto individual como colectiva en las actividades del laboratorio debe ser monitoreada continuamente para garantizar que los miembros del laboratorio trabajen con eficacia y que el laboratorio funcione de manera eficiente. Una vez que el laboratorio ha estado en funcionamiento durante un período de alrededor de un año, se debe llevar a cabo una revisión de todos los factores que contribuyen a las actividades del laboratorio para determinar si deben realizarse cambios.

PROGRAMAS DE CAPACITACIÓN

Los programas de capacitación deberán ponerse a disposición del personal, toda el área de la ciencia forense digital puede ser muy estresante, sobre todo si el material siendo objeto de estudio se relaciona con delitos graves o siniestros, si la pornografía o la pedofilia están involucrados. Es esencial tener las políticas y acuerdos establecidos para los programas de capacitación del personal siempre que se consideren necesarios, se deberán tener programas de capacitación programadas en períodos predeterminados. El personal deberá asistir a los programas de capacitación para fomentar sus habilidades en las investigaciones y de esta manera ayudar a tomar medidas apropiadas en investigaciones difíciles. El programa de capacitación deberá ser respetado por todo el personal a cargo.

POLÍTICAS TERCIARIZADAS Y EXPERTOS EXTERNOS

Con la creciente diversificación de software y sistemas de hardware y una complejidad cada vez mayor en los tipos de sistemas a investigar, es poco realista creer que todas las habilidades y experiencia requeridas estarán disponibles en el laboratorio forense digital. La política que se utiliza en relación con la externalización de tareas (si hay un exceso de trabajo que se lleva a cabo o si las habilidades no están disponibles dentro el laboratorio) debe establecerse de antemano. Además, es probable que se tenga que subcontratar el trabajo, para esto los proveedores potenciales deben ser investigados por adelantado por cuestiones de tarifas, si son aceptables, si se ha comprobado sus habilidades, su integridad, su disposición en cualquier momento según sea el caso a investigar y si su adopción de normas se encuentra acorde a las políticas del laboratorio.

La política por la cual una organización o experto puede ser llamado, y cuándo, y en qué condiciones pueden ser llamados, y cuándo, y en qué condiciones se puede acoplarse también deben definirse con antelación para que el personal este claro en las expectativas de la organización. Al utilizar expertos externos, se debe tener cuidado en la contratación de "ex-hackers". Los hackers[75], phreakers[76], u otros malhechores no deben ser contratados como expertos externos independientemente de su experiencia o conocimiento. La realidad es que, sin importar sus habilidades o conocimientos, su

[75] Se podría decir que en un inicio los hackers fueron los constructores del manual de lo "no documentado" de la realidad que está inmersa en las soluciones de informática que aún no se descubre, o se escribe para que otros la observen, con el avance de los 80s se presentan los primeros enfrentamientos de grupos de hackers, a partir de este momento, el termino hacker paso de un título que se ganaba por sus méritos y logros diferenciadores, a uno que se asociaba con "vándalo o intruso informático" la cultura que con muchas horas de trabajo un grupo de mentes pensantes desarrollo, con logros científicos, se transformó en una cultura oscura que terminaría confinando la esencia del hacker.

[76] Un phreaker es un individuo que ha sido iluminado por la frecuencia de los tonos que emiten los dispositivos de comunicaciones, de las ondas hertzianas y los espacios electromagnéticos para distinguir los códigos que ellas llevan, que se traducen en números, indicaciones o llamadas que se hacen de un lugar a otro.

integridad y confiabilidad siempre será cuestionable y cuestionado por ejemplo, por un abogado defensor ante un tribunal.

REQUISITOS DEL ESTABLECIMIENTO

El tamaño físico del laboratorio es otro tema que debe abordarse en la etapa de la planificación. El tamaño del laboratorio se determina mediante el equilibrio entre lo que se desea y lo que se puede invertir. Lo esencial es que el laboratorio sea lo suficientemente grande como para cubrir el papel que se ha identificado en los términos de referencia. Otra cuestión que afectará al establecimiento será el lugar elegido para el laboratorio, esto probablemente se debe a varios factores: el centro de operaciones de la organización, la ubicación del personal disponible, la proximidad entre otras organizaciones o funciones (por ejemplo, el equipo de recuperación de desastres o el personal de auditoría), la seguridad y otros temas.

Se tendrá que tomar en cuenta que la instalación tendrá que tener un nivel mayor de seguridad, para lograr esto y mejorar la capacidad de resistencia del laboratorio como los desastres naturales, daños accidentales, se debe evitar la ubicación en un sótano o en una planta baja. Por otra parte, se debe evitar la ubicación del laboratorio en la planta superior de un edificio de gran altura ya que a menudo tienen que moverse los equipos pesados y voluminosos.

También se debe tener en cuenta la cantidad de personal que pueda permanecer en el laboratorio y los tipos de procedimientos que se espera llevar a cabo en su interior. La planificación inicial debe tratar de proyectarse hacia el crecimiento y de esta manera cubrir con el suficiente espacio para el personal del laboratorio, el área de trabajo que permita el desmantelamiento de sistemas, el almacenamiento de equipos, área de realización pruebas, áreas de descanso, área de reuniones, entre otros. Si es probable que para casos de carácter especialmente sensibles el laboratorio necesite una habitación que este separado de la zona principal del laboratorio con el fin de reducir al mínimo el número de personas que podrían tener acceso a la información como resultado de las investigaciones.

El tipo de información que puede constituir la información confidencial podría incluir información estatal, material clasificado, información corporativa sensible, información sobre el personal, transacciones financieras o material sexualmente explícito.

Cuando en el laboratorio se trabaje con información sensible, los planes y procedimientos para abordar este tipo de trabajo se deben poner en marcha, estos mecanismos deben ser considerados de antemano para tratarlos sin ninguna interrupción. El tipo de medidas que se pueden considerar comprende un área de proceso separado, el registro al área, la auditoría de acceso al material, la "regla

de los dos hombres" donde una persona no tiene acceso exclusivo al material y separa en un almacenamiento seguro los datos de los archivos del material y cualquier otro documento producido por él.

El laboratorio deberá estar precisamente equipado y localizado en un nivel adecuado de seguridad para poder llevar a cabo el trabajo. Esto variará de una organización a otra y también puede cambiar con el tiempo según la credibilidad del laboratorio para volverse más "confiable".

Un laboratorio en general necesitara contar con las siguientes áreas:

- Área de recepción y almacenamiento
- Área de reuniones y espera
- Área de descanso y cafetería
- Almacenamiento de equipos y posesiones personales
- Área de imágenes
- Área de desmontaje
- Área de almacenamiento seguro
- Área de investigación sensible
- Área de escaneado
- Área de análisis
- Oficina de administración

Se requerirá un número significativo de enchufes en cada área de trabajo, también será necesario un número de puertos de red para la red de laboratorios, pero éstos deben ser cuidadosamente considerados y controlados.

El laboratorio deberá contar con una seguridad adecuada, en el establecimiento no tendrán que haber espacios para áreas de recepción donde el personal no sea del laboratorio, ni mucho menos que tengan que acceder al área de procesamiento del laboratorio. Dependiendo del tipo de organización hay algunas de estas cuestiones que ya están previstas por la organización en general. Muchas organizaciones ya cuentan con instalaciones que poseen un cierto nivel de seguridad que son adecuadas y solamente deberán ser modificadas para satisfacer las necesidades de seguridad del laboratorio.

Dependiendo de la configuración del área de trabajo en el laboratorio, se debe considerar la separación de las estaciones de trabajo en cubículos separados para mantener la privacidad, evitar la visibilidad inadvertida del material que se tenga en pantalla de una estación de trabajo por cualquier

persona que utilice otras estaciones de trabajo. Siempre que sea posible, los monitores deben colocarse lejos del punto de acceso al laboratorio, por dos razones: la primera es para evitar que alguien que accede al laboratorio no pueda tener una visión al material en los monitores de las estaciones de trabajo, y en segundo lugar, que el analista no pueda ver las personas que entran al laboratorio. Mientras que el posicionamiento de los monitores debe evitar vistas inadvertidas y también es importante que, siempre que sea posible, el personal no esté trabajando en entornos aislados. Uno de los controles establecidos por la norma ISO/IEC 27001 en el control A.11.3.3 Política de pantalla y escritorio limpio nos brinda un panorama para evitar el acceso a usuarios no autorizados y en el cual nos podemos referir para contrarrestar este tipo de problemáticas (27001:2005, ISO/IEC, 2005).

Se requieren tres tipos distintos de almacenamiento:

1. Se requiere un volumen significativo de almacenamiento para las pruebas (es normal que el material se almacena durante un período de semanas, meses, e incluso años)

2. También hay una necesidad para el almacenamiento de las imágenes creadas y cualquier producto de la investigación ya sean documentos o medios digitales. Deberá considerarse la posibilidad de almacenar las imágenes en lugares externos, así como las copias de seguridad

3. Dentro del área de trabajo también habrá una necesidad de espacio para almacenar todos los cables, conectores, accesorios y herramientas necesarias en el proceso de las investigaciones forenses digitales.

OTROS ASUNTOS A TENER EN CUENTA EN EL DESARROLLO DEL LABORATORIO

El laboratorio se encontrará en un ambiente de alta tecnología con una gran cantidad de equipos electrónicos sensibles al uso, dentro de los procedimientos, el uso de material antiestático será utilizado apropiadamente. El laboratorio deberá tener una red que estará aislada de todas las conexiones externas, se deberá tener en consideración el tipo de servidor, el ancho de banda de las comunicaciones, medios de almacenamiento (deberán contar con suficiente almacenamiento).

Además de la red, también se necesitará una conexión de internet independiente dentro del laboratorio para poder comprobar información, descarga herramientas, descargar parches y actualizaciones. Será necesario que estos equipos estén cuidadosamente colocados y asegurar su uso

adecuado teniendo la certeza de que no hay contaminación cruzada[77]. Se tendrá que asegurar de que este equipo forma parte de una red corporativa, que los administradores de sistemas son conscientes del uso que se les dé y asegurarse de que tiene control con el privilegio de acceso. Toda actividad en este sistema debe ser registrada y auditada regularmente, se sugiere que el sistema utilice una dirección IP fija dada por el administrador competente, para que, se audite todo el tráfico en estos equipos.

Un aspecto a menudo que se pasa por alto es que el personal tendrá un área de trabajo donde podrán desmantelar, reconstruir los ordenadores y otros dispositivos por lo cual el laboratorio necesitará un sistema de aire acondicionado muy eficiente.

El laboratorio también requerirá un área de almacenamiento para los documentos, discos limpios, y otros artículos desechables, así como un área para el almacenamiento a corto plazo de los equipos.

UN EJEMPLO DE UN LABORATORIO FORENSE DIGITAL

La Figura muestra un diseño de un laboratorio que comprende el espacio para todas las áreas, esto sería adecuado para un laboratorio de tamaño razonable, con base en el comercio forense digital.

Opción de diseño de un laboratorio forense digital (Andy Jones & Craig Valli, 2009)

[77] Cada especie debe ser embalada por separado en sobres de papel o cajas de cartón. No se debe embalar más de una especie en un paquete. Se podrán incluir en el mismo paquete o contenedor, evidencias que se encuentren debidamente tratadas (secas) y separadas de tal forma de impedir la contaminación cruzada de ellas.

El laboratorio deberá tener un sistema contra incendios adecuado, detección de intrusos, sistemas de alarma, sensores de movimiento y estos se deben de incorporar a los sistemas de la organización principales si en dado caso existen. Área de imágenes

Para mayor seguridad, idealmente, el laboratorio no deberá contar con ventanas, ya que el lugar elegido para el laboratorio debe estar en el centro del edificio, si el laboratorio tiene ventanas, la colocación de ventanas deberá ser analizada, incluso si el laboratorio está situado en la parte más alta del edificio deberá ser analizado. Medidas para contrarrestar el uso de ventanas en el laboratorio es rellenar el espacio y asegurarse que no sea permitido el acceso, también se deben de evitar ventanales ya que se podría tener visualidad desde afuera. Esto puede parecer un enfoque paranoico, pero siempre se debe tener en cuenta que el material que se procesa adentro del laboratorio es sensible y en consecuencia será de interés para los demás.

En la figura no hay espacio dedicado a los servidores, esto se debe que la ubicación de los servidores es subjetiva, en algunas organizaciones prefieren situarlos en el Área de Análisis o Área de Imagen (esto es parte de la preferencia personal de algunos autores), mientras que otros prefieren ubicarlos en el Área de Almacenamiento Seguro y Área de Investigación sensible.

IDENTIFICACIÓN DE LOS CLIENTES

Una de las cuestiones más importantes que se tendrán que resolver será para que clientes trabajará el laboratorio. Dicho de otra manera, ¿Cuáles serán los clientes del laboratorio? Sera el personal corporativo de la organización, para el departamento de auditoría, para el departamento de TI, para el departamento de justicia, la policía, o serán clientes comerciales. Cuando se haya determinado el tipo de cliente del laboratorio se estará en mejores condiciones para identificar la forma en que el laboratorio y su personal van a interactuar con ellos y el tipo de habilidades interpersonales necesarias. Debe haber una comprensión clara del límite de las responsabilidades entre los diferentes roles.

En la jerarquía de la organización es conveniente que el laboratorio forense digital responda directamente a la gerencia de seguridad de alta tecnología, a la gerencia de investigación o al jefe de seguridad. Si es posible evitar, el laboratorio no debe estar por debajo del departamento de TI o el departamento de auditoría. El laboratorio forense digital puede apoyar en las investigaciones del de departamento de TI y del departamento de auditoría pero debe conservar su independencia de ellos.

Si las normas básicas no están establecidas desde el inicio es preferible documentar los términos de referencia del laboratorio, de lo contrario habrá una expansión inevitable de las funciones o tareas de del laboratorio forense, de igual manera es casi seguro que ocurra ya que los demás departamentos

comenzarán a darse cuenta de la amplia gama de habilidades y conocimientos que posee el personal del laboratorio. Después de todo, el personal altamente capacitado técnicamente competente será requerido por sus habilidades para ayudar a resolver otro tipo de problemas en otras áreas de TI.

PRIORIZACIÓN DE CASOS

Antes de que el laboratorio entre en funcionamiento, el tipo de tareas que se aceptarán en el laboratorio y la prioridad de los diferentes tipos de casos se deben de determinar. Si se establecen las prioridades y se incorporan en los proceso desde un principio, se evitará que los argumentos y presiones indebidas al personal se realicen. Periódicamente deben ser revisados y ajustados según sea necesario regular la aceptabilidad de las tareas y su priorización relativa. El papel del administrador del laboratorio o el oficial de recepción, si se han creado, se encargarán de los procesos de aceptación del día a día y la priorización de los trabajos que entrarán en el laboratorio y normalmente se encargara de resolver los conflictos de los requisitos que se producen.

REVISIÓN DE CALIDAD

Los procedimientos son esenciales para controlar la calidad del trabajo realizado por el laboratorio forense digital. Esto asegurará que una adecuada calidad de servicios se establezcan, mantengan y que los procedimientos sean entendidos por el personal que se encuentran en la dirección del laboratorio. Los procedimientos en la revisión de la calidad no sólo apoyarán la integridad de la labor llevada a cabo por el laboratorio, sino que también será esencial en el apoyo a cualquier certificación externa o por alguna autoridad pertinente.

ESTÁNDARES

Las normas son esenciales en cualquier tipo de laboratorio, sobre todo cuando el resultado del trabajo puede ser analizado en un tribunal o en el que la vida de una persona puede verse afectada. Cumpliendo con las normas, ya sea dentro de una organización o una comunidad ayudará a la comunicación y la comprensión dependiendo del tipo de organización a la cual pertenece, es muy posible lograrlo con normas internacionales así como con normas locales o normas de la organización. Si los procedimientos siguen la dirección de estas normas y se abordan desde un principio, el personal tendrá la confianza de trabajar con normas reconocidas a nivel mundial y su trabajo podrá ser presentado ante cualquier tribunal o acción civil. Dos de los estándares más conocidos que se deben considerar son la norma ISO/IEC 9000[78] que es un conjunto de normas de gestión de calidad y la

[78] ISO 9000 es un conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO).

ISO/IEC 27000[79] que es un conjunto completo de controles que comprende las mejores prácticas en seguridad de la información.

Los estándares internacionales nos proveen una guía de acción a seguir, sin embargo debido a las realidades de cada laboratorio será necesario hacer una adaptación a estos estándares, siguiendo para ello las mejores prácticas y estableciendo sus protocolos de control y evaluación, sin perder de vista el objetivo último del análisis en función.

EQUIPO DE PRUEBA

El laboratorio forense digital contendrá una cantidad importante de equipos eléctricos y electrónicos que se necesitan examinar a intervalos regulares para su seguridad eléctrica. El equipo utilizado para tareas forenses también deben ser probados con regularidad para asegurarse de que son "estériles" y poder llevar a cabo sus funciones (y solamente sus funciones) como se esperaba. Otros equipos en el laboratorio también puede necesitar ser calibrados periódicamente, estas pruebas deben llevarse a cabo en períodos regulares o cuando hay alguna duda acerca de la seguridad, la calibración, o la efectividad.

EQUIPOS Y SOFTWARE

Una vez que el rol y el alcance de los trabajos para el laboratorio se han constituido en base a los clientes que se dará el servicio, será posible averiguar qué equipo y software se necesitará. Debido a la especialización tanto del hardware como el software y el tipo de la ciencia forense digital, probablemente se requerirá una serie de herramientas. Es normal que se tengan herramienta capaz de llevar a cabo cualquiera de las tareas forenses digitales, de esta manera, los resultados de unos se puede comparar con los resultados de otros para asegurar la consistencia.

SELECCIÓN DE EQUIPO

La selección de los equipos dependerá de si se pertenece a un ente de la aplicación de la ley o si pertenece a una organización comercial. Un número de compañías producen herramientas forenses digitales y sólo suministran sus productos a las agencias u organizaciones gubernamentales y a las fuerzas del orden que trabajan para ellos y que están avaladas por ellos. Esto no impide la adquisición de herramientas para llevar a cabo cualquiera tarea forense, pero puede reducir el número de alternativas disponibles, dependiendo del tipo de organización a la cual pertenece.

[79] La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Como mínimo, se necesitará una estación de trabajo para la tarea de cada analista, y el espacio suficiente para trabajar con todos los equipos periféricos, herramientas, archivos y demás protocolos requeridos durante una investigación. Además de los equipos necesarios para poder llevar a cabo las tareas pertinentes el personal del laboratorio, también debe haber por lo menos un sistema de repuesto para permitir el mantenimiento y las fallas. Además un terminal adicional disponible en el laboratorio dedicado a las búsquedas en Internet.

También se deberá decidir cómo las estaciones de trabajo deben estar en red, la capacidad de los dispositivos de red y la capacidad de almacenamiento digital. Los ahorros en la inversión de equipos de corta duración resultan en un mayor gasto posteriormente. Al decidir sobre los requisitos de hardware se debe tener en cuenta que las estaciones de trabajo necesitarán lo siguiente:

- Soporte rápido de imágenes en la extracción de la evidencia
- Soporte de IDE, SCSI, un portátil, micro unidades y lector de tarjetas
- Apoyo a una variedad de medios de almacenamiento extraíbles, incluidas las unidades de cinta, unidades Zip, unidades LS120, unidades JAZZ, disquetes y unidades USB, ya sea a través de las unidades externas o en compartimientos intercambiables
- Grabadoras de DVD
- Accesorios para soportar discos duros y dispositivos PCMCIA

Un número de opciones tanto de hardware como software se pueden emplear para garantizar la protección contra escritura cuando los sistemas se deben asegurar y que no haya posibilidad de contaminación de las pruebas del sistema en la creación de imágenes. La elección del sistema de "protección contra escritura" puede estar influida por el sistema de imágenes que se ha elegido, o por las mejores prácticas. Algunos de los bloqueadores de hardware y software de escritura más comúnmente utilizados son:

HARDWARE

- Guidance Software Fastboc[80]
- Tableau forensic bridges (hardware with blockers)[81]
- ForensicPC Mini-Digidrive write-blocking device for reading up to 12 different common Flash memory media
- Drive Lock Serial-ATA DriveLock Kit[82]
- Digital Intelligence UltraBlock and Firefly devices

[80] https://www.guidancesoftware.com/about/Pages/about-guidance-software.aspx
[81] http://www.tableausoftware.com/
[82] http://www.datadev.com/

- ICS ImageMasster DriveLock IDE
- Paralan SCSI Write Blocker
- MyKey Technology Inc. NoWrite
- Wiebe TECH Forensic Drivedocks
- LCTechnology International Firewire Second Generation Read Only Removable IDE Bay

SOFTWARE

- PDBLOCK[83]
- Royal Canadian Mounted Police Hard-Disk Write Lock

SOFTWARE FORENSE DIGITAL

Un amplio número de suites para la realización de imágenes y análisis forense digital son aceptadas y disponibles actualmente. El software varía en el costo y capacidad, además se necesitará una gama de herramientas de tareas individuales para llevar a cabo tareas específicas. Cuando se haya decidido sobre el software que mejor se adapte a las necesidades del laboratorio deben probarse para asegurarse de que funcionan en los sistemas configurados, es esencial asegurarse de que el software funciona de la manera publicada ya que la funcionalidad del software puede llegar a ser un problema en cualquier procedimiento disciplinario o judicial si no ha sido probado perfectamente.

Dada la amplia diversidad de delitos informáticos tanto de alta tecnología como de otro tipo que se va a investigar, se necesita una variedad de herramientas de software para ver diferentes aspectos de los datos que se están analizando, al seleccionar estas herramientas es conveniente seguir el consejo de las asociaciones profesionales y forenses pertinentes, así como los grupos de autoayuda disponibles para encontrar las herramientas más adecuadas, ya que estas organizaciones o grupos tienen experiencia y han dado su aprobación para la resolución de casos que se han comparecido ante un tribunal en la corte.

En el laboratorio forense la producción siempre será examinada y desafiada por lo cual es esencial asegurarse que las licencias del software que se utiliza son válidas y actualizadas.

Al utilizar software ilegal no sería ético y se caería en la negligencia, sería totalmente socavar la credibilidad e integridad del laboratorio. Además, se debilitaría toda prueba que se haya analizado y producido, podría ser perjudicial en algún caso el uso de estas herramientas sin licencia. También tendría un impacto negativo en la credibilidad del laboratorio, y dar como resultado la pérdida de

[83] http://www.digitalintelligence.com/

cualquier certificación obtenida, posiblemente incluso causar el cierre del laboratorio perdiendo su reputación a través del uso de dicho software.

ALMACENAMIENTO DIGITAL

El volumen de almacenamiento requerido será influenciado por varios factores, incluyendo el tipo de trabajo, tipos de clientes, las mejores prácticas de laboratorio, legislación, y la industria. Estos serán aspectos a considerar antes de poder tomar una decisión sobre el volumen de almacenamiento que se necesitará, así como la ubicación donde se almacenarán. Casos activos siendo investigados y los casos que no se han resuelto completamente, ya sea a través de la corte o tribunales también tendrán que ser almacenados, ya sea en un servidor o de alguna otra manera que los harán fácilmente disponibles y sobre todo a la brevedad. Casos terminados necesitaran ser almacenados por algún tiempo porque cabe la posibilidad que en una investigación sea apelada, pero no tienen que ser almacenados en el sistema en "vivo". En cambio, deben ser almacenados en una manera que garantice su integridad y su disponibilidad futura. Si bien la ciencia forense digital es aún una ciencia joven, el tipo de material utilizado para almacenar los grandes volúmenes de datos necesarios todavía no se ha demostrado ser un problema importante, pero será sin duda uno en el futuro, teniendo en cuenta los períodos de tiempo que los registros forenses deberán conservarse. También se tiene que tener en consideración las leyes nacionales sobre este tipo de casos, en algunos países los CDs fueron seleccionados como medios de almacenamiento hace unos años por una serie de leyes en cumplimiento con este tipo de casos.

EQUIPO EN LA ESCENA DEL CRIMEN

Se tendrá que decidir qué tipo de equipos serán necesarios para la escena del crimen en una investigación forense digital. Esto incluirá los tipos de estaciones de trabajo, como portátiles, equipos de realización de imágenes, la cantidad y tipo de equipamiento necesario para (almacenar) los sistemas incautados en la escena del crimen. Para la construcción de los kits en una escena del crimen, se debe considerar que se trabajará en escenas contaminadas y por tanto debe incluir los equipos de protección, no sólo para el examinador, sino también para asegurar que la integridad de la escena física no se vea comprometida y contaminada.

Además de las herramientas para la recolección de imágenes, también se debe considerar este tipo de kit en la escena del crimen:

- Guantes estériles
- Overoles estériles
- Linternas

- Destornilladores
- Bolsas
- Etiquetas
- Cinta adhesiva
- Dispositivos de comunicaciones
- Dispositivos para poder realizar pruebas de conexiones Bluetooth y WiFi
- Cámaras Espejos (para buscar en espacios donde no se puede ver fácilmente)
- Rotuladores y marcadores permanentes
- Cuadernos
- Formularios
- Contenedores y un carrito para transportar el material
- Alargadores de alimentación y adaptadores

Esta lista no es exhaustiva, sino que se ofrece una visión sobre el equipo que necesita tener a la mano en una escena del crimen.

También necesitará espacio de almacenamiento en el laboratorio para el equipo incautado en la escena del crimen, además del espacio de almacenamiento que necesitará para el equipo incautado se deberá recordar mantener el equipo durante un período considerable de tiempo, mientras dure la investigación. Vale la pena considerar desde el principio que mientras procesa más y más casos, el volumen de los equipos tendrá que almacenar crecerá rápidamente.

RECURSOS DE INFORMACIÓN

Con el fin de poder llevar a cabo cualquiera de los roles en el laboratorio forense digital, el personal en el laboratorio debe mantener el conocimiento continuo sobre la evolución en sus ámbitos de competencia y aumentar sus conocimientos para abordar las cuestiones que no se habían tratado antes. Para ello, se tendrá que tener acceso a una gran variedad de recursos de información, por ejemplo suscripciones a diarios y revistas, compra de libros, suscripciones a proveedores reconocidos para obtener información en línea, y así sucesivamente. La mayoría de éstos se debe pagar y el costo de ellos debería tenerse en cuenta en el presupuesto del laboratorio.

Otras fuentes de información valiosas y con conocimientos actualizados pueden ser organizaciones similares a los laboratorios forenses digitales o asociaciones forenses digitales, se pueden mencionar el Instituto Nacional de Estándares y Tecnología (NIST)[84], El Centro Nacional del Crimen de Cuello

[84] http://www.nist.gov/

Blanco[85], el FBI[86], las universidades que participan en leyes o investigaciones forenses digitales, los sitios de software, fabricantes de equipos forenses o proveedores de servicios. A medida que la disciplina de la ciencia forense digital se vuelve más ampliamente el número de fuentes y repositorios de información digital forense seguirá aumentando.

SALUD Y SEGURIDAD OCUPACIONAL

Todo el entorno forense digital es potencialmente peligroso para la salud, el personal utiliza y trabaja equipo de alta tecnología, desmantelando ordenadores y otros dispositivos. Cuando se requiere se visita la escena del crimen y se trabaja en ambientes de alta presión, ya que se desconocen los equipos informáticos y deberán tener el cuidado de no contaminar los equipos.

Los temas más amplios relacionados con la salud y la seguridad ocupacional deben abordarse desde el principio, el personal debe estar capacitado e informado sobre las medidas de salud y seguridad ocupacional, sesiones de información sobre estos temas deben reforzarse continuamente.

Se deben considerar controles sobre pruebas eléctricas y químicas de seguridad en el laboratorio, así como controles de salud y de seguridad ocupacional para asegurarse de que no hay prácticas o procedimientos inseguros.

RETENCIÓN DE DATOS Y POLÍTICAS DE ALMACENAMIENTO

Un laboratorio forense digital que no tenga una política de retención de datos bien definido se desarrollará rápidamente sin espacio de almacenamiento. También existe la probabilidad de que la retención innecesaria de datos será ilegal en la mayoría de jurisdicciones. Una política para la conservación de datos debe establecerse y aplicarse con anterioridad a la entrada en funcionamiento del laboratorio y debe validarse con las autoridades legales. La política de retención de datos debería ser aplicada rigurosamente con controles periódicos para garantizar que el laboratorio es compatible con las autoridades legales.

EL REPORTE DE HALLAZGOS

Una vez que se ha establecido la función y la base de clientes del laboratorio, se deben tomar decisiones sobre los tipos de informes que se producirán, los cuales serán suministrados en las investigaciones pertinentes. Esta política debe permitir que los documentos a medida que se vaya adquiriendo experiencia vayan cambiando a través del tiempo, para que los procedimientos en las investigaciones queden reflejados con todos los detalles necesarios.

[85] http://www.nw3c.com/
[86] http://www.fbi.gov/

PLANES

Antes de que el laboratorio inicie operaciones se debe desarrollar una serie de planes para garantizar que el laboratorio cumpla con las políticas y procedimientos de la organización (si es aplicable), con las normas, estándares y mejores prácticas de la industria. Los planes que se necesitan a tener en cuenta son: la seguridad ocupacional de laboratorio, planes de seguridad, planes de contingencia, planes de manejo de incidentes, planes de recuperación de desastres y planes operativos, deben ser establecidos y monitoreados ininterrumpidamente con el fin de garantizar un laboratorio forense digital eficaz y eficiente.

COMUNICACIONES

Es una triste realidad que muchas de las personas destacadas en habilidades técnicas y de software no tienen el mismo nivel con las habilidades de comunicación. Las comunicaciones son fundamentales para el éxito del laboratorio. El laboratorio forense trabaja para clientes y tiene que haber un diálogo para que los procedimientos aseguren las necesidades de los clientes y su satisfacción, así como los requisitos de los clientes deben transmitirse al personal de forma clara y concisa. Si los investigadores no entienden las capacidades y limitaciones del laboratorio forense, no van a ser capaces de realizar tareas con eficacia. Las comunicaciones juegan un importante papel en el ámbito del laboratorio porque de acuerdo a las habilidades técnicas en analizar un determinado caso se deben expresar todas las ideas y el seguimiento de la investigación correctamente. Los protocolos deben estar claramente definidos y deben ser de fácil comprensión, ya que la asignación de las tareas del laboratorio debe ser establecida, acordada, entregada y aceptada de forma transparente.

ALCANCE DEL REQUISITO PARA EL LABORATORIO FORENSE DIGITAL

INTRODUCCIÓN

El objetivo de este apartado es proporcionar una orientación sobre los diversos requisitos de un laboratorio, su rendimiento, el número de personal, la cantidad y tipo de equipo necesario para satisfacer el volumen del trabajo previsto.

La primera hipótesis que se puede hacer es que no importa qué tipo de laboratorio se está creando, la necesidad apremiante de mantener el proceso forense es primordial; esto debido, a que incluso un caso de cumplimiento rutinario puede producir materiales ilícitos o actividades ilegales que puedan ser utilizadas en la corte.

Anteriormente se mencionaron cuatro tipos comunes de investigación, las cuales ya fueron definidas:

- Las investigaciones penales
- Investigaciones de litigio civil
- Descubrimiento de datos
- Recuperación de datos

Para efectos de establecer el ámbito del laboratorio, la delimitación no se justifica en gran medida hasta que se está llevando a cabo una investigación. Por ejemplo, si se está llevando a cabo una tarea de adquisición para ser presentada en un tribunal o en el otro extremo de la escala, para recuperar los datos, sea cual sea el motivo el proceso emprendido debe seguir la mejor práctica forense con el fin de alcanzar el máximo potencial para el resultado esperado.

Como se ha mencionado anteriormente, el proceso forense se divide en tres etapas principales:

- Adquisición
- Investigación
- Presentación.

Cada etapa en sí misma se refiere a la siguiente por medio de la continuidad. A menudo en el caso de que la adquisición de la prueba se pueda llevar a cabo por un equipo diferente en un lugar separado, sin embargo, eso no elimina la necesidad de que el equipo y el proceso dentro del entorno del laboratorio sean los más adecuados.

Hardware y software de alto desempeño son sólo dos tercios de la exigencia de un laboratorio; la tercera y última de vital importancia es el proceso de pensamiento o análisis, también conocido como el personal de expertos debidamente cualificados, estas, son las piezas más complejas en cualquier laboratorio.

La dotación de recursos debe realizarse en función a las cargas de trabajo que han sido planificadas como resultado de la monitorización precisa de la capacidad de rendimiento del laboratorio. Esto a menudo es una tarea muy compleja, debido a que se debe buscar un equilibrio entre el trabajo a realizar y los recursos necesarios con el fin de no caer en el uso excesivo de recursos. Si el laboratorio está centrado en el cumplimiento de la ley o se ha enfocado como un establecimiento totalmente comercial de pago por servicio, la asignación de recursos y el uso prudente es fundamental para el éxito.

RENDIMIENTO

En un mundo perfecto, los humanos trabajan a un ritmo constante en cada tarea y utilizan la misma cantidad de recursos; cada vez para realizar la tarea emplean esfuerzo, tiempo y energía, por lo que la predicción del rendimiento de una tarea y la asignación de recursos se vuelven triviales.

Un laboratorio correctamente configurado debe hacer uso de procesos y dispositivos estandarizados. Muchas veces no son debidamente estimados el tiempo y el esfuerzo requerido para completar las tareas. Uno de los rasgos interesantes de la ciencia forense digital es que es un proceso intensivo centrado en la máquina, lo que permite una predicción más precisa de líneas de tiempo de trabajo. Las interacciones humanas en el proceso de análisis forense digital son las habilidades para analizar, informar y presentar los hechos.

Los siguientes son algunos ejemplos para ilustrar lo mencionado anteriormente. En primer lugar, la limpieza de los datos de un disco duro de una determinada marca y modelo se logra utilizando un equipo informático estándar, en el que se ejecuta software estandarizado y teniendo límites físicos. Así que el tiempo de limpieza para este disco duro se puede predecir con una precisión de más o menos un pequeño margen de error y se coloca dentro de una ruta crítica de trabajo del proyecto.

Del mismo modo, otras tareas que se llevan a cabo, tales como el tiempo necesario para crear hashes criptográficas para el mismo disco duro, también deben ser predecibles dentro de los límites indicados. También debería ser posible predecir el tiempo que se necesita para hallar los datos en el disco duro con el fin de recuperar archivos borrados cuando se han recogido datos suficientes, de hecho, hay muy poca interacción humana real con el proceso de análisis, debido a que al automatizar los estados finitos utilizados en los procesos informáticos usados al examinar los datos digitales, esta interacción con los datos por parte de una persona se vuelve innecesaria.

La clave para la predicción precisa es tener datos suficientes sobre la cual hacer los pronósticos. Para los profesionales existentes, muchos de estos datos son operacionales y más probablemente se incrustan en la documentación que se ha producido. Lo que hay que garantizar es la captura abierta y el registro de este tipo de flujo de trabajo de la información, ya que es de vital importancia para la gestión efectiva de los recursos humanos.

La siguiente es una lista de las tareas rudimentarias que deben ser seguidas, con el fin de realizar la estimación del trabajo futuro y la predicción de la línea de tiempo:

- **MEDIOS DE LIMPIEZA:** Limpieza de los medios antes del uso de imágenes
- **MEDIOS DE IMÁGENES FORENSES:** Imágenes de evidencia original

- **MEDIOS DE REPLICACIÓN FORENSE:** Creación de copias validadas para el análisis
- **INDEXACIÓN DE MEDIOS:** La indexación de los medios para la búsqueda de palabras clave
- **TALLADO DE DATOS:** Extracción de archivos borrados en los medios
- **BÚSQUEDAS ESTANDARIZADAS:** Las búsquedas implican palabras clave específicas, fecha y hora
- **ARCHIVADO DE CASOS:** Resguardo adecuado de todos los archivos en los medios adecuados

La recolección y el análisis de estos datos proporcionarán los medios precisos para estimar el costo a ser utilizado para las cotizaciones de trabajo. Estos datos son cruciales para la ejecución eficiente de un laboratorio en términos de costo y rendimiento. La información obtenida del tiempo necesario para las tareas automatizadas que son necesarias en el proceso forense, puede ser utilizada en la estimación de los plazos del proyecto, el cual es un elemento crítico en el análisis forense digital. El establecimiento de estos datos también puede ser utilizado como parte de la justificación para el personal o equipos adicionales, en especial cuando se haga frente a plazos por situaciones como investigaciones con órdenes judiciales.

Un uso adicional para la información de flujo de trabajo puede ser una medida eficaz de desempeño para el personal. Los datos de flujo de trabajo recolectados pueden demostrar, por ejemplo, que un miembro del personal se toma, verbigracia, de 40 a 60 por ciento más tiempo para completar las tareas de una calidad similar en comparación con otros miembros del equipo. Esta información ayuda a realizar algún tipo de intervención requerida, como por ejemplo el reciclaje, la reasignación o reducción de personal.

Otro uso de esta información de flujo de trabajo, desde el punto de vista del capital humano es que puede ser utilizado como una comprobación de validez operativa. Por ejemplo, si una tarea que implica que un disco duro se completó en tres minutos en lugar de la referencia de 30 minutos para este tipo de unidad, es probable que existan problemas en la ejecución, por ejemplo, el proceso ha terminado antes, existe un fallo de software, o el disco duro ha fallado.

EL "TRABAJO"

Uno de los elementos más importantes que afecta en el proceso forense, es el factor humano, el riesgo que el empleado no tenga la capacidad de concretar la prueba asociada con la tarea en cuestión. El nivel de prueba requerido para algunas causas penales puede ser significativo, debido al concepto de la prueba de tener que estar más allá de toda duda razonable. Relatos anecdóticos de los investigadores policiales indican que el dibujo de la fase de análisis es a menudo un método empleado por los abogados defensores para retrasar el proceso de la persecución de un caso. Esto está en

contraste con una investigación civil o tareas de recuperación de datos, las cuales pueden depender de la localización y recuperación de un único archivo de medios en los que puede haber cientos o miles de datos que se relacionan con el mismo incidente. Lo que importa en estos casos es que el comportamiento o las pruebas solicitadas se han encontrado y no es la profundidad o severidad del incidente lo importante, ya que a menudo sólo una exposición es lo suficientemente grave.

EL HARDWARE Y SOFTWARE

Los siguientes párrafos abordan una serie de cuestiones en relación con el hardware y el software que se debe considerar al tomar decisiones sobre el equipo que se utilizará en el laboratorio.

ESTACIÓN DE TRABAJO DEL ANÁLISIS FORENSE

Como se mencionó antes, la ciencia forense digital es una empresa sensible al tiempo y consiste en una serie de tareas intensivas y de recursos que se rigen por la naturaleza finita de las máquinas que las ejecutan.

Tareas como la indexación de palabras clave de unidades de disco duro o de la limpieza de la misma empujan constantemente al hardware a sus límites físicos finitos, lo que por desgracia a menudo no llega a los límites teóricos.

En el documento "Una investigación sobre la eficacia de las herramientas forenses, mecanismos de borrado de Disco Duro"**Fuente especificada no válida.** Se hace referencia al borrado seguro de los discos duros e indica que los tiempos tomados fueron impactados tanto por la velocidad de la CPU y la RAM en términos de memoria disponible, también la configuración física del sistema. Existen pocos argumentos de que la velocidad de la tarea depende en gran medida de la capacidad de procesamiento del hardware con el que se cuente en ese momento. Esencialmente un dólar ahorrado en el momento de la compra de equipos puede ascender a decenas de miles de dólares perdidos durante la vida útil del sistema como consecuencia de las pérdidas y retrasos. Por lo tanto, es muy importante cuando se está configurando un laboratorio utilizar los sistemas más rápidos disponibles y revisar su desempeño en forma oportuna, por lo general de forma trimestral.

El equipo seleccionado también debe estar en la lista de proveedores aprobados para cualquier sistema operativo que va a correr. Si no está certificado, no lo compre, ya que desde ese instante ya se está introduciendo un punto de polémica. En todo momento se debe de estar utilizando controladores certificados para los periféricos, como tarjetas de vídeo. Mediante el uso de controladores certificados, se elimina el riesgo y también se asegura que sus equipos se apeguen a criterios de rendimiento y estándares conocidos.

Tabla 1 Especificación técnica para una estación de trabajo forense

Tarjeta Madre (Mainboard, Motherboard):	Este debe ser un elemento de la lista de proveedores aprobados. Debe tener un número adecuado de ranuras de expansión de periféricos[87] disponible. Evite los casos de una sola ranura que tienen un gran componente de a bordo para el dispositivo periférico común. La placa base debe apoyar las conexiones USB y FireWire [88]de alta velocidad.
La Unidad Central de Procesamiento (CPU):	Debe ser el más rápido que se pueda comprar; preferiblemente con múltiples procesadores y de 64-bits.
Subsistema de Disco Duro:	La velocidad más alta posible que permitirá múltiples de lectura / escrituras. Debe hacerse pruebas de las tasas de transferencia sostenidas y de ruptura. IDE, SATA, SCSI. La capacidad de manejar arreglos RAID y discos grandes. Siempre que sea posible, una capacidad de intercambio en caliente mejorará el desempeño.
Memoria RAM:	La memoria debe ser certificada a la placa base. La velocidad más rápida que se puede comprar para la placa base. Instalar el máximo posible para el sistema operativo.
Discos duros:	Como la más alta velocidad posible. Debe hacerse la prueba de las tasas de transferencia sostenidas y de ruptura.
Case o Gabinete:	En caso de tener una fuente de alimentación de gran alcance con capacidad excedida y múltiples conectores. Compartimientos de unidades múltiples. Refrigeración suficiente.

El número de estación de trabajo forense requerido depende típicamente del número de analistas en el laboratorio. Los requisitos de espacio son, básicamente, un mínimo de 3 a 5 m2 por puesto de trabajo. Cada estación de trabajo o espacio deben tener suficientes tomas de corriente para la conexión de los sistemas y dispositivos periféricos. Todas las estaciones de trabajo forenses deben ser

[87] Periféricos, son dispositivos que permiten ampliar las capacidades básicas de un equipo de computo

[88] FireWire es un tipo de conexión para diversas plataformas, destinado a la entrada y salida de datos en serie a gran velocidad. Suele utilizarse para la interconexión de dispositivos digitales como cámaras digitales y videocámaras a computadoras.

validadas, verificadas y ejecutadas en un Entorno Operativo Estándar (SOE[89]). Un entorno operativo estándar incluye el sistema operativo subyacente, así como cualquiera de las aplicaciones instaladas que se utiliza en ese hardware en particular.

El sistema operativo debe ajustarse a configuraciones estándar y debe ser la misma versión utilizada en todos los equipos que emplean ese sistema operativo en particular y de la base de hardware. Una vez establecida esta línea de base, las aplicaciones forenses básicas (por ejemplo, EnCase, FTK, Autopsia, Sleuthkit, Xways) deben cargarse y probarse para verificar su correcto funcionamiento. La versión final resultante debería entonces ser fotografiada y su replicación debe ocurrir a través de un proceso para imágenes para ser verificado. Todo este proceso, más los parches de actualización u otros cambios aplicados estarán plenamente documentados en línea con normas como la ISO 17025[90]. Por otra parte, ninguno de los cambios debe llevarse a cabo en sin la adecuada gestión del cambio de TI.

ESTACIONES DE IMAGEN DE DISCO

Las estaciones de imagen de disco pueden ser cualquiera de los equipos basados en los puentes forenses, equipo basado en una infraestructura de red o ser un hardware de imágenes especializado, como el equipo de Silos III[91]. El elemento crítico en el uso de las estaciones de imagen de disco es que las combinaciones de hardware y software utilizados deben ser validadas y verificadas regularmente. Esto es esencial para garantizar y demostrar el correcto funcionamiento de los equipos durante la obtención de pruebas. Una herramienta infaltable son los duplicadores forenses que se han convertido en uno de los mejores instrumentos no solo para casos forenses sino para temas de Data Recovery, su posibilidad de copia en modo imagen o clonación bit a bit hace que se pueda determinar si la falla de un dispositivo es solo lógica o física.

Las estaciones de imágenes por computadora requerirán tarjetas y conectores del controlador de hardware especializados para acceder a tipos de discos duros comunes. Por ejemplo, deben ser capaces de conectarse tanto a dispositivos de 2,5 y 3,5 pulgadas, tanto para tecnologías IDE (PATA y SATA) y SCSI (1, 2, 3, UW, U160, U320) como un mínimo, así como FireWire y puertos USB de alta

[89] Estándar Operative Environment (SOE) se suele implementar como un estándar de imagen de disco para el despliegue en masa a varios equipos en una organización. Se incluyen el sistema operativo base, una configuración personalizada, las aplicaciones estándar utilizados dentro de una organización, actualizaciones de software y paquetes de servicios. Un SOE puede aplicarse a los servidores, ordenadores de sobremesa, portátiles y dispositivos móviles.

[90] ISO 17025: es una normativa internacional desarrollada por ISO (International Organization for Standardization) en la que se establecen los requisitos que deben cumplir los laboratorios de ensayo y calibración. Se trata de una norma de Calidad, la cual tiene su base en la serie de normas de Calidad ISO 9000

[91] Silos es un IEEE-1364-2001, simulador utilizado por los principales diseñadores de IC (Circuitos Integrados). Un estándar de la industria desde 1986, sus poderosas características de depuración interactivas proporcionan entorno de diseño más productivo de hoy para FPGA, PLD, ASIC y diseños digitales personalizadas.

velocidad. Los controladores deben estar en una lista de proveedores certificados para los sistemas operativos en los que se están utilizando. El uso de cables convertidores que no tienen chips también es útil. La provisión de conexiones Ethernet de alta velocidad también es vital para permitir la adquisición y transferencia de medios basados en la red.

ESTACIONES DE IMAGEN DE DISPOSITIVO MÓVIL

Este tipo de estación de recolección de imágenes está más orientado a ser utilizado por un ordenador portátil por algunas razones. En primer lugar, la mayoría de los dispositivos móviles no tienen una gran capacidad de almacenamiento interno que podría superar la capacidad de un ordenador portátil adecuadamente equipado. La imagen del dispositivo debe realizarse preferentemente a los medios, como un DVD o un disco duro USB conectado. En segundo lugar, el uso de un ordenador portátil proporciona una solución totalmente rápida, debido a que la vida de la batería de un dispositivo es corta en algunos dispositivos móviles y esto hace que sea adecuado el uso de una portátil para la clasificación en el lugar del siniestro y preservación de pruebas. Finalmente, las computadoras portátiles tienen su propia fuente de alimentación incorporada, su batería.

Una estación de imágenes de dispositivo móvil también necesita una conexión serial RS-232[92], Bluetooth e infrarrojos, con el fin de proporcionar conexiones con otros dispositivos móviles. Esta gama de métodos de conexión son necesarios para cubrir todas las posibles formas de conectarse a los dispositivos móviles, smartphones atípicamente, BlackBerries y dispositivos PDA. Los teléfonos más antiguos pueden requerir el uso de conexiones de hardware especializado o la construcción de un cable para la conectividad.

Este tipo de solución de imagen se basa principalmente en soluciones de software de proveedores especializados. Además del software, es necesaria una cantidad considerable de cables, enchufes, y alternativas de suministro de energía. Las soluciones basadas en hardware, tales como .XRY [93]son simplemente una versión muy especializada. Este tipo de equipo es el más adecuado para el trabajo de laboratorio en el lugar del siniestro.

[92] El protocolo RS-232 es una norma o estándar mundial que rige los parámetros de uno de los modos de comunicación serial. Por medio de este protocolo se estandarizan las velocidades de transferencia de datos, la forma de control que utiliza dicha transferencia, los niveles de voltajes utilizados, el tipo de cable permitido, las distancias entre equipos, los conectores, etc.

[93] Micro Systemation – el fabricante de las soluciones forenses para análisis de dispositivos móviles. XRY es una aplicación de software diseñada para funcionar en un PC con Sistema Operativo Windows. La extracción de datos de dispositivos móviles es una tarea muy especializada y no se trata del mismo trabajo que recuperar información de ordenadores. La mayoría de los dispositivos móviles no comparten el mismo sistema operativo y son dispositivos propietarios que tienen un sistema operativo único.

Este tipo de solución requiere un gran desembolso de capital para comprarlos debido al amplio desarrollo, apoyo continuo y actualizaciones necesarias para este tipo de sistemas.

Dos importantes piezas de hardware para su uso con dispositivos móviles son los de reacondicionadores automatizados de batería (descargador/recargador) y fuentes de alimentación variable. El reacondicionador de baterías es un dispositivo que permite que incluso las baterías de dispositivos móviles que tienen funcionalidad limitada pueda ser reacondicionado para que mantengan la carga por más tiempo. Estos dispositivos no son baratos, pero debido a la creciente demanda, se vuelve recomendable incluir estos dispositivos en la lista de dispositivos del laboratorio. La alimentación variable permitirá una conexión, a los efectos de la adquisición, a través de cualquiera tipo de conexiones para suministrar energía a un dispositivo móvil cuya batería puede haberse agotado.

Por último, para cualquier sistema de análisis de dispositivo móvil, un proceso de aislamiento de la red debe ser considerado, los dispositivos móviles son normalmente capaces de conectarse a varios tipos de redes, incluidas las redes de telefonía móvil, Bluetooth y WiFi. Los dispositivos móviles cuando se utilizan como elementos de pruebas deben ser aislados de estas redes. La falta de aislarlos adecuadamente de un canal o de la red puede generar en la evidencia contaminación o pérdida permanentemente de los datos, ya sea por accidente o intención. Como ejemplo, basta con encender un teléfono inteligente que ha estado desconectado durante un período de tiempo prologado, esto puede dar lugar a una avalancha de correos electrónicos y mensajes SMS que eliminan o borran elementos de interés en el dispositivo.

Uno de los desafíos insignificantes que esto presenta es la amplia gama de frecuencias sobre las que operan estas redes: los teléfonos celulares (800MHz a 2100MHz), Bluetooth y WiFi (2.4GHz). La solución a este problema requiere el uso de medidas que proporcionan aislamiento que detiene la salida y la entrada de las ondas electromagnéticas. Esto comúnmente se llama un escudo o jaula Faraday. Una jaula de Faraday es normalmente una carcasa metálica que reduce o detiene los campos electromagnéticos y las frecuencias que intenten entrar o salir. Hay varias opciones disponibles en la actualidad. Uno es el uso de una bolsa de aislamiento hecha de materiales para la atenuación de la señal de los dispositivos móviles.

Si el laboratorio está previsto para el procesamiento de un volumen significativo de dispositivos móviles, se justifica entonces la investigación en la construcción de una jaula de Faraday.

SOFTWARE

A menudo se da el caso que el software de análisis forense digital supera el coste del hardware que lo puede correr. Las herramientas tradicionales de informática forense como el EnCase caen en la categoría de software de alto costo, aquí también se incluye el software de .XRY, el software de código abierto es gratuito pero requiere una cantidad significativa de pruebas y verificación para asegurar que los resultados obtenidos con ella se puede replicar con otras herramientas. Además, hay inconvenientes añadidos como parte de las principales desventajas, ya que no tienen ningún tipo de soporte por parte del proveedor y su baja productividad debido a las pocas actualizaciones que se desarrollan al software.

Existe un gran debate acerca del uso software de código abierto frente a las ofertas de software comerciales en muchas áreas, y la ciencia forense digital no es diferente. La principal diferencia es que en la ciencia forense digital, independientemente de si se trata de software comercial o de código abierto, el software debe ser probado para asegurarse de que funciona según lo especificado. El punto importante es que estas aplicaciones independientemente de su origen, comercial o libre es el de dar apoyo, estabilidad y admisibilidad. El viejo adagio "si no está roto no lo arregles" debe ser traducido aquí como "si funciona y es validado, no lo parches".

Ya sea que se utilice software comercial o de código abierto o hay ciertas piezas de funciones específicas del software necesario, el costo del software y el tiempo para el soporte y mantenimiento de la misma deben tenerse en cuenta en su presupuesto.

Tabla 2 Comparación de software de código abierto y comercial

	Comercial	**Open Source**
Licencia de uso u operación	$ 300- $ 30000	Gratis
Soporte de productos	normalmente incluido	Por tiempo
Corrección de errores	normalmente incluido	No imperativo (Apoyo de comunidades de desarrollo)
Apoyo judicial	normalmente incluido	Por su cuenta

Como se mencionó anteriormente, lo que el software de código abierto nos ahorra en gastos iniciales, a menudo puede ser consumido fácilmente por extensos costos de soporte. En la tabla 3 se enumeran algunos ejemplos de herramientas comerciales y de código abierto.

Tabla 3. Ejemplos de Herramientas Comerciales y de código abierto

	Comercial	Open Source
Software de análisis de Discos Duros	EnCase Forensic Toolkit (FTK) Access Data Forensic Toolkit	Auditor
Software de Dispositivos Móviles	MobilEdit Paraben Device Seizure Susteen SecureView Oxygen Forensic Suite	
Software de Virtualización	VMWare Virtual PC	Xen (Linux) Qemu (Linux y Windows)

ALMACENAMIENTO DE LA EVIDENCIA

El almacenamiento de la evidencia es un área de las actividades del alcance del laboratorio que a menudo se olvida, muchas veces se incluye sólo cuando se da una ocurrencia. Debe considerar que incluso pequeñas prácticas forenses digitales podrían ser solicitadas, posiblemente, dentro de periodo de tiempo como un año y se debe tener en cuenta que los dispositivos de almacenamiento de datos actuales, requieren que su capacidad de almacenamiento sea de más capacidad, como por ejemplo un Petabyte para el almacenamiento de pruebas en vivo.

Se requieren dos tipos básicos de almacenamiento:

- Almacenamiento en vivo
- Almacenamiento de archivo

Se requiere almacenamiento en vivo para los casos activos, mientras que el almacenamiento de archivos, se da por casos o por imputación, este es todo el material que necesita ser archivado y conservado, por lo general por un período obligatorio de tiempo. El tiempo se ha determinado en gran medida por sus registros y requisitos probatorios, que son establecen de acuerdo a una base jurídica. Por ejemplo, en instituciones bancarias es requerido por Ley, el resguardo de información contable por un periodo mínimo de 10 años.

El almacenamiento en vivo no tiene que ser de alta velocidad; sin embargo, debe ser fiable y poseer redundancia. La redundancia es esencialmente la cantidad de componentes individuales que pueden fallar antes de que se produzca una pérdida o corrupción de datos. La redundancia se logra mediante el uso de una tecnología llamada RAID (matriz redundante de discos económicos o matrices redundantes de discos independientes). Lo que esta tecnología hace es combinar dos o más unidades de disco en una unidad lógica, a continuación, se aplica una combinación de técnicas conocidas como mirroring (Espejo) y tolerancia a fallos (corrección de errores) para alcanzar los niveles deseados de

protección frente al desempeño, una de las principales ventajas de este enfoque es que la tecnología es ampliable y utiliza estándares de la industria para el almacenamiento.

El tamaño físico del o los dispositivos de almacenamiento si tendrá un impacto significativo en sus requerimientos de alimentación eléctrica del laboratorio. Es importante señalar que se debe tener en cuenta los requisitos de energía tanto para los dispositivos de almacenamiento y de control ambiental a través de aire acondicionado refrigerado. Esto puede presentar problemas significativos en la planificación para la implementación de un laboratorio dentro de un edificio que ya se encuentra habitado o construir uno que no está cerca de una fuente disponible de fuentes de energía de respaldo.

ALMACENAMIENTO DE ARCHIVOS

Actualmente el almacenamiento de archivos se realiza utilizando tecnologías como DVD-R, CD-R, cintas magnéticas de alta capacidad. Es importante señalar que esto no es una solución permanente, ya que los datos se encontraran almacenados por un periodo determinado de tiempo. El requisito de espacio de carga estará determinado por la cantidad de información que requerirá ser almacenada, aquí también se debe considerar espacios físicos, ya que cada grupo de cintas, DVD o CD ocupan un área del laboratorio. También hay una necesidad de "archivo" del hardware y software que produjo los archivos para su posterior recuperación.

En cuanto a la instalación de almacenamiento se puede considerar un espacio separado, lo ideal es una habitación que tiene un alto nivel de seguridad con controles físicos y lógicos de acceso, para el almacenamiento de pruebas. Si la instalación se utiliza para el almacenamiento directo o de archivo; la prueba necesita protección no sólo de corrupción de datos, también se deben cuidar del deterioro como resultado de un mal control del medio ambiente. Las instalaciones en sí también se deben tener los controles de contención que permiten la supervisión del personal entrante y saliente, se incluyen sistemas de vigilancia de vídeo, alarma de incendio, control climático y de supresión de incendios, además del control ambiental que ya se ha mencionado anteriormente, esto a través del aire acondicionado refrigerado.

BANCOS DE TRABAJO DE HARDWARE

Una de las áreas que se vuelve fundamental en todo laboratorio forense digital, es un lugar destinado para el desmontaje y reparación de hardware. Se debe contar una amplia y adecuada gama de herramientas como por ejemplo, mesa de trabajo, destornilladores, soldadores, multímetros, micro taladros, y cualquier otra parafernalia necesaria para desmontar y/o reparar dispositivos electrónicos

digitales y analógicos. Esta área también debe contener un armario o espacio de trabajo que se encuentre libre de polvo para el desmontaje y montaje de los discos duros y otros dispositivos sensibles al polvo. El área también debe estar libre de fuentes de electricidad estática y deberá disponer de zonas totalmente conectadas a tierra en la que el equipo puede ser atendido. En esta área, se debe colocar un miembro del personal experto en electrónica o especializado en hardware, debe estar adecuadamente formado para llevar a cabo el desmontaje o reparación.

ACTUALIZACIONES, MANTENIMIENTO, OBSOLESCENCIA Y RETIRO DE LOS EQUIPOS

Uno de los elementos de la planificación de un laboratorio que rara vez se piensa es la planificación para el mantenimiento y eventual retiro de los equipos. El análisis forense digital es actualmente una disciplina en rápido movimiento que necesita un equipamiento de última generación para mantener una ventaja competitiva. La cuestión de si los equipos deben ser alquilados o comprados dependerá de las circunstancias y el capital de inversión con el que se cuente, pero la cuestión fundamental desde el punto de vista de alcance es el del mantenimiento, retiro y reposición de equipos.

Todo el hardware debe ser revisado de forma anual, las principales estaciones de trabajo forense deben tener una revisión cada seis meses. La tecnología avanza rápidamente, este tipo de avance en hardware puede tener impactos operacionales significativos, es decir, el procesamiento más rápido de tareas, lo que podría resultar en una reducción de los plazos de funcionamiento. Una simple sustitución o actualización de un CPU puede ver tanto como una mejora de 50 a 100 por ciento en la capacidad de procesamiento.

Todo el hardware de la computadora debe ser retirado al final de un período de tres años o el cese de la garantía. El costo de reparación de hardware está asociado en gran parte por la compra de equipo más rápido y más reciente. Problemas claros y previsibles a menudo surgen con componentes de reemplazo de abastecimiento, como memorias RAM o tarjetas de video, para dispositivos más allá de su garantía.

DESARROLLO DEL PLAN DE NEGOCIOS

INTRODUCCIÓN

Esta parte cubrirá el desarrollo del plan de negocios para la creación y el funcionamiento del laboratorio forense digital.

EL PLAN DE NEGOCIOS

El desarrollo de un plan de negocios es un asunto subjetivo, con una lista de recomendaciones y ejemplos de mejores prácticas que se pueden adoptar para la implementación del laboratorio. Por supuesto, la organización es probable que tenga sus mejores prácticas y las formas aceptadas de hacer las cosas, los lineamientos que se proporcionarán no pretenden ser una plantilla rígida, sino que se pretende ofrecer un ejemplo de un tipo de modelo de negocio para crear un laboratorio forense digital.

Para proporcionar un contexto, el siguiente plan de negocios ha sido escrito como si el laboratorio forense digital funcionaría dentro del Departamento de Seguridad, por lo tanto se inicia con un resumen ejecutivo, ya que este tipo de documento será presentado a la gerencia.

RESUMEN EJECUTIVO

Este documento es el plan de negocios para una nueva actividad propuesta que será gestionado por el departamento de seguridad de la organización.

- La actividad se refiere a la prestación de un servicio forense digital, dirigida a hacer cumplir la ley, normas, políticas en departamentos gubernamentales, grandes corporaciones, pequeñas y medianas empresas en el mercado tecnológico
- La necesidad de este servicio forense digital surge del crecimiento en la detección y persecución de delitos informáticos, que por medio de la investigación forense, incautar evidencia que pueda proporcionar a los peritos ante un tribunal las pruebas necesarias para la resolución de casos
- El propósito de este modelo de negocio es el de presentar a la gerencia información necesaria para determinar si debe o no continuar con el negocio
- El negocio de la ciencia forense digital requiere una inversión relativamente pequeña y tiene un periodo de recuperación de menos de tres años
- El negocio de la ciencia forense digital tiene tanto un riesgo técnico bajo como un riesgo financiero bajo, y es capaz de ser gestionado por el departamento de seguridad
- El servicio forense digital proporcionará un bajo costo y un servicio fácil de entender por lo que puede ser una solución muy eficaz para el clima actual del negocio
- La previsión de ingresos

ESQUEMA DE LA PROPUESTA

La siguiente sección del plan de negocios es el esquema de la propuesta que ofrece una breve explicación del propósito del plan y una indicación del alcance.

- Esta propuesta se refiere a la creación de un servicio forense digital conocido como "El Laboratorio Forense Digital". El servicio funcionará sobre una base de lunes a viernes de 8:00AM a 5:00PM con una flexibilidad en el horario según sea la investigación, satisfará una necesidad en el ámbito de la aplicación de la ley para el uso en procesos judiciales. Además ofrecerá el mismo servicio para clientes corporativos en los tribunales laborales que implican el uso indebido de activos digitales.
- Se debe presentar el riesgo financiero y una facturación prevista por servicios.

EL NEGOCIO

La siguiente sección del plan de negocios describe con más detalle el negocio que será propuesto y explica lo que se debe presentar.

LA NATURALEZA DE LA OFERTA DEL SERVICIO FORENSE DIGITAL:

- El objetivo del servicio forense digital es proporcionar a los clientes un servicio confiable y eficiente, que dará servicio a la demanda en la aplicación de la ley en los departamentos gubernamentales como resultado de las operaciones en curso y nuevas legislaciones.
- Por ejemplo el mercado en la aplicación de la ley y en los departamentos estatales para las investigaciones basadas en dispositivos digitales es uno de los mercados de rápido crecimiento en los EE.UU., el Reino Unido y Europa. Esto ha sido provocado por una infusión de fondos del gobierno y la creación de una serie de departamentos de alta tecnología en la investigación del delito informático. La creación de estas unidades fue una reacción al aumento de las denuncias de delitos motivados por dispositivos digitales y la falta de personal capacitado para hacer frente a las cuestiones planteadas.

EL ALCANCE DEL NEGOCIO FORENSE DIGITAL:

- Se debe tener claro la previsión de ingresos y una facturación prevista por servicios.
- Habrá una serie de ofertas a los clientes, todos basadas en la ciencia forense digital. El laboratorio proporcionará un servicio de análisis en el dispositivo digital para incautar pruebas que se utilizarán en tribunales judiciales o en tribunales laborales. El laboratorio proporcionará a las personas a actuar como peritos informáticos forenses en los tribunales y, en caso necesario, proporcionarán capacitación a las organizaciones en técnicas forenses digitales.
- Fecha de inicio de las ofertas de los servicios del laboratorio forense digital, por ejemplo, se pondrá en marcha el 01 de enero de 2015.

- El laboratorio utilizará inicialmente herramientas estándar de la industria para el análisis forense digital en imágenes, pero a medida que el requisito para la formación, recuperación y análisis de determinados elementos y tipos de información se vuelva más clara, se adquirirán más herramientas para cumplir con los requisitos.

ESTRATEGIA DE NEGOCIOS DE LA ORGANIZACIÓN EN RELACIÓN CON LA FORENSIA DIGITAL:

- Los principales factores que han influido en la estrategia para este modelo de negocio es la inversión, el capital humano, la experiencia existente y la cultura dentro de la organización.
- Un factor que no debería influenciar en la estrategia es el deseo de la organización para ser un centro reconocido de excelencia en las áreas de investigación en seguridad informática y delitos informáticos. No se ve que sea un factor limitante para el crecimiento de la empresa.
- La estrategia para establecer la organización matriz como centro de los servicios forenses digitales y la investigación forense digital. Este modelo de negocio, siendo modesto no busca establecer la organización matriz como líder del mercado.
- Los beneficios no financieros[94] de esta actividad permitirán que el personal involucrado pueda convertirse en altamente competente y que a su vez beneficiará a la organización en su totalidad y mejorará la reputación de la organización.
- Mediante la realización de investigaciones forenses el personal adquirirá conocimientos y habilidades en áreas que apoyarán la infraestructura organizativa.

PRODUCTO, CLIENTES, MERCADOS, CANALES, MARCA, Y PRECIOS DE SERVICIO DEL LABORATORIO FORENSE DIGITAL:

UNA PEQUEÑA DESCRIPCIÓN DE LO QUE REALIZA LA FORENSIA DIGITAL

- Los dispositivos digitales se han vuelto más ubicuos e integrados en aspectos de la actividad diaria y en la vida personal de los individuos, por lo que tiene su uso como herramienta y como fuente de evidencia en las investigaciones criminales. En el cumplimiento de la ley se debe tener en cuenta el rol del dispositivo digital en todo tipo de delito, desde asesinatos, tráfico de drogas, chantajes, pedofilia, entre otros. El dispositivo digital puede ser utilizado como una herramienta en la comisión del delito o simplemente como un repositorio de información relacionada con el crimen. Los oficiales del cumplimiento de la ley no tienen la experiencia suficiente para llevar a cabo las investigaciones necesarias, utilizando sus propios recursos, la

[94] Beneficios no financieros: Incremento en la productividad de los empleados, menor oposición al cambio, se previenen problemas, impone orden y disciplina en la empresa. Además de ayudar a las empresas a evitar los problemas financieros, la administración estratégica ofrece beneficios tangibles, por ejemplo: una mayor alerta ante las amenazas externas, mayor comprensión de las estrategias de los externos, etc.

aplicación de todos los dispositivos digitales y sistemas necesarios. Como resultado, en muchos sitios, hay un retraso grave en la resolución de casos. Los servicios ofrecidos por el laboratorio forense permitirá ser visto por las organizaciones encargadas de la aplicación de la ley como una organización de confianza que puedan subcontratar para sus investigaciones.

- Además existen diferentes tipos de clientes que requieren cada vez más los servicios forenses digitales y no tienen las habilidades forenses digitales de investigación necesarias. Esta necesidad de la industria corresponde con las organizaciones comerciales que requieren estos servicios con el fin de satisfacer las necesidades de incrementar los niveles de seguridad.

LA NECESIDAD DE UN SERVICIO FORENSE DIGITAL

- La cantidad de trabajo forense digital que ha surgido en estos últimos años debido a la proliferación del uso de dispositivos digitales como también al resultado de la aplicación de la ley en operaciones comerciales para abordar delitos informáticos, se ha traducido en la creación de unidades de investigación sobre delitos informáticos tratando de aplicar la ley de cumplimiento pero estas unidades que cada vez están siendo abrumadas por el volumen de trabajo y la complejidad de casos. Además el tiempo necesario para capacitar al personal, los salarios, el suministro de herramientas, entre otros, son factores que ameritan la necesidad de un laboratorio forense digital.

CLIENTES

- Los clientes inicialmente se podrán tomar de los departamentos gubernamentales y organizaciones comerciales. A medida que se establece el servicio se ampliará a otro tipo de clientes.

MERCADOS

- En un principio el objetivo serán las organizaciones involucradas en el cumplimiento de la ley, entidades de seguridad, departamentos de gobierno, la banca, mercados de servicios financieros, de salud, de fabricación, el mercado minorista y de telecomunicaciones.
- Investigaciones realizadas por autoridades competentes locales y seminarios dirigidos a profesionales de la seguridad de la información.

CANALES

- El principal canal de comercialización será a través de la propaganda que se dé a través de los clientes existentes y algunos contactos.

PRECIOS

- El servicio forense digital será cargado en función de cada puesto de trabajo. Los honorarios estarán basados en la variedad de servicios que se requieran.
- La estrategia de precios se basa en la necesidad de recuperar, como mínimo, todos los costos fijos y variables con un margen suficiente para obtener ganancias, mientras que, el máximo, proporcionar un servicio a un costo similar o inferior con respecto a la competencia.

FORTALEZA COMPETITIVA DEL SERVICIO FORENSE DIGITAL

ANÁLISIS DE LA COMPETENCIA

- Hay tres tipos principales de competencia, la primera son los proveedores de servicios forenses digitales, la segunda son los proveedores de productos de servicios forenses digitales y el tercero son los clientes con sus propios recursos internos.
- Los proveedores de servicios son organizaciones como Digital Forensic Services Inc, Kroll Ontrack[95], Midwest Forense, QinetiQ[96], y Gestión de Riesgos Internacionales.
- Los proveedores de productos como Guidance Software[97] los proveedores de EnCase Digital Forensics Tools (la herramienta más utilizada en el cumplimiento de la ley para los ordenadores y dispositivos de red), Paraben[98] (la herramienta más utilizada para los dispositivos móviles de baja gama), XRY (es una herramienta de análisis forense digital y análisis forense de dispositivos móviles de la empresa sueca Micro Systemation[99] utilizada para analizar y recuperar información de dispositivos móviles de alta gama), asi como UFED TK (la solución ruguerizada de análisis forense de dispositivos móviles de Cellebrite[100]).
- Los proveedores de productos anteriores no están en competencia directa con la organización, en la medida en que no suministran a sus clientes un servicio. Sin embargo, están en el negocio de proporcionar a nuestros potenciales clientes soluciones de software y hardware, con la intención de que sus clientes operan sus propios sistemas, y por lo tanto no necesitan de nuestros servicios.

DIFERENCIADORES

[95] http://www.krollontrack.com/
[96] https://www.qinetiq.com/Pages/default.aspx
[97] https://www.guidancesoftware.com/
[98] https://www.paraben.com/
[99] https://www.msab.com/
[100] http://www.cellebrite.com/es/

- Además de proporcionar a los clientes servicios forenses digitales, se pretende que el laboratorio ofrezca servicios adicionales, aunque no sea el único en el mercado, diferenciarán la oferta de otros competidores.

PUNTOS DE VENTA ÚNICOS (USPS)

- La oferta de servicios del análisis forense digital es único, ya que es capaz de proporcionar un servicio independiente utilizando un software estándar de la industria. Algunas encuestas realizadas con anterioridad han identificado la necesidad de este servicio. Sin embargo, los clientes potenciales son extremadamente cautelosos en cuanto a quién van a confiar para realizar este servicio. La respuesta es que la organización se posicione mediante la confianza.

ASUNTOS COMERCIALES CLAVES EN LA ORGANIZACIÓN EN RELACION A LA FORENSIA DIGITAL

- Diversos asuntos empresariales claves pueden afectar el éxito del negocio del servicio forense digital.
- No se conocen asuntos políticos, económicos, ambientales, económicos, sociales que pueden afectar el éxito de la empresa del servicio forense digital. Sin embargo, puede haber problemas de personal, así como aspectos legales y financieros que deben ser abordados.
- El negocio del servicio forense digital requiere un determinado nivel de personal operativo con el fin de mantener los servicios del laboratorio. Este nivel de recurso mínimo deberá ser capaz de ofrecer el servicio a muchos clientes. Así, las ventas no se limitarán por la contratación de personal adicional, por encima de este nivel base. Sin embargo, la organización debe atraer y retener al personal adecuado. Sin embargo, si por alguna razón el negocio no es capaz de reclutar y retener personal clave suficiente, el negocio fracasará.
- El negocio del servicio forense digital requerirá una inversión limitada. Si, por cualquier razón, los fondos necesarios no se produce, el negocio no será viable.
- El negocio del servicio forense digital tendrá que abarcar ciertas actividades como la comercialización, el enlace con el cliente y hasta en cierto punto el entretenimiento que es actualmente desconocido en las organizaciones. Si, por cualquier razón, estas actividades no se realizan, la empresa fracasará.
- El negocio del servicio forense digital deberá estar localizado en un lugar apropiado para prosperar sobre el entorno.
- La inversión necesaria para poner en marcha este negocio debe de cumplir con las aspiraciones de participar en nuevos proyectos empresariales de la alta gerencia y alinearlos correctamente con la realidad.

RESUMEN CONVINCENTE DE LA PROPUESTA DE NEGOCIO PARA LA ORGANIZACIÓN

- El negocio del servicio forense digital oportunamente se establecerá en el mercado. El negocio requiere una inversión modesta, con bajo riesgo técnico y comercial, que producirá beneficios potencialmente importantes y continuos. La organización ganará a través de sus investigaciones y de la reputación de los conocimientos técnicos de clase mundial en el campo de la ciencia forense digital. El negocio proporcionará una plataforma para mejorar su reputación a través de la exposición de una serie de casos en vivo ya través del contacto con los clientes potenciales.

ADMINISTRACIÓN

ORGANIZACIÓN DEL SERVICIO FORENSE DIGITAL

- Bajo este modelo de negocio se propone que el servicio forense digital opere dentro del departamento de seguridad de la organización, como un departamento independiente de otras áreas de TI.

PERSONAL CLAVE PARA EL SERVICIO FORENSE DIGITAL

- El gerente y sub-gerente del departamento deben tener los conocimientos y la experiencia que se necesita en el negocio para entregar el asesoramiento técnico debido. Ellos formarán el núcleo del negocio y se necesitarán de sus habilidades para todo tipo de requerimiento. Otros miembros del personal requerirán habilidades y experiencia en algún determinado servicio que proporcione el laboratorio forense digital.

INTERFACES E INTERDEPENDENCIAS

- Por el lado de la oferta, el negocio dependerá del acceso a los proveedores de productos forenses digitales. El servicio forense digital debe evaluar y seleccionar los mejores productos de su clase para su uso en la entrega del servicio.
- Sin obligaciones y dependencias conocidas tendrán que ser abordados los servicios en relación con asuntos de reglamentación o conflictos de intereses con las normas o procedimientos corporativos.

RECURSOS

- La disponibilidad de personal cualificado es fundamental para el éxito de la empresa. Este problema representa el segundo riesgo más importante para el éxito de la empresa. No se prevé que la organización tendrá un problema en el corto plazo, la realidad es que a largo

plazo, si el negocio es muy exitoso, surgirán problemas como normativas impuestas en la aplicación de la ley. Con el nivel de formación y la habilidad necesaria de un investigador forense para realizar actividades efectivas, el potencial del investigador es altamente remunerado en el comercio. De acuerdo a los suministros externos de recursos, instalaciones, materiales, equipos operativos, software y servicios de comunicaciones no existen requisitos conocidos que se encuentren disponibles en el mercado.

UBICACIÓN E INSTALACIONES

- El servicio forense digital será operado desde un alojamiento aislado de las instalaciones corporativas o de la organización matriz.

CAPITAL INTELECTUAL

PROPIEDAD INTELECTUAL DEL SERVICIO FORENSE DIGITAL

No hay ningún requisito para la adquisición de la propiedad intelectual por parte de la empresa forense digital. Sin embargo, se prevé que, con el tiempo, el laboratorio desarrollará DPI[101] que agregará valor a través de la concesión de licencias y la reputación.

SABER DEL SERVICIO FORENSE DIGITAL

- El equipo forense digital tendrá que aprender a manejar el servicio de la manera más económica. Esto mejorará a medida que se adquiere experiencia.

ENFOQUE FINANCIERO

- La dotación de personal se basa en la cantidad y roles necesarios para llevar a cabo las actividades del negocio. Los niveles de remuneración se asignan a los diferentes roles. El modelo de rendimiento, realiza una comprobación de validez para determinar si el negocio tiene demasiados o muy poco personal.
- Los costos de comercialización y de entretenimiento si aún no se han identificado. Se requiere un juicio para estimar el nivel de dinero necesario para generar suficiente sensibilización en el mercado y la generación de negocios.

INGRESOS Y GASTOS ANTICIPADOS PARA EL SERVICIO FORENSE DIGITAL

[101] La propiedad intelectual, según la definición de la Organización Mundial de la Propiedad Intelectual, se refiere a toda creación de la mente humana.1 Los derechos de propiedad intelectual protegen los intereses de los creadores al ofrecerles prerrogativas en relación con sus creaciones.

- Una estimación presupuestaria de cinco años de ingresos y gastos, excluidos los impuestos, deberán ser las proyecciones del negocio.

COSTOS DE FORMACIÓN PARA EL LABORATORIO FORENSE DIGITAL

- Se deberá realizar el costo de formación y esfuerzo realizado por el personal.

CUESTIONES JURÍDICAS Y REGLAMENTARIAS RELATIVAS AL SERVICIO FORENSE DIGITAL

- No aplicable en este caso de negocio

BENEFICIOS PARA LA ORGANIZACIÓN

FINANCIEROS

- La rentabilidad potencial del negocio es alta. Esto no se basa en las expectativas extravagantes de un alto número de ventas. De hecho, las asunciones han sido modestas en cuanto a la captación probable de nuevos clientes. Los altos beneficios surgirán del hecho de que el servicio forense digital es un servicio que se presta al incremento del negocio, y que los costos marginales[102] de la prestación de servicios son bajos en comparación con los ingresos potenciales.

NO FINANCIEROS

- El negocio del servicio forense digital desplaza al Departamento de Seguridad hacia la oferta de servicios que complementan los actuales servicios basados en consultoría. Con un costo y esfuerzo marginal mínimo, los servicios pueden ser renovados año tras año para seguir produciendo ingresos.
- El servicio del laboratorio forense digital puede ser utilizado como base para el lanzamiento de servicios adicionales a los clientes, ya que el mercado siempre necesita cambios. Una vez que el servicio se está ejecutando, las ventas no se verán limitados por la capacidad de la organización.
- Los organismos del cumplimento de la ley podrán obtener tanto el servicio del laboratorio, análisis y asesoría ad-hoc.

RIESGOS Y FACTORES CRÍTICOS PARA EL ÉXITO DEL SERVICIO FORENSE DIGITAL

[102] En economía y finanzas, el coste marginal o costo marginal, mide la tasa de variación del coste dividida por la variación de la producción

FASE DE CONFIGURACIÓN

- Laboratorio no configurado adecuadamente y no preparado para las actividades del negocio con anticipación.
- Personal con formación insuficiente.
- Insuficiente inversión.

RESPONSABILIDAD DEL PRODUCTO

- El negocio del servicio forense digital exigirá un seguro de responsabilidad civil profesional. El nivel de aseguramiento requerido estará bajo investigación y será fundamental, ya que los clientes podrán demandar al laboratorio en caso de una investigación mal manejada. También hay una posibilidad de que un cliente puede irse con otro proveedor alternativo si el laboratorio no es sensible y no proporciona una oferta de servicios adecuada.

DESARROLLO DEL MERCADO

UNA SERIE DE ASUNTOS CLAVES SON PROBABLES QUE IMPIDAN QUE EL SERVICIO FORENSE DIGITAL PENETRE EN EL MERCADO:

- Un líder en el servicio puede surgir a dominar el mercado y este líder en el mercado puede a través de una tecnología superior, mejores prácticas y ofertas más atractivas impedir la penetración en el comercio.
- Una comercialización insuficiente, deficiente y con poca calidad puede negar al laboratorio el éxito.
- El servicio forense digital puede no ser capaz de ofrecer el nivel de servicio esperado por los clientes, lo que resulta una pérdida de reputación, de modo que será más difícil atraer nuevos negocios y retener a los clientes existentes.

GESTIÓN Y SERVICIO DE ENTREGA

- Existe el riesgo de que la organización maneje el negocio del servicio forense digital como un proyecto más que como un negocio.
- Existe el riesgo de que los técnicos analistas de servicios forenses digitales pueden no ser capaces de categorizar y priorizar las investigaciones y hechos de manera eficaz.
- Hay un riesgo técnico que la cantidad de esfuerzo que se necesita para llevar a cabo un análisis forense de un sistema ha sido subestimado.

- Hay un riesgo técnico que el software utilizado por los analistas en el laboratorio del servicio forense digital sea incapaz de analizar el material de una manera eficaz. Esto podría resultar de un asesoramiento ineficaces en el cumplimento de normas.

FINANCIEROS

- Las variables más sensibles que afectan a la rentabilidad son el número de clientes (el volumen de ventas), el precio de venta (la tarifa de pago) para los servicios forenses digitales, y el número de clientes que el personal de laboratorio puede gestionar con eficacia.

LEGAL

- Ciertos factores legales o reglamentos conocidos según la jurisdicción que podrían afectar adversamente el negocio.

PLAN DE SALIDA DEL NEGOCIO POR PARTE DE LA ORGANIZACIÓN

- Se prevé que el negocio de la ciencia forense digital va a continuar, de una forma u otra, a perpetuidad.
- Si el negocio falla, la mayoría del personal en el laboratorio podría reasignarse fácilmente dentro de la organización así como los equipos.

RESPONSABILIDADES ADMINISTRATIVAS EN LA SALIDA

- La salida será administrado por el jefe del departamento de finanzas de la organización.

DISTRIBUCIÓN DE LOS ACTIVOS Y PASIVOS

- La distribución de los activos y pasivos se mantendrá en el departamento de seguridad.

SÍNTESIS DE IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL

La implementación de un Laboratorio Forense Digital es un procedimiento complejo en donde se deben considerar algunos elementos primordiales, a modo de síntesis colocamos los pasos que se deben seguir antes y durante el establecimiento de un Laboratorio Forense Digital, estos pasos son:

1. Se deben determinar aspectos del proyecto de implementación, los cuales permitirán decidir si se crea o no un laboratorio de informática forense, para esto es importante determinar necesidad, modelo y plan de negocio (Impacto, Probabilidad de éxito y Costo de la inversión).
2. Presentar proyecto
   - Determinar un ROI
   - Determinar el alcance del laboratorio
   - Definir las actividades a realizar en el laboratorio
   - Definir los términos de referencia
3. Definir funciones, deberes y responsabilidades de los miembros del laboratorio
   - Los niveles del personal
   - Roles
   - Perfil y selección del personal
   - Planes de formación y capacitación
4. Determinar el presupuesto de creación
   - Costo de capital (compra de equipo y software, construcción o renovación del lugar físico)
   - Costo de funcionamiento (gastos de operación, salarios y mantenimiento)

Una vez decidida la implementación, es importante considerar aspectos operativos, los cuales se listan a continuación:

1. Definir los requisitos del establecimiento. Un laboratorio en general necesitara contar con las siguientes áreas:
   - Área de recepción y almacenamiento
   - Área de reuniones y espera
   - Área de descanso y cafetería
   - Área de almacenamiento de equipos y posesiones personales
   - Área de imágenes
   - Área de desmontaje
   - Área de almacenamiento seguro

- Área de investigación sensible
- Área de escaneado
- Área de análisis
- Oficina de administración

También se definen aspectos como:

- Determinación de zonas
- Seguridad perimetral
- Cantidad de tomas de energía, puertos de red
- Equipo e infraestructura
- Hardware y Software

1. Determinar procedimientos y normas de funcionamiento
   - Estándares y protocolos
   - Procedimientos de trabajo
   - Colección de evidencias
   - Procesamiento de información
   - Almacenamiento de la evidencia
2. Determinación de los clientes (priorización de casos, revisión de calidad)
3. Comunicaciones y reportes (El reporte de hallazgos, planes, comunicaciones)

La siguiente imagen muestra en síntesis los procedimientos generales a considerar en la implementación de un Laboratorio Forense Digital.

RESUMEN

En este capítulo se ha examinado una serie de cuestiones que deben tenerse en cuenta con el fin de desarrollar el modelo de negocio y obtener el apoyo necesario de la alta gerencia, así como los fondos necesarios para establecer un laboratorio forense digital. Se ha examinado una serie de factores que deben ser abordados para garantizar el laboratorio y una vez establecido ser capaz de funcionar a su operación máxima y el trabajo que produzca sea de nivel aceptable. También se examinaron cuestiones relativas a la contratación de personal, la asignación de funciones y la posterior formación, así como el bienestar de los empleados de laboratorio.

Además, se ha utilizado para proporcionar una guía sobre una serie de cuestiones que deben tenerse en cuenta, pero a menudo se pasan por alto cuando se establece el alcance de la exigencia para el laboratorio. Estos problemas que han sido examinados incluyen el rendimiento potencial del trabajo, la cantidad de personal necesario, y las consideraciones en cuanto a la cantidad y tipo de equipo necesario para satisfacer el volumen de trabajo previsto. Las cuestiones relativas a la elección de código abierto o software comercial han sido discutidas, así como el almacenamiento de datos a largo plazo y a corto plazo.

Por último, se han señalado asuntos que deben tenerse en cuenta y los argumentos que deben ser planteados en el desarrollo del plan de negocios para la creación y funcionamiento del laboratorio forense digital. Este plan de negocios que se ha utilizado se ha basado en estándares internacionales que han tenido éxito en organizaciones comerciales y se ha modificado sólo para que sea lo más genérico posible. Si bien cada entorno y organización es ligeramente diferente, algunos requisitos se pueden extender y abordar en el plan de negocios y al final debería proporcionar un buen esquema.

CAPÍTULO 5: UBICACIÓN DEL LABORATORIO

INTRODUCCIÓN

En este capítulo se abordan una serie de elementos que deben ser considerados al momento de decidir sobre la ubicación del laboratorio. Estos incluirán la ubicación del laboratorio en términos de la localización geográfica, la ubicación con respecto a la organización, y la ubicación del laboratorio dentro de un edificio.

La ubicación y la seguridad del laboratorio es un elemento crítico que suele pasarse por alto o no es considerado de forma adecuada. Gran parte de los datos forenses almacenados deben tener una ubicación física que sea segura, estable, y estéril. La continuidad de la evidencia demanda un alto nivel de control de acceso que sea auditable a los datos que están siendo procesados o almacenados.

LA UBICACIÓN DE UN LABORATORIO

El primer aspecto crítico es la ubicación y seguridad inherente del sitio, esta debe estar relacionado con el acceso a las instalaciones, ante una eventualidad se, infiere normalmente que una "respuesta", se proporcionará de manera rápida y ordenada, esto obliga a que la instalación del laboratorio cuente con fácil acceso a las principales vías de comunicación.

Otro aspecto que afecta la selección del sitio es la susceptibilidad del sitio ante eventos de origen natural que pueden afectar las operaciones, tales como, incendios, inundaciones, tormentas y terremotos. Es importante tener en consideración los sitios en donde se ubicará la infraestructura, entre los aspectos a evaluar se encuentran: (Andy Jones & Craig Valli, 2009)

- No ubicar la infraestructura en una zona de inundación, ya que se corre el riesgo de deslave o inutilización debido al daño del agua
- No ubicar la infraestructura cerca de una instalación de almacenamiento de materiales inflamables tales como combustibles, solventes, plantas o fabricas que trabajen con químicos
- No ubicar la infraestructura en una zona de vientos fuertes
- No ubicar la infraestructura en la parte superior de una línea de falla tectónica o una zona de actividad volcánica

El sitio también debe estar ubicado con fácil acceso a los servicios que pueden ser necesarios, así como permitir el ingreso de equipos, algunos de gran tamaño, por lo que es recomendable colocarlo en una planta baja del edificio. El laboratorio forense digital, deberá contar con suficiente capacidad de energía y telecomunicaciones, la disponibilidad de energía es un tema importante para el establecimiento de cualquier laboratorio de computación y muchos edificios no tendrán suficiente

capacidad de reserva para atender a las grandes instalaciones de ordenadores. La seguridad de las comunicaciones y la energía es un requisito esencial para cualquier instalación; para alcanzar los niveles requeridos de seguridad, implica la instalación de gabinetes y/o armarios especializados, así como puertas en los puntos de acceso utilizados en el edificio para los servicios públicos.

La determinación de la exigencia del laboratorio, requiere que en lo posible, los proveedores de los servicios de energía y comunicaciones garanticen niveles de servicios y provean soluciones ante mínimas fallas y redundancia en situaciones que lo ameritan, así como considerar en su momento la implementación de sitios alternos, esto siempre y cuando la organización que maneja el laboratorio así lo requiera.

Un enfoque verdaderamente redundante a los suministros de servicios críticos puede mitigar significativamente los riesgos operacionales resultantes de fallas por un tercero. El uso de dos proveedores de servicios para la prestación de Servicios de Internet es un ejemplo de ello. Si el ISP primario falla, el otro ISP debe ser capaz de cubrir la carga operacional base. Es preciso señalar, que deben ser dos ISP físicamente separados, tanto en términos de la acometida en el edificio y el enrutamiento a Internet, con el fin de que esto tenga algún valor.

En el caso de la energía, puede ser necesaria la prestación de generación de energía en el sitio de respaldo, sobre todo si el laboratorio forense digital se utiliza para analizar los dispositivos involucrados en incidentes importantes y de alta prioridad, como el terrorismo o el contrabando de drogas.

El sitio en sí debería utilizar los principios de defensa en profundidad en su construcción, como contramedidas, tanto físicas (estructuras, caminos de acceso) y lógicas (control de acceso, defensas de la red). El principio de defensa en profundidad es el uso de lo que puede considerarse círculos concéntricos o capas de defensas apropiadas, a veces se hace referencia como la defensa de la cebolla. Cada capa debe ser una barrera que debe ser penetrado antes que la siguiente se pueda acceder. (Ver fig. 5.1)

Figura 5.1. Concepto de la defensa por capas

El perímetro exterior del sitio debe ser una combinación de barreras que controlan el flujo de material, información, y personas en el sitio. Debe tener un mínimo de puntos de salida, preferentemente separados, con controles de acceso adecuados instalados en cada uno. Esto podría lograrse a través de la instalación de vallas, el uso efectivo de la iluminación perimetral y cámaras, restricción de acceso de vehículos a través del uso de controles tipo pluma o bolardos para controlar los flujos de tráfico.

Otra medida que se puede implementar es la separación de aparcamiento para el personal y los visitantes. Las áreas del personal deben ser controladas a través de sistema de entrada de tarjeta magnética, tener barreras físicas y los controles adecuados para evitar su alteración; las plazas de aparcamiento para los visitantes no deben estar en las cercanías de una salida de edificio. Todos los visitantes deben pasar por una zona de control en donde se reportará su ingreso y posterior salida, así como la asignación de un custodio mientras se encuentre en las instalaciones del laboratorio.

Otra característica a considerar es que el edificio en sí debe tener un grado bajo fuego. Esto se logra normalmente a través del uso de materiales resistentes al fuego, lo ideal sería que el edificio debe estar construido con materiales que no permiten que contribuya al proceso de fuego como combustible en el caso de un incendio y que también le permita mantener su integridad estructural. Materiales de carga internas (es decir, materiales contenidos en el edificio) no deben ser inflamables. En áreas donde existe actividad sísmica regular, el edificio debe estar construido de tal manera (o tener una clasificación de construcción) que mitiga estos efectos.

El perímetro del edificio debe usar cerraduras adecuadas en las puertas y ventanas, y éstos deben ser utilizados en conjunto con la iluminación adecuada, sistemas de vigilancia y alarmas. Deben aplicarse láminas a todas las ventanas; esta es una cinta metálica que se aplica a las ventanas para que en el caso de una explosión o cuando alguien intenta romper el vidrio, la lámina evita que el vidrio se haga añicos. En algunos sistemas de seguridad, una pequeña corriente eléctrica se aplica a la lámina por lo que cualquier grieta o al rayado de la ventana se activará una alarma. Del mismo modo, si el material a procesar en el laboratorio es de una sensibilidad suficientemente alta, las paredes o cavidades pueden usar alambres finos para detectar incursión.

El uso de candados y llaves son normalmente un elemento esencial en cualquier instalación segura; sin embargo, se suele pasar por alto una medida de control de acceso físico y con demasiada frecuencia vemos puertas empleadas con bloqueos caros y tarjetas con banda magnética que utilizan paneles de vidrio de media altura, y como resultado, lo que podría permitir que un delincuente simplemente rompa el vidrio y eluda el bloqueo para acceder a la habitación. Todas las puertas (y los marcos en donde se colocan) en cualquier punto de control deben ser de una construcción adecuada sólida y pesada, preferentemente de metal, cuyos paneles de vidrio debe limitarse al tamaño mínimo permitido para satisfacer cualquier requisito de seguridad y salud. Todas las puertas también deben ser de cierre y bloqueo, cualquier puerta que de acceso a áreas sensibles de una instalación deben ser provistas de una alarma acústica que suena si se deja abierta o entreabierta durante un período prolongado de tiempo, los procedimientos deben ser puestos en marcha para garantizar el funcionamiento de las alarmas, esto se puede lograr mediante el uso de interruptores magnéticos o eléctricos contenidos dentro del marco de la puerta. Cualquier movimiento a través de una puerta de control de llave o de entrada debe ser diseñado para eliminar la posibilidad de bloquear accesos no autorizados de personas que traten de ingresar inmediatamente después de un usuario autorizado.

EL USO DE ZONIFICACIÓN INTERNA

La estructura interna del edificio debe tener implementadas zonas de control para el acceso al público, acceso normal (personal externo con escoltas), y el acceso restringido el (el acceso interno restringido basado en la necesidad). La zona debe estar claramente delimitada con la señalización adecuada, un punto que a veces se pasa por alto.

Todos los visitantes deben firmar y registrar su salida, y esto debe ocurrir en un área de atención al público, donde se verifica la identidad de la persona, y en la que se le asigna al visitante a un empleado del laboratorio que será responsable de ellos como su escolta. Todo el personal y los visitantes deben llevar su credencial de identificación en todo momento; los pases para los visitantes también deben mostrar la fecha de expedición y el período de validez. Al concluir la visita, el visitante debe firmar

salida en la zona de recepción y entregar la tarjeta de identificación que se le entrego al momento de ingresar.

CONTROLES DE LA FUENTE DE ALIMENTACIÓN

Como se mencionó anteriormente, la fuente de alimentación debe estar asegurada en el punto de conexión al suministro. Todas las fuentes de poder internas deben estar condicionadas, en otras palabras, un regulador de energía se debe poner en el lugar con el fin de evitar que los picos (un aumento por encima del poder de base) y las caídas de tensión (una disminución de la corriente de la base) dañen los equipos. El siguiente paso es la instalación de un sistema de alimentación ininterrumpida (UPS) que suministra energía en caso de un corte de corriente; la alimentación del UPS se extrae de las baterías de reserva que se mantienen en carga máxima por la fuente de alimentación principal cuando esté disponible.

Al desarrollar el laboratorio, debe calcularse el costo del requisito mínimo para la alimentación de la UPS con el fin de permitir el apagado de equipos de una manera ordenada y controlada.

Los UPSs son de dos tipos principales, estos se denominan como activos o pasivos.

- Activo es un tipo de UPS que es en realidad un regulador de energía y suministra una fuente de alimentación regulada constante a los dispositivos conectados. Estos tipos de UPS mitigan los daños causados por los picos y caídas de tensión.
- Un UPS pasivo supervisa la línea de picos y caídas de tensión y responde por el cambio a la energía de la batería.

La mayoría de los sistemas de UPS utilizan una batería de alta capacidad (normalmente ácido de plomo) para suministrar la energía para la alimentación de reserva. Como resultado, estas tecnologías, por su propia naturaleza, decaerán a capacidad cero durante un determinado número de ciclos de carga/descarga o simplemente la vida útil del aparato.

La vida útil típica de estas baterías es de alrededor de dos a tres años, momento en el que deben ser reemplazados. Una característica habitual en el ciclo de auditoría de TI debe ser el mantenimiento y pruebas de estas baterías, tanto para la capacidad y la habilidad de responder con una carga completa. En la actualidad los UPS tienen software de gestión combinada con el hardware físico. Este software permite la vigilancia activa de la condición de una batería, y algunos de los sistemas han incorporado funciones de alerta basado en umbrales de tolerancia ajustables.

Como se mencionó anteriormente, algunas circunstancias operativas requerirán la provisión de una fuente de alimentación alternativa fiable a través de la capacidad de generación de espera. Esto está

determinado en gran medida por la necesidad de la empresa y estará basado en casos dados, la función de laboratorio y propósito. Cabe señalar que estos sistemas necesitan un mantenimiento regular y pruebas, así, que debe ser realizado por profesional debidamente cualificado y familiarizado con los requerimientos de generación de reserva.

CÁMARAS

Las cámaras de seguridad a lo largo de una instalación permiten la supervisión de las operaciones, y en el caso de un laboratorio forense, debe considerarse obligatoriamente. Las cámaras mismas deben tener una capacidad suficiente para permitir la identificación de una persona dentro de los confines del área bajo vigilancia. Sistemas de CCTV[103] debe registrar y almacenar imágenes de una resolución suficiente para identificar a las personas o las acciones emprendidas en el rango de zona de vista de las cámaras. Las imágenes también se debe capturar a una velocidad que permite la detección precisa de los comportamientos en instancias específicas, sólo tomar una instantánea cada cinco segundos pueden pasar por alto pruebas vitales.

Cualquier área donde se está utilizando CCTV también debe tener controles automáticos de iluminación instalado por lo que un agresor potencial no puede simplemente apagar las luces para evitar la detección. Se recomienda el uso de sensores sensibles al movimiento para que cualquier movimiento dentro de un cuarto oscuro haga que la iluminación se active.

Suficientes cámaras deben ser instaladas para asegurarse de que, sin excepción, cualquier actividad o acciones de cualquier persona sean registradas y documentadas plenamente en áreas de acceso restringido. Además de esto, el material grabado debe ser archivado por un período suficiente de tiempo, ya que pudiesen ser requeridos para investigar cualquier violación o incidentes. El tamaño y la extensión de los archivos es en última instancia una decisión de negocios que será determinado como resultado de las evaluaciones de riesgos y la experiencia. Las cámaras instaladas deben ser una mezcla de dispositivos abiertos y encubiertos en un esfuerzo por documentar todo el comportamiento. En el sistema de cámara también debe tenerse en cuenta las cargas de los UPS de modo tal que la cámara pueda seguir en funcionamiento ante un caso de fallo de alimentación principal.

AIRE ACONDICIONADO

En los laboratorios de computación, el aire acondicionado seco (humedad cero) debe ser utilizado en todo momento. A diferencia de los sistemas evaporadores, este tipo de aire acondicionado no pone

[103] Circuito cerrado de televisión o CCTV (siglas en inglés de closed circuit television) es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades.

el agua en forma de vapor en el aire. Los sistemas de evaporación, si bien son más baratos en costo, estos simplemente no son adecuados para su instalación en un área que utiliza circuitos eléctricos; la razón para la exclusión de los sistemas evaporativos es que el vapor de agua utilizado para crear el diferencial de temperatura se condensa de nuevo en gotitas de agua, y por las leyes de la termodinámica se condensará en un elemento caliente que se está enfriando. Este estado está siempre presente en un equipo cuando está apagado, por ejemplo, los componentes, incluso en un modo de suspensión, se enfriarán por un tiempo, y como resultado se acumulará condensación.

Desde un punto de vista de seguridad física, todos los conductos de aire acondicionado deben ser lo suficientemente pequeño para evitar que un intruso se filtre sin pasar por la seguridad mediante el uso de ellos como espacios de acceso. En el caso de edificios establecidos con grandes conductos, esto puede ser fácilmente realizado con la instalación de parrillas o barreras de restricción adecuadas. Si esto no es factible por una variedad de razones: por ejemplo, los pactos patrimoniales que se adquieren en el alquiler de un edificio, entonces la instalación de sensores y alarmas de movimiento correspondiente se debe ejecutar dentro de estos conductos y canalizaciones.

Las unidades de aire acondicionado deben ser capaces de mantener un constante rango de temperatura ambiente. Dependiendo de su ubicación geográfica, esto determinará el tipo de capacidad de aire acondicionado que necesitará. La carga de calor para el aire acondicionado también varía debido a las cargas estáticas que se crearán en un área o habitación en particular. Muchos factores influyen en el cálculo de la carga de calor, por ejemplo, el número de ordenadores y su salida de calor, así como la posición, la ubicación y tamaño de las ventanas.

Es importante que los cálculos de la carga de calor sean las apropiadas y el trabajo de instalación y diseño sea realizado por profesionales y expertos en aire acondicionado.

CONTROL DE EMISIONES

Las redes inalámbricas (tanto WiFi, 3G, redes de telefonía móvil, GSM, etc.) son una realidad y ahora saturan grandes extensiones metropolitanas. Existe una posibilidad de que estas señales legítimas puedan interferir con el análisis forense de dispositivos sospechosos. Este problema es de particular relevancia cuando, por ejemplo, sea necesario el examen de los teléfonos móviles, PDAs, o computadoras portátiles con capacidad inalámbrica. Con sólo encender estos dispositivos, pueden intentar conectarse automáticamente a una red y comenzar a descargar o sincronizar datos en el dispositivo, el envío y/o recepción de SMS y MMS, actualizaciones de archivos, listas de tareas, etc.

Estas conexiones y saturación de las ondas de radio pueden causar una sobre escritura accidental de pruebas vitales almacenadas en el dispositivo. Por otra parte, en otro nivel, se puede permitir que un

delincuente astuto pueda eliminar las pruebas del dispositivo cuando tenga control de la red y se encuentre conectado en ella. El funcionamiento de los equipos inalámbricos dentro de un edificio también presenta un problema significativo e identificable para la transmisión de las comunicaciones, que puede resultar en la pérdida inadvertida de información. El uso de una jaula de Faraday o de una señal de retardo se justifica como contramedida en áreas donde se utilizan o se examinan estos dispositivos.

El posicionamiento de los monitores del ordenador debe considerarse cuando las ventanas y las superficies reflectantes están presentes en el laboratorio. La colocación incorrecta de un monitor podría potencialmente permitir la supervisión del monitor a través de simple vista, o incluso con el uso de un teleobjetivo desde cierta distancia. Cabe señalar que las personas que siguen la información en casos sensibles no son siempre los acusados, a veces son los medios de comunicación.

Los laboratorios que se ocupan de forma rutinaria con material pornográfico u obsceno deben crear un área de trabajo independiente, acordonar o poner en cuarentena las áreas de estaciones de trabajo involucrados para el trabajo, esto por razones de seguridad y salud mental con el fin de evitar que el personal sin querer vea este tipo de imágenes. En algunas legislaciones solo el perito designado puede manipular este tipo de material.

Otro tipo de emisión que debe ser controlado es la Interferencia Electromagnética (EMI) generados en conductos de energía. El EMI puede ser perjudicial para cualquier cosa que utiliza el magnetismo para el almacenamiento, también puede afectar a la red de transmisión, por lo que la separación de los cables de red de los cables de energía en conductos separados es obligatorio.

CONTROL DE INCENDIOS

El control de incendios es un ejemplo de un servicio que a veces se pasa por alto y puede tener efectos catastróficos para los equipos digitales. Algunos de los equipos utilizados en la ciencia forense digital son relativamente específicos y pueden ser difíciles de sustituir en un corto plazo.

La mayoría de los sistemas de control de incendios en los edificios son rociadores que controlan un incendio por aspersión del área general afectada, con grandes volúmenes de agua. Estos son eficaces, pero no son la mejor solución para computadoras y equipos digitales. En algunos casos, las compañías de seguros no ofrecen cobertura de daños de agua causados por sistemas de incendio cuando el riesgo es un riesgo previsible.

Se necesitará un sistema de dióxido de carbono para las salas de servidores y las zonas de almacenamiento de evidencia. Los sistemas de protección de incendio con agentes

limpios son utilizados para todas aquellas aplicaciones donde los sistemas de protección convencionales como rociadores no son la mejor alternativa por el daño colateral que puedan producir, Los sistemas de supresión con agentes limpios utilizan agentes gaseosos con características importantes como: dieléctricos (no conductores de la electricidad), inodoros, incoloros, seguros para las personas y para los equipos, con estos sistemas se garantiza la protección de los equipos y se evita la interrupción de la operación. Dentro de las aplicaciones de estos sistemas se tienen: centros de datos (Data Center), cuartos eléctricos, cuartos médicos (salas de cirugía, centros de radiologías, farmacias), cuartos de comando o control, sitios de interés público como bibliotecas, en la industria (centro de maquinarias, equipos móviles, plantas de emergencia, generadores, transformadores), en el sistema bancario (bóvedas, cajas de seguridad), entre otros. Estos sistemas de control de incendios pueden ser costosos y requieren mucho tiempo para llevarse a cabo. Así que se debe tener cuidado para seleccionar un sistema que no es en sí perjudicial para ordenadores o medios de almacenamiento.

SEGURO

Un sitio bien asegurado también debe afectar a la tasa de la prima de seguro solicitado. El uso de algunas contramedidas eficaces y reconocidas puede tener un impacto significativo en las primas de seguros para una instalación. Vale la pena ponerse en contacto con los posibles aseguradores y pedir una lista de protección preferente y otros tratamientos.

RESUMEN

En este capítulo se ha examinado una serie de aspectos que deben ser considerados al momento de decidir sobre la ubicación del laboratorio. Los factores que podría afectar las decisiones acerca de la ubicación geográfica del laboratorio y su posicionamiento dentro de un edificio han sido examinadas y tratados diversos temas.

Por último, se han realizado recomendaciones sobre los servicios que se requieren para que el laboratorio funcione con eficacia.

CAPÍTULO 6: SELECCIÓN, EDUCACION Y FORMACION DEL PERSONAL DE LABORATORIO FORENSE DIGITAL

INTRODUCCIÓN

En este capítulo se discutirá una serie de cuestiones relacionadas con la selección del personal idóneo para el laboratorio. Esto incluirá la evaluación de la idoneidad del personal, calificaciones, experiencias, referencias, antecedentes y un examen de seguridad. El capítulo también se ocupará de la necesidad de la provisión de apoyo para el personal el cual debería incluir el acceso a consejerías y evaluaciones psiquiátricas.

Hay pocos argumentos requeridos del personal necesario para un laboratorio forense digital, en donde se requerirán una variedad de habilidades y experiencias. Hay varias funciones operativas claves, sin embargo, no se requiere de ninguna configuración de laboratorio, independientemente del tipo de tareas forenses digitales emprendidas. Estas funciones pueden ser esenciales a tiempo completo, independientemente del tamaño del laboratorio, uno de los miembros del personal puede realizar una serie de funciones diferentes dentro de su trabajo.

ROLES EN EL LABORATORIO

A continuación se detallan los principales roles que tendrán que ser realizados en el laboratorio. El tamaño del laboratorio, el tipo de organización y el tipo de trabajo que se llevará a cabo. Esto afectará la decisión de la administración si una o más funciones se combinan o si hay varios miembros del personal designados para llevar a cabo una de estas funciones. Si el laboratorio es grande, entonces puede ser necesario crear otros roles.

EL GERENTE DE LABORATORIO

El gerente del laboratorio será responsable de la gestión del día a día del laboratorio. Esto incluiría funciones tales como la planificación de tareas, gestión de la continuidad del negocio, gestión de documentos, la gestión de calidad y procesos de revisión, gestión de recursos humanos y la gestión de la seguridad. Además, el director del laboratorio podría estar a cargo de la responsabilidad de la gestión financiera de las operaciones.

ANALISTAS Y EXAMINADORES FORENSES DIGITALES

Los examinadores y analistas son competentes en el uso de uno o más instrumentos en procesos forenses digitales a un nivel experto. Estos roles suelen tener, como mínimo, un certificado del proveedor de la herramienta forense del producto que se está utilizando, o una formación importante en la experiencia del trabajo. Preferiblemente, estas personas también tendrán alguna titulación

superior en una disciplina adecuada, por ejemplo, la informática o la ciencia forense digital, títulos universitarios, formación en criminalística, certificaciones internacionales en la materia y las herramientas utilizadas por el investigador le darán mayor entidad a sus dictámenes periciales.

ADMINISTRADORES E INVESTIGADORES DE CASO

Los administradores e investigadores no tienen que ser expertos forenses digitales, pero tendrán que estar capacitados en temas de ciberdelincuencia y temas forenses digitales. Ellos serán las personas que actuarán como enlace o interfaz con el mundo exterior y con otras agencias. Estas personas serán responsables de la gestión del día a día de los procedimientos y de la interacción dentro y fuera del laboratorio.

TÉCNICOS DE LABORATORIO

Un técnico de laboratorio tiene un nivel de habilidad que les permite realizar con seguridad y eficacia un conjunto de tareas básicas en el laboratorio, con respecto a los estándares definidos, procedimientos y métricas. El tipo de tarea que habitualmente lleva a cabo un técnico de laboratorio supondrá un conocimiento fundamental que está incrustado tácitamente en la lógica del dispositivo o proceso que se utiliza. Un buen ejemplo de esto es la operación de una herramienta de imagen como Rimage o Silo 3, donde gran parte de la interacción es la verificación, selecciones del menú y la fijación de hardware.

Estos roles técnicos se realizan en apoyo de las tareas que requieren un mayor nivel de conocimientos o comprensión cognitiva, por ejemplo, el examen y el análisis de los datos contenidos en un disco duro de Windows con formato NTFS. Mientras que un examinador experimentado sería capaz de generar o replicar las imágenes de los medios de comunicación, aunque no es lo mejor y más productivo de su tiempo.

En general, el número y la especificación de estas funciones técnicas dependen típicamente en el enfoque y la carga de trabajo del laboratorio. La única excepción es que todos los laboratorios tendrán necesidad de un técnico de imagen. Un técnico de imagen es responsable de la adquisición de datos de los dispositivos digitales y recabar imágenes forenses para validar que se mantenga la continuidad de las pruebas sobre una documentación adecuada. Esto sólo se puede lograr utilizando métodos y herramientas que podrían posteriormente ser analizadas por cualquier examinador forense digital para la corrección de la operación de las herramientas y el proceso de validación.

SELECCIÓN DEL PERSONAL

La selección eficaz del personal es fundamental en cualquier ámbito de trabajo; sin embargo, dentro del área de análisis forense digital, la mala selección dará como resultado, procesos deficientes que

pueden atraer consecuencias catastróficas. El personal que ha utilizado procesos deficientes, haya deliberadamente malversado las aplicaciones y no haya cumplido con las normas prescritas podría involucrar todas las pruebas y hacerlas inadmisibles en algún caso. Aunque la evidencia no es declarada inadmisible, se pone en duda la credibilidad del laboratorio y conduce al cuestionamiento de todos los resultados producidos en él. Por tanto, es imprescindible que la selección del personal sea un proceso bien estudiado que ofrezca los mejores candidatos disponibles.

CUALIFICACIONES VS EXPERIENCIA

En un laboratorio forense que está empleando procesos científicos sólidos para capturar, identificar y extraer los datos para su posterior presentación ante un tribunal de justicia o tribunal como evidencia, el personal debidamente cualificado es esencial. El personal que supervisa o realiza un análisis sobre el tratamiento de las pruebas debe ser capaz de presentar sus resultados en los tribunales. Con la experiencia suficiente, también debe ser capaz de actuar como testigo experto (esto puede variar dependiendo de la jurisdicción). El personal debe ser capaz de hablar y presentar argumentos convincentes, tanto en un alto nivel técnico para explicar temas complejos en términos simples, en su área de especialización. El procesamiento de la evidencia de que cualquier especialista en el análisis forense digital ha seguido, debe utilizar principios científicos sólidos, para describir con coherencia y precisión cada proceso llevado a cabo. Por el contrario, el personal también debe ser capaz de analizar a otros expertos y defender reclamaciones formuladas por los expertos opuestos.

El personal que se reconozca de ser capaz de prestar un testimonio ante un tribunal de justicia en calidad de experto, normalmente se debe haber validado en base a los conocimientos de esa persona. Tradicionalmente, esto se logra a través del reconocimiento establecido en la educación formal y los procesos científicos académicos, que normalmente tiene realización con un título universitario en una disciplina relevante. Este grado es normalmente validado junto con otro estudio de investigación en el área de la especialización. Esta es una vía adecuada y reconocida en el ámbito de la ciencia forense tradicional; sin embargo, debido a su muy corta historia y la rápida evolución de del área, la ciencia forense digital tiene algunos temas de actualidad.

Uno de los problemas claves con la selección del personal es la evaluación de sus competencias o experiencias en análisis forense digital. Actualmente, no hay normas de competencias obligatorias para los examinadores forenses digitales, ya sea por una organización gubernamental o una asociación profesional reconocida. La aparición de determinados grados y cursos forenses digitales son recientes.

Los títulos universitarios actuales en TI proporcionan una base sólida para los examinadores de la informática forense a nivel técnico. Sin embargo, será necesaria la formación con respecto al puesto de trabajo en el uso de herramientas y procesos forenses específicos, además de un título o

certificación. Por otra parte, un título de las ciencias de la informática rara vez se ocupa en cuestiones legales y probatorias, por ejemplo, en la continuidad de las pruebas, los conceptos jurídicos y problemas encontrados en ámbitos de ley. Estos temas se abordan en el trabajo o requieren mayor capacitación externa.

La capacitación de los proveedores en aspecto de habilidades es un filtro potencial para una competencia forense digital y a nivel de experiencia. Cabe señalar que la capacitación de proveedores normalmente sólo proporciona el título del uso de paquetes específicos de ese proveedor. Esta formación normalmente no es suficiente para que una persona sea calificada como investigador forense digital. Es eminentemente plausible que una persona que no tiene un conocimiento profundo de la informática o la ciencia forense podría completar la formación de estas certificaciones por parte de estos proveedores con éxito y lograr la certificación en el uso de un paquete o suite de software particular. Sin embargo, la ausencia de normas establecidas para la presentación de pruebas como experto dentro de otros campos de la ciencia forense digital, pueden añadir peso a la determinación de conocimientos técnicos.

Recientemente un grupo de forenses digitales en Australia, en aplicación a leyes nacionales, estatales, académicas y sectores comerciales han desarrollado un marco para evaluar las competencias de los investigadores forenses digitales. El marco que se ha desarrollado se divide en tres áreas principales de habilidades:

1. El primero de ellos es la adquisición y preservación de la evidencia original.
2. La segunda área se ocupa del análisis de las pruebas, que es la producción de un análisis científico usando procesos forenses, tecnológicos y técnicas válidas.
3. El tercero es el informe de pruebas y presentación, la presentación de pruebas a terceros, tribunales de justicia externos son a través de la presentación convincente de los hechos que han sido revelados por una investigación.

SELECCIÓN DE EMPLEADOS

No hay duda de que las pruebas psicológicas y de organización son ciencias imperfectas; sin embargo, tienen las condiciones para la detección de empleados potenciales que pueden resultar difíciles de manejar o que no son aptos para su designación. Los test psicológicos pueden detectar al personal que tiene problemas potenciales con la integridad, honestidad y posteriormente pueden ser que acepten sobornos, se encuentren en casos de corrupción u otras prácticas indeseables. El análisis forense digital trata cuestiones que pueden ser angustiantes e inquietantes en una serie de niveles. Las pruebas psicológicas se pueden utilizar para filtrar los candidatos que son más propensos o susceptibles a los efectos de estas tensiones. El uso de este tipo de pruebas permite al empleador

tomar una decisión más acertada. Sería temerario, por ejemplo, dar una tarea a un investigador un caso de contrabando de arañas si el padece de aracnofobia. Algunas pruebas se pueden utilizar para determinar con fiabilidad las habilidades en la resolución de problemas, que son una habilidad crucial para cualquier examinador forense digital.

Algunas pruebas de personalidad como la de Myers Briggs[104] pueden resultar útiles en el proceso de selección del personal. Este tipo de pruebas se pueden utilizar para crear una mezcla más optimizada de los tipos de personalidad. Esta prueba sería la más apropiada en un laboratorio de investigación ya que no todas las soluciones probables son adecuadas para un determinado tipo de personalidad o rasgo, y también muchos tipos de personalidad en la organización pueden ser contraproducentes.

El trabajo en equipo es un elemento esencial en un laboratorio forense digital, incluso si el laboratorio es un equipo de dos personas. Estas pruebas psicológicas y de organización pueden identificar fácilmente el personal que no se adecuen a grupo o a un trabajo en equipo.

REVISIÓN DE ANTECEDENTES

Otro aspecto importante para la selección del personal es de investigar y verificar previamente todos aquellos antecedentes potenciales de un candidato. Esto incluiría, pero que no se limitan a los controles financieros, referencias de empleadores anteriores, antecedentes policiales y la verificación de títulos y certificaciones pertinentes.

En la investigación del control financiero es importante verificar la solidez o resaltar posibles problemas en el comportamiento del personal. Un ejemplo de un problema de este tipo puede ser el descubrimiento de préstamos múltiples a corto plazo, deudas de tarjeta de crédito, posiblemente indicando un problema de juego u otras cuestiones personales que no sean de una mala gestión fiduciaria y que podrían tener un impacto en el trabajo. Deudas recurrentes de este tipo son excelentes vectores para objetivos de soborno o corrupción, ya sea el de permitir mayor compromiso o la ampliación de malos comportamientos.

Los antecedentes policiales son una forma de asegurarse de que el futuro empleado no tenga algún tipo de antecedente penal en curso. Este tipo de información proporciona una indicación de cualquier delito grave que pueda haber ocurrido en el pasado. Algunas jurisdicciones, sin embargo, tienen límites sobre la cantidad de información que puedan proporcionar en este sentido. Por ejemplo, en algunas jurisdicciones hay un límite en el número de años que está disponible esta información.

[104] El Indicador de tipo de Myers-Briggs (o MBTI por sus siglas en inglés) o, más brevemente el Indicador de Myers-Briggs, es un test de personalidad diseñado para ayudar a una persona a identificar algunas de sus preferencias personales más importantes

La verificación de títulos que se reclaman es otro proceso importante en la investigación de la selección del personal. Esto es particularmente importante en el actual entorno digital forense debido a la falta de certificaciones y cualificaciones dentro del área de la disciplina. Para la verificación de algunas certificaciones se requiere un ID de prueba por parte del candidato. Cabe señalar que muchas certificaciones de la industria expiran después de períodos relativamente cortos. Por titulaciones, como títulos o diplomas expedidos por autoridades judiciales, acreditaciones en escuelas técnicas, universidades, entre otros, igualmente necesitan verificación. Ha habido numerosos casos en el mundo donde los individuos han afirmado tener títulos que en realidad no poseen. Incidentes como estos hacen que sea esencial verificar la institución certificadora de que la persona ha completado el grado o título en cuestión.

AUTORIZACIONES DE SEGURIDAD

Las autorizaciones de seguridad son importantes y sobre todo tienen un impacto en el sector privado. Los sectores forenses digitales de investigación (por ejemplo, la policía, fuerza militar o las organizaciones secretas del gobierno que tienen que ver con material clasificado o restringido) normalmente ya tienen procedimientos y sistemas bien establecidos en relación a controles de seguridad.

APOYO PARA EL PERSONAL

Por desgracia, todavía hay una alta proporción de cantidad de casos en investigaciones forenses digitales que tienen que ver directamente con la posesión y distribución de imágenes ilegales. Estas imágenes y películas son típicamente de naturaleza sexual, involucran a niños menores, zoofilia, o asesinato (películas snuff[105]). Estas imágenes y películas son gráficas, a menudo violentas y en última instancia perturban en la naturaleza del ser.

La exposición a largo plazo de este tipo de material podría causar la desensibilización a lo mejor. Es más probable que el personal desarrolle daños psicológicos como resultado de la exposición a largo plazo de este tipo de material. Incluso el personal que puede parecer no ser afectado por una cantidad de tiempo considerable, posiblemente, puede desarrollar trastornos de estrés post-traumáticos. Para contrarrestar este tipo de daños el personal a cargo, siempre que sea posible, se deben rotar los puestos de trabajo para reducir al mínimo el nivel de exposición. Ha habido muy poco en el camino de la investigación sobre los efectos de la exposición prolongada a este tipo de imágenes y películas, principalmente debido a lo reciente de este tipo de material en Internet. Paralelismos razonables

[105] Las películas snuff o vídeos snuff son supuestas grabaciones de asesinatos, violaciones, torturas y otros crímenes reales (sin la ayuda de efectos especiales o cualquier otro truco) con la finalidad de distribuirlas comercialmente para entretenimiento.

pueden extraerse de otras áreas en las que la exposición a largo plazo a los eventos traumáticos ha dado lugar a la necesidad de controlar ese estrés en los recursos humanos de una empresa.

La mayoría de los sistemas de gestión establecidos para los delitos informáticos o equipos forenses digitales requieren pruebas psicológicas regularmente en el personal. Sin embargo, el período de revisión es muy variable, en algunas organizaciones se requieren chequeos mensuales, mientras que en otras organizaciones pueden ser de 12 hasta 18 meses. Este intervalo dependerá en gran medida el tipo y nivel de casos llevados a cabo durante un período determinado. También es importante que el tiempo del personal con respecto a la cantidad de tiempo empleado en estos casos, o dentro de estas áreas, se registrado con precisión.

La prestación de servicios de asesoramiento al personal puede mitigar fácilmente algunos de los riesgos relacionados con la exposición a largo plazo a este tipo de material gráfico. La prestación de servicios de asesoramiento puede prevenir o mitigar un problema relativamente menor en la salud mental del individuo involucrado en este tipo de trabajo. Alternativamente, el asesoramiento puede ayudar en la evaluación continua la salud mental del individuo. Estas evaluaciones dan una idea de las prácticas de gestión y las estructuras de la salud mental del equipo.

La creación y el uso de programas de tutoría donde el personal más capacitado y con más experiencia proporcione apoyo a los empleados más jóvenes para que puedan proporcionar un mecanismo de apoyo adicional para hacer frente a los problemas que puedan surgir. La mayoría de personal capacitado habrá experimentado muchas de las cuestiones críticas que los trabajadores jóvenes podrían encontrar en un determinado momento, los trabajadores con poca experiencia deberían expresarse a los funcionarios de alto rango sus sensaciones de este tipo de casos para promover las experiencias vividas.

AUXILIARES Y AGENTES CONTRACTUALES

Los auxiliares y agentes contratados no son las personas que realmente realizan el procesamiento o análisis del material dentro del laboratorio forense digital. Este tipo de personal son los que realizan tareas auxiliares, como la limpieza, el mantenimiento del sitio dentro de las instalaciones del laboratorio. El personal en realidad no puede ser empleado directamente del propio laboratorio, pero puede ser parte de los acuerdos de terceros. Esto puede presentar más problemas para tener una instalación de seguridad y es uno de los aspectos que a veces se pasa por alto porque este personal es visto como un "problema de otra persona."

Otra categoría que debe incluirse en este grupo es el personal de TI subcontratado que puede utilizarse sobre una base contractual. En el caso del personal de TI contratado, a menudo hay poca

necesidad de hacerles entrar en un área restringida con el uso de VLAN adecuada (red de área local virtual) o una VPN (red privada virtual) se tiene mucho más control. Esta categoría de personal puede estar contenido en una DMZ[106] físico, por así decirlo, dentro del edificio, restringiendo su acceso a algunas zonas. Esto puede tener algún impacto significativo en los requisitos de diseño y espacio de la red; sin embargo, esto puede ser contrarrestado fácilmente por el aumento de la seguridad física. Algunos gerentes financieros pueden ver el espacio adicional para este tipo de contención como un gasto. Pero no debe ser considerado de esta manera en cuanto a seguridad.

Cuando el personal auxiliar o contractual tiene acceso a una instalación de mayor nivel que un miembro del personal de laboratorio a tiempo completo, las evaluaciones de seguridad y las asignaciones son defectuosas. Este personal, como mínimo, debe ser sometido a los mismos procedimientos de inspección de seguridad y de investigación de antecedentes que el personal interno del laboratorio. El personal que necesite acceder a las zonas restringidas o áreas que requieren autorización de seguridad externa debe tener los mismos niveles que los usuarios regulares en relación al acceso.

EDUCACIÓN Y FORMACIÓN

En este apartado se abordará la necesidad de la formación del personal para lograr el equilibrio entre la formación necesaria y mantener una unidad efectiva con un entrenamiento exhaustivo. Es probable que este tipo de formación cause gastos innecesarios y deje a la organización vulnerable a la caza furtiva de personal por las empresas u organizaciones rivales. También se abordará una estrategia para el desarrollo de áreas especializadas dentro de los equipos de trabajo. La mayoría de organismos profesionales tienen un nivel mínimo de educación, aunque tienen mecanismos de formación para que los usuarios puedan estar al día. El área de análisis forense digital en la actualidad tiene pocos órganos de carácter global para la representación profesional donde estén estipulados estándares educativos profesionales a un nivel mínimo para convertirse en un investigador forense digital.

FACTORES EXTERNOS

Las industrias de TI y comunicaciones continúan creciendo a un ritmo exponencial y así mismo se están produciendo nuevas tecnologías, dispositivos y sistemas operativos. Este rápido crecimiento impacta sobre la necesidad de la formación continua de los profesionales forenses digitales. Por ejemplo, la

[106] En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

cronología de los sistemas operativos de 32 bits de Windows ha evolucionado con una serie de sistemas operativos que el investigador forense digital debe examinar.

Mientras los sistemas de archivos para estas variantes como: FAT16, FAT32, HPFS y NTFS, que son la estructura del registro del sistema puede variar considerablemente. Sin embargo, el registro del sistema tiene principios similares de operación a través de las diferentes versiones de Windows.

La misma variedad en sistemas operativos están a la disposición, como el sistema operativo Macintosh, Unix, Linux, IBM AIX, HP/UX, SunOS y Sun Solaris. Sin embargo, debido a la posición dominante de Microsoft en el mercado de sistemas operativos, un investigador forense digital debe estar capacitado para hacer frente a más del 90 por ciento de los sistemas operativos y sistemas de archivos instalados en las diferentes computadoras que pudiera encontrar en una investigación.

Patrones similares surgen en el área de dispositivos móviles. La línea de tiempo para el iPod de Apple ha estado en plena evolución desde del 2002 hasta la fecha[107]. Cada uno de estos iPods, aunque en una forma similar, contienen una serie de diferencias. Ellos utilizan un sistema en un chip diseñado por Apple. Los dispositivos iPod son comúnmente particionados, ya sea como un iPod basado en Windows mediante una partición FAT32 o como un iPod basado en Macintosh mediante un sistema de archivos HFS+[108]. Cada uno de estos sistemas de archivos requiere conjuntos de herramientas y bases de conocimiento diferente para el examen forense de lo que externamente parece ser el mismo dispositivo.

De igual manera otros dispositivos móviles, tales como teléfonos móviles, Smartphone y PDAs tienen tantas complejidades potenciales como en el uso de la memoria, sistemas de archivos, herramientas y técnicas.

SOFTWARE FORENSE

Las herramientas de software forense (y suites de herramientas) realizados por los diferentes proveedores tienen discrepancias y diferencias en la forma en que operan. Si bien un especialista forense puede comprender los procesos y procedimientos forenses que se realizan mediante el uso de software durante un proceso forense, en muchas ocasiones se logra de diferentes formas.

Los proveedores de software a menudo obtienen gran parte de sus ingresos en la formación y certificación de individuos. Dichos proveedores generan ingresos mediante la liberación de nuevas y mejoradas versiones de su software para hacer frente a las nuevas tecnologías o las nuevas

[107] http://en.wikipedia.org/wiki/Template:Timeline_of_iPod_models
[108] HFS Plus o HFS+ es un sistema de archivos desarrollado por Apple Inc. para reemplazar al HFS (Sistema jerárquico de archivos).

problemáticas que se han descubierto con las tecnologías existentes. La organización debe cuestionar el gasto de más de $2,000 para una licencia y luego el gasto para realizar el entrenamiento a un nivel de certificación en cada versión de la herramienta de software del proveedor. Muchas veces se piensa que con la compra de herramientas termina el problema y no se tiene en cuenta la capacitación que es fundamental para el correcto aprovechamiento y explotación de las funcionalidades de la herramienta. La capacitación representa un costo que muchas veces no se tiene en cuenta. A manera de ejemplo, una licencia de EnCase Forensic tiene un costo de $3,600, incluyendo el mantenimiento y las actualizaciones por un año (SMS). La capacitación oficial tiene tres niveles: introductorio, intermedio y avanzado, cada uno es un curso de 32 horas con un costo de $2,500 por asistente.

No hay duda de que la ciencia forense digital es un área de rápido movimiento en comparación con áreas forenses tradicionales más maduras, donde se producen los cambios a un ritmo mucho más lento. Las áreas forenses tradicionales también requieren que cualquier miembro del personal sea competente en su área de especialización y que reciba formación en las herramientas y técnicas necesarias para su trabajo diario. Sin embargo, debido a que el ritmo del cambio y el desarrollo de herramientas y técnicas se llevan a cabo durante un período más largo, los gastos generales de la formación y la habilidad de mantenimiento es mucho menor.

El enfoque que se ha adoptado en la actualidad en la ciencia forense digital gira en torno a la provisión de la formación basada del proveedor de nuevas versiones de software que puedan ser realizados por un miembro del personal, preferiblemente el oficial de entrenamiento, o si es posible todo el equipo. Cualquier método tiene un gran costo asociado con él.

El modelo de formación orientado al oficial de entrenamiento permitiría entonces al oficial de entrenamiento poder construir y documentar un proceso para actualizar conocimientos del software, capacitar y evaluar el conjunto de habilidades al personal que estará involucrado en el nuevo sistema o técnica como mecanismo de procedimiento. Algunos proveedores también tienen esquemas de instructores certificados los cuales entrenan al personal designado de acuerdo a su rol.

Este modelo de formación o certificación para el oficial de entrenamiento requiere un esfuerzo considerable por parte del oficial de entrenamiento en cuanto al aprendizaje de los contenidos y el desarrollo del plan de estudio. Esto a menudo incurre en un costo significativo y tendría que tenerse en cuenta en cualquier decisión. Los retrasos en el suministro de la capacitación pueden ocurrir como resultado del ciclo de aprendizaje del oficial de entrenamiento para adquirir las habilidades necesarias.

Aunque la formación puede ser adaptada para satisfacer los requerimientos de la organización, de hecho puede introducir directrices en lo que respecta al argumento de las competencias internas de

formación del personal. Se debe tener en cuenta la posición de que si un miembro del personal se enfrenta en un caso jurídico con un abogado defensor y si este saliese con este tipo de preguntas: ¿Tiene usted experiencia en recabar las pruebas en disputa con la herramienta EnCombobulator 2008 y la opción 12 del menú? ¿Puede aclararnos la opción 12 del menú? A pesar de que sólo puede ser el menú Ayuda, si el funcionario no es capaz de responder a esto, podría ser perjudicial para su credibilidad. Por lo tanto, es importante que siempre que sea posible ningún tipo de formación en la empresa sea sometido a la revisión por algún proceso externo de validación para garantizar la integridad del contenido de la certificación.

El modelo basado en la formación del proveedor dispone una serie de beneficios para la organización. La primera ventaja es que se trata de una validación externa del nivel de habilidades del practicante por un tercero. Otra es que están normalmente bien documentados y pueden ser apoyados por libros de texto.

En segundo lugar, la formación mediante el proveedor se basa en un plan de estudio desarrollado que sería entregado a todas las partes que deseen obtener la certificación de la misma manera. Esto reduce potencialmente la probabilidad de cualquier disputa sobre la competencia de un individuo en particular que ha llevado a cabo la formación y obtenido la certificación. También proporciona una medición inicial de la competencia para el experto.

Por último, los exámenes para estas certificaciones son gestionados por organizaciones independientes que están separadas del proveedor del software o hardware. Esto confirma una vez más y valida la independencia del proceso. Sin embargo, esta certificación de habilidades da al empleado la oportunidad de exteriorizarlos en su currículo vitae y utilizarlo en la búsqueda de empleo con otra organización.

EDUCACIÓN SUPERIOR

El análisis forense digital es una disciplina emergente que tiene su base en lo forense y la informática. Muchos de los investigadores forenses digitales más competentes y experimentados de hoy en día provienen de instituciones de la aplicación de la ley y de organismos militares, algunos de ellos sin carreras académicas de esta rama de la informática forense y con muy pocos títulos académicos tradicionales para respaldar su nivel de especialización. La mayor parte de sus experiencias las han formado en sus puestos de trabajo, sin embargo, muchos de estos expertos están actualmente llevando a cabo cursos de educación superior como resultado de los cursos de informática forense que ahora se ofrecen y se encuentran disponibles.

En el sector de la educación superior hay una oferta de cursos en la ciencia forense digital en pregrado y de posgrado a nivel internacional; sin embargo, sólo unas pocas instituciones ofrecen realmente un grado completo en seguridad informática o en la ciencia forense digital. Una licenciatura normalmente tarda de tres a cuatro años de estudio a tiempo completo. Estos cursos suelen consistir en un primer año en el que los estudiantes aprenden los fundamentos teóricos y conceptos rudimentarios para su uso en las especialidades de segundo y tercer año.

La finalización de la educación superior es un proceso mucho más lento para lograr un título en comparación con la formación basada de un proveedor. Cabe señalar, sin embargo, que el beneficio de esta formación se puede realizar como un objetivo de estudio dentro de la educación superior. Por ejemplo, el estudiante universitario puede obtener una certificación en dispositivos móviles u otra certificación de la ciencia forense digital. Las habilidades y conocimientos alcanzados se pueden usar casi de inmediato y no se limitan a la operación de la herramienta de un proveedor específico, pero de igual manera se necesita una comprensión más amplia de los problemas subyacentes.

Dependiendo del país en el cual se emprendan los estudios, pueden ser sin costo, de bajo costo, un alto costo o basado en cuotas; sin embargo, lo económico es un factor determinante en la calidad. Otros factores importantes que deben ser tomadas en cuenta a la hora de seleccionar las opciones de educación. En primer lugar, es si el proveedor es acreditado a nivel internacional. En segundo lugar, es el nivel de experiencia de los que dirigen el programa. En un ambiente universitario, esto normalmente significaría que los docentes cumplan con algún título universitario a nivel de postgrado o un nivel doctoral. En tercer lugar, el personal que imparte los conocimientos debe ser activo en la investigación en el tema apropiado.

Uno de los diferenciadores claves con la educación superior es que hay un mayor nivel de compromiso intelectual y una comprensión del tema, en comparación con el entrenamiento. La diferencia entre una persona educada y una persona entrenada es que mientras una persona entrenada sabe qué "botones apretar" (aplica un principio), una persona educada sabe por qué, puede explicar el por qué y muy probablemente pueda construir un mejor botón (aplicar, describir y analizar).

Un problema a menudo es que muchos practicantes experimentados toman la educación superior como una ruta no válida de formación para satisfacer sus requisitos. Por lo que algunos programas de educación superior proporcionarán algún tipo de créditos en función de la formación previa y la experiencia, lo que acorta la duración de la carrera. Estas exenciones están sujetas en ocasiones a que el candidato debe completar una evaluación de desafío que es típicamente la forma de un examen.

Esto se hace para certificar que la persona tiene un conocimiento suficiente de los conceptos y contenidos.

BALANCE

Hay pocos argumentos de que los profesionales forenses digitales deban recibir capacitación para retener la competencia. Sin embargo, los problemas en tratar de determinar el nivel adecuado de formación para los investigadores forenses son complejos. La ciencia forense digital cuenta actualmente con una falta de personal debidamente cualificado, y una ventaja competitiva puede ser adquirida a través de la formación en una herramienta o técnica en particular. Entra en juego la constante evolución de la tecnología informática, la cual se logra solo con la práctica y el reforzamiento del conocimiento.

DESARROLLO DE ESPECIALIDADES

La forma más eficaz de obtener una formación, normalmente es el enfoque basado en el equipo, porque la mayoría de los equipos no funcionan por consenso, es importante contar con los jefes de equipo. Estos líderes deben ser la persona reconocida por su experiencia o especialización en un área determinada de la disciplina. No se espera que el personal sea experto en todos los aspectos de la ciencia forense digital, y mucho menos con la creciente diversidad de dispositivos, esto simplemente no es posible. Con la formación en equipo, es posible dar al personal un sentido de valor en el equipo, un lugar en la organización y un sentimiento de pertenencia. Estudios como el estudio del Efecto de Hawthorne[109] (mayo, 1932). Lo que el estudio demostró fue que hay un aumento de la productividad de los trabajadores y de bienestar cuando el personal se siente importante y parte de un equipo.

El desarrollo de especializaciones puede ser un arma de doble filo. El análisis forense digital por su naturaleza casi exige el desarrollo de especialistas; sin embargo, este mismo acto de especialización desarrolla diferencias, se puede utilizar como punto de apalancamiento para más recompensas, o como un camino para salir de la organización. Si el desarrollo de especializaciones se desarrolla bien puede dar a un equipo un equilibrado y una ventaja significativa sobre sus competidores.

Una organización de aprendizaje es aquella que valora su personal y el capital intelectual que posee. Empresas como Nokia, Shell, BP y otras que han utilizado estos enfoques con sus ejecutivos y equipos durante muchos años. El concepto básico es que para conseguir un ascenso o una recompensa, un individuo debe aumentar de manera tangible el nivel de habilidad de los subordinados o pasar activamente el conocimiento para el equipo. El mismo enfoque se debe utilizar con un equipo forense

[109] El Efecto Hawthorne es una forma de reactividad psicológica por la que los sujetos de un experimento muestran una modificación en algún aspecto de su conducta como consecuencia del hecho de saber que están siendo estudiados, y no en respuesta a ningún tipo de

digital. Este enfoque no sólo impulsa la diversificación, si no que se propagan las habilidades especializadas entre su personal y se convierte en un sistema de auto-replicación de difusión y desarrollo. Este tipo de gestión del capital intelectual es vital para que el equipo de análisis forense digital tenga éxito a largo plazo. Este enfoque también amortigua la crisis organizativa que puede suceder cuando una de las "estrellas" sale.

Algunas especialidades básicas fundamentales necesarias para un equipo forense digital en base a un marco de especialización, podrían ser:

ADQUISICIÓN: Las habilidades en la obtención de evidencias de dispositivos digitales se están convirtiendo en algo muy especializado, con tal de satisfacer la demanda de una gama cada vez más amplia de dispositivos. Hay formación genérica en los sistemas de herramientas, métodos y sistemas de archivos de computadoras que todos los investigadores forenses deben llevar a cabo. A mediados de la década de 1990, en su mayor parte, esto habría sido suficiente para la mayoría de las fuentes de los datos encontrados durante la adquisición de datos. Ahora, sin embargo, debido a la explosión de fuentes de evidencia digital las habilidades deben ser promovidas. Algunos de los dispositivos emergentes que se pueden encontrar son los teléfonos celulares 3G, PDAs, dispositivos integrados (iPods, USBs), firmware, redes y productos GPS, por nombrar sólo algunos.

ANÁLISIS: El análisis de los datos es una habilidad básica. Hay, de nuevo, una serie de competencias genéricas que todos los examinadores deben tener con respecto a la palabra clave de búsqueda, indexación y extracción de datos. Sin embargo, también hay habilidades especiales que se pueden desarrollar en cuanto a registro, file carving[110], la extracción y la ingeniería inversa.

PRESENTACIÓN: La presentación de los datos en una forma de redacción de informe y la presentación oral de contenido es una habilidad en sí misma. Sólo porque una persona es técnicamente brillante, por ejemplo, es un experto en la disección de código malicioso, no significa que sea un experto en la presentación de la misma.

PLANIFICACIÓN Y PRESUPUESTACIÓN

La mayoría de las versiones de software basados en proveedor se llevan a cabo con un programación que se publica con antelación. Estas fechas de lanzamiento previstas permiten a la organización planificar con eficacia el presupuesto de todos los requisitos de la capacitación del proveedor. A su vez, esto permite una adecuada gestión del recurso humano. Una buena gestión se produce al

[110] File carving is the process of reassembling computer files from fragments in the absence of filesystem metadata.

asegurarse de que el personal pertinente estará disponible para asistir a la capacitación y que se adapta a sus necesidades y las necesidades de la organización.

Con el fin de estimar los requerimientos del presupuesto, se debe tomar en cuenta los niveles de competencia que existen dentro de la organización. El costo total de la capacitación también incluirá el coste de la sustitución de la persona que está recibiendo la capacitación, el suministro de viaje, alojamiento, viáticos y otro gasto que se justifique. En la formación basada en la universidad, puede haber poca o ninguna carga directa en el costo de la organización, se deben considerar los honorarios de los cursos, temas en la planificación y el presupuesto. Puede haber algún impacto directo en el calendario laboral de la persona ya que muchos de los cursos se ofrecen sobre una base de tiempo estipulado. Las organizaciones deberían de dar la oportunidad de estudio en reconocimiento de la necesidad de tener capacitado a su personal ya que esto repercute en la capacidad operativa de la empresa.

La mayoría de las organizaciones que no proporcionan apoyo logístico y organizativo para la formación y la educación de sus empleados crean un ambiente de resentimiento. En el lado positivo, las organizaciones que brindan apoyo tienden a generar lealtad y presentan una decisión importante de oportunidad para los empleados con beneficios en la empresa.

EVALUACIÓN DE LA FORMACIÓN Y COMPETENCIA

Muchas instituciones envían su personal a capacitaciones y esperan que el personal gane las habilidades necesarias. Por desgracia, a menudo hay muy poca evaluación realizada en base a las competencias transferidas más allá de una prueba sencilla al final de la capacitación. Esto no es el resultado más satisfactorio. Una de las mejores maneras para que la organización se beneficie y que los empleados demuestren las competencias aprendidas es por medio de la transferencia de habilidad a otros miembros del equipo.

Uno de los peligros en la actualidad con la formación en el dominio de la ciencia forense digital es que gran parte de la educación es la formación impulsada por los proveedores y este tipo de educación que se ofrece es, en realidad, la formación específica sobre el producto de un proveedor y la ejecución de la misma para lograr resultados con ese producto dado. Si bien es esencial para el uso eficaz y adecuado de las herramientas, esto no es realmente la educación. Es fundamental la idea de cómo el proveedor vende la formación en su software o hardware. Pero la educación es acerca de las teorías y principios del funcionamiento que permitan el aprendizaje permanente, mientras que el entrenamiento se da para lograr un objetivo final con una herramienta determinada. Por otra parte, mediante el desarrollo de habilidades a través de un enfoque centrado en el proveedor, un profesional

tenderá a ver soluciones a un problema que no puede ser el más conveniente o eficiente y va a terminar centrándose en una herramienta en lugar de centrarse y analizar el problema.

Uno de los principales marcos educativos utilizados es la Taxonomía de Bloom[111]. Esta es una taxonomía de aprendizaje bien establecida en los artefactos y objetos de aprendizaje. La Taxonomía de Bloom se compone de seis niveles de abstracción que se aplican a la categorización de las habilidades y el desarrollo de mecanismos de evaluación adecuados. Estos niveles son:

- Conocimiento
- Comprensión
- Aplicación
- Análisis
- Síntesis
- Evaluación

El concepto de esta taxonomía se ha ajustado para que coincida con los requisitos del análisis forense digital.

Hay dos principios generales para el marco:

- Que el marco debe ser independiente del proveedor y las habilidades deben centralizarse
- Que el marco debe emplear teorías educativas en el desarrollo del marco

Las teorías de aprendizaje educativas pueden ayudar en la estructuración de los objetivos de aprendizaje, los resultados y las herramientas para la construcción de una matriz de competencias que se ocupa de la competencia o del aprendizaje. La mayoría de las habilidades se aprenden a través del ejemplo, capacitación o educación; muy pocas son innatas o intrínsecas en un persona o de tabula rasa. Incluso la sencilla capacidad de esquivar un objeto volador como una pelota de béisbol en rápido movimiento es demasiado a menudo un comportamiento aprendido dolorosamente.

Hay seis niveles de experiencia para la calificación de habilidades (Niveles enumerados del 1 al 6). El uso de los niveles está destinado a demostrar una jerarquía progresiva en la habilidad o el logro de la capacidad en ejecución del proceso. Estos niveles se utilizan para generar actividades o criterios de rendimiento para obtener la certificación de una competencia básica en un nivel particular. El uso de los seis niveles inspira en gran medida a partir de la Taxonomía de Bloom de aprendizaje que describe una progresión de la adquisición de conocimientos y habilidades. Los seis niveles que se presentan en

[111] La Taxonomía de objetivos de la educación conocida también como taxonomía de Bloom, es una clasificación que incluye los diferentes objetivos y habilidades que los educadores pueden proponer a sus estudiantes.

este marco se construyen de manera que cada nivel proporciona los conocimientos necesarios para otros niveles. La progresión o la certificación a un nivel sólo se hacen como resultado de lograr el dominio de los niveles anteriores de especialización. Estos niveles están destinados a ser discretos y se espera que la gente incluso altamente capacitada y experimentada sólo pueda alcanzar el nivel 6 de competencias a través de algunas zonas de dominio dentro de la matriz. Los niveles de competencia son descritos como:

NIVEL 1 - DEFINIR: Este nivel indica el nivel más bajo de competencia. Una persona sería capaz de definir lo que es una actividad, proceso o concepto, por ejemplo:

- Definir una imagen forense
- Definir un hash criptográfico

NIVEL 2 - APLICAR: Este nivel indica la habilidad de aplicar una actividad, proceso o concepto. Por ejemplo:

- Aplicar un hash criptográfico
- Aplicar un procedimiento para lograr una adquisición de una imagen forense.

NIVEL 3 - EXPLICAR: Este nivel está indicado por la capacidad de aplicar una actividad, y explicar el proceso o concepto. Por ejemplo:

- Explique cómo se crea un hash criptográfico.
- Explique cómo se adquiere una imagen forense.

NIVEL 4 - EVALUAR: Este nivel está indicado por la capacidad de evaluar críticamente una actividad, proceso o concepto. Por ejemplo:

- Evaluar hashes criptográficos para la idoneidad de una tarea.
- Evaluar los distintos métodos de adquisición de imágenes forenses para una situación dada.

NIVEL 5 - CRÍTICA: Este nivel se indica por la capacidad de la crítica de una actividad, proceso o concepto utilizando un proceso científico. Por ejemplo:

- Analice el uso de hashes criptográficos por otro examinador, usando una variedad de métodos para llevar a cabo la evaluación.
- Analice el procedimiento de adquisición de otro examinador utilizando métodos adecuados.

NIVEL 6 - SÍNTESIS: Este nivel está indicado por la capacidad de sintetizar el material pertinente para producir un informe profesional o una solución validada para una actividad, proceso o concepto forense mediante un proceso científico sólido. Por ejemplo:

- Producir un informe pericial sobre el procedimiento de adquisición de un disco duro de otro examinador.
- Producir un informe pericial de la corte sobre la tema de controversia de un hash MD5.
- Resuelve un problema forense multipartito, como la adquisición y verificación de un sistema RAID en vivo.

A modo de ejemplo, se proporciona un desglose de un flujo del marco basado en la Adquisición de Evidencia como la competencia central. Los resultados son el objetivo final o la base de habilidades que un examinador forense digital debe aspirar a alcanzar para demostrar su competencia. Se espera que un examinador forense digital competente debería ser capaz de:

- Adquirir una copia exacta de los datos digitales de un dispositivo digital o aparato con la mínima perturbación de la evidencia original.
- Explicar los principios fundamentales de la informática y la ciencia forense que se aplican a la adquisición de la evidencia digital.
- Aplicar procesos y principios forenses válidos para adquirir la evidencia digital.
- Aplicar la tecnología apropiada para adquirir evidencia digital de una manera válida a efectos legales.
- Validar los procesos de adquisición forense y los resultados mediante métodos científicos sólidos.
- Validar la tecnología de adquisición forense utilizando métodos y principios científicos sólidos.
- De manera convincente comunicar verbalmente o por un informe escrito un proceso o técnica relacionada con la adquisición de la evidencia digital.

A partir de estos resultados, se generarán los niveles de habilidad o los objetivos de conductas que pueden ser generados. A modo de ejemplo, se detallan los resultados de la prueba de Adquisición de Evidencia en el **RESULTADO A-1** del Nivel de Competencias 1, 2 y 3. Una vez más, las listas de las competencias no están completas y están destinados sólo a modo de ejemplo.

RESULTADO A-1

Adquirir una copia exacta de los datos digitales de un dispositivo digital o aparato con la mínima perturbación de la evidencia original.

NIVEL 1: Este nivel demuestra cuando un candidato puede:

- Definir una imagen forense o una copia a nivel de bits.
- Definir un procedimiento simple para adquirir una imagen forense de una memoria USB o de un disco duro de ordenador utilizando el software de imágenes forenses adecuado.
- Definir un hash criptográfico.

NIVEL 2: Este nivel demuestra cuando un candidato puede:

- Aplicar un procedimiento simple para adquirir una imagen forense.
- Aplique un hash criptográfico para verificar un archivo, directorio o imagen.

NIVEL 3: Este nivel demuestra cuando un candidato puede:

- Explicar cómo se usa un hash criptográfico para verificar una copia forense.
- Explicar el procedimiento para adquirir una imagen forense de un dispositivo digital.
- Explicar el concepto de una partición y cómo se relaciona con una imagen de un disco.

EVALUACIÓN DE COMPETENCIAS

Uno de los elementos claves del marco es la estructuración de evaluación de las competencias en el marco de referencia.

Para demostrar competencias de **NIVEL 1** normalmente se requiere el aprendizaje memorístico de hechos básicos relativos a los resultados pertinentes. El dominio de este nivel se puede demostrar adecuadamente mediante el uso de un test de selección múltiple o respuestas cortas.

El **NIVEL 2** es la aplicación de conceptos y procesos aprendidos de la consecución del **NIVEL 1**. La demostración del dominio de este nivel elemental sería mejor evaluarlo por la aplicación práctica del concepto/proceso bajo las condiciones de una prueba.

Para poder realizar esta prueba y corroborar las habilidades, una persona podría ponerse a prueba de una manera práctica para mostrar su capacidad de aplicar un procedimiento dado la adquisición y verificación de una imagen forense. El procedimiento real puede ayudar a la selección del candidato, basarse en un proceso del departamento o a realizar una validación de un estándar utilizado por la organización. Es fundamental que la adquisición y la verificación de la imagen forense sean observadas de cerca y evaluada en el proceso de evaluación.

El **NIVEL 3** es un progreso de niveles anteriores y el examinador ahora debe combinar y utilizar su conocimiento del área mediante la demostración de la capacidad de explicar un concepto o proceso. Se considera que esta etapa representaría el nivel básico de competencia para un examinador forense

digital capaz de presentar el material a un órgano jurisdiccional. En el ejemplo anterior, se explicaba un procedimiento para adquirir una imagen forense de un dispositivo digital, lo que significaría que un examinador podría explicar el fundamento de conceptos, procesos y procedimientos necesarios para adquirir una imagen forense, ya sea por vía oral en un tribunal de justicia o en un informe escrito. La evaluación de esta habilidad se puede realizar por medio de una prueba de evaluación escrita o una presentación oral del tema en cuestión. La demostración práctica con el diálogo y la instrucción demuestran el dominio en este nivel.

Mediante el uso de un marco como el que se ha explicado, una organización de análisis forense digital puede programar de manera efectiva la adquisición y evaluación de habilidades.

PROTECCIÓN DE SU INVERSIÓN

Algunas empresas hacen grandes inversiones para mantener a su personal competente y calificado, particularmente en áreas donde es más fácil retener al personal, asegurándose la organización del apoyo del personal que se está capacitando. Este entorno crea una situación de oportunidad/costo transformándose en la obtención y el mantenimiento de las habilidades del empleado, que a la vez es un factor que considera en el momento de cambiar a un empleador con las mismas prestaciones. Otra forma es vincular contractualmente el personal de los gastos de formación mediante el uso de un contrato formal donde el personal reconoce que en caso de poner fin a su contrato será responsable del pago proporcional de la formación brindada por la empresa.

También se debe de analizar el riesgo cuando no se capacita a todo el personal, ya que todos deben de estar al mismo nivel de formación, esto es por la pérdida de personal. Se perdería tiempo y dinero en estar formando a un individuo por no haberlo capacitado en grupo. Este tipo de decisiones las tendrá que manejar el gerente del laboratorio. Se debe recordar que el mejor activo de una empresa es el capital humano.

RESUMEN

En este capítulo se ha examinado una serie de cuestiones que se relacionan con la selección del personal idóneo para el laboratorio. Se ha examinado la selección con una combinación adecuada de personal y las medidas que se pueden implementar para asegurar que tengan las habilidades, calificaciones y experiencia en el puesto. Se ha abordado algunas de las cuestiones relacionadas con el empleo de personal auxiliar, el contratado y sus accesos al laboratorio, así como el control cuando están dentro del laboratorio. El capítulo también examinó cuestiones relacionadas con la provisión de apoyo para el personal, incluyendo el acceso al asesoramiento y las evaluaciones psiquiátricas.

Además se ha examinado que debe considerarse en relación con la formación del personal, la educación y la retención del personal. Se ha examinado los problemas con respecto a la formación proporcionada por el proveedor, la educación académica, la validación y certificación de las competencias del personal. El capítulo también examinó el tema del desarrollo personal, la motivación, la retención y el desarrollo de habilidades especializadas para cumplir con el papel de la organización. El capítulo se ha puesto de relieve en una serie de consideraciones y decisiones que el gerente debe tomar para hacer el uso más eficaz de las finanzas y los recursos disponibles.

CAPÍTULO 7: ADMINISTRACIÓN DE LA COLECCIÓN DE LA EVIDENCIA

En este capítulo se abordarán los problemas en la gestión relacionada con la colección de la evidencia en la escena del crimen, un aspecto crucial en cualquier investigación. También se tratarán temas como la continuidad de la evidencia y la cadena de custodia.

El mantenimiento o la falta administración de la cadena de custodia es una de las mayores causas para la inadmisibilidad de la evidencia. La evidencia debe ser manejada de una manera que permita la completa auditoría, revisión de procesos, posesión y revisión de pruebas que se hayan realizado desde que fue protegida y extraída de la escena del crimen para su eventual presentación en una audiencia. La integridad del registro es primordial para asegurarse de que todo lo efectuado puede ser probado más allá de toda duda razonable.

Hay normas y manuales existentes, tales como el ASTM E 1492 - 05[112], AS/NZ HB 171[113] y IOEC 2002 que son relevantes para asuntos forenses digitales, los cuales sean utilizados como base de este capítulo.

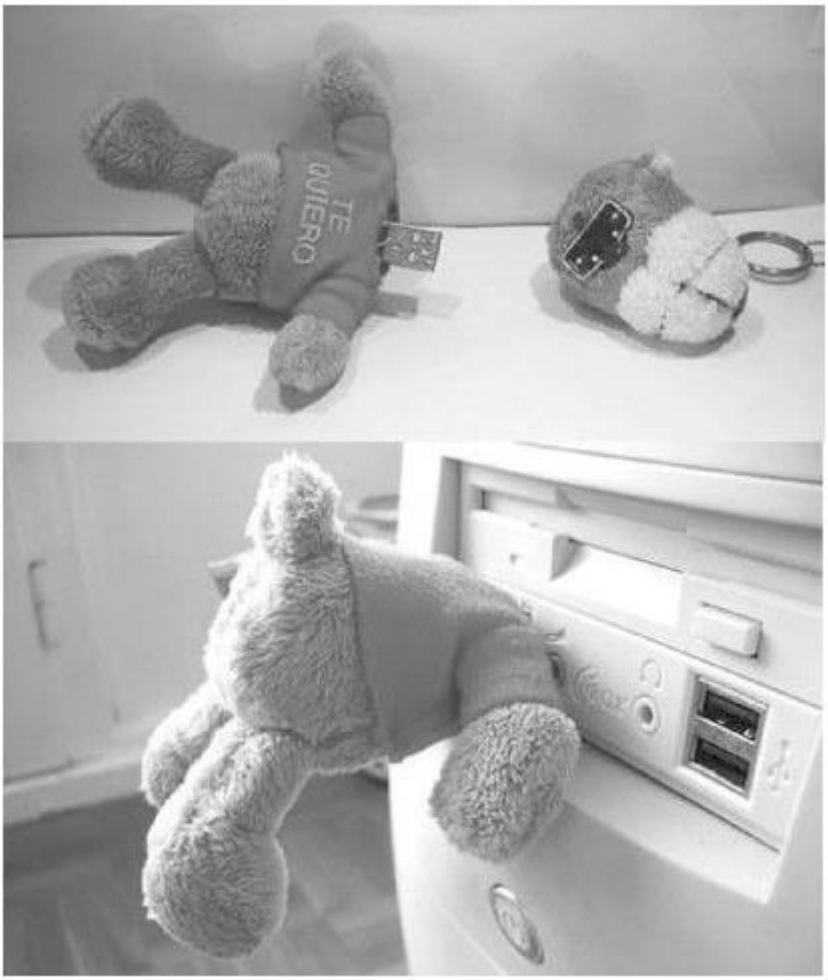
RECOLECCIÓN DE LA EVIDENCIA

La recolección de evidencia dentro del contexto forense digital es cada vez más difícil por la diversidad de dispositivos digitales que pueden contener posibles pruebas. Además, los datos que contienen los dispositivos digitales se están convirtiendo cada vez más volátiles.

En el sentido tradicional de la informática forense se relacionaba el análisis a un disco duro de un ordenador o portátil que normalmente se encontraba en el domicilio del sospechoso, lugar de trabajo, pero esta situación ya no es el caso, ya que los datos están alcanzando una variedad de formas de almacenamiento así como tipos de dispositivos digitales.

En el ejemplo de la figura se muestra una llave de almacenamiento USB en forma de oso de peluche, el cual podría contener su propio entorno de ejecución y varios gigabytes de datos destacados para la recolección de la evidencia.

[112] Practice for Receiving, Documenting, Storing, and Retrieving Evidence in a Forensic Science Laboratory
[113] Guidelines for the Management of IT Evidence



Fundamentalmente, todas las fuentes que puedan almacenar datos se traducirán en objeto de análisis por parte del examinador forense digital para su revisión e interpretación de los datos incautados.

DISEÑO DEL SISTEMA PARA LA RECOLECCIÓN DE EVIDENCIA

Cuando los elementos de interés son procesados y admitidos como evidencia de un incidente se deben llevar a cabo una serie de pasos para garantizar la continuidad de la evidencia y tener la capacidad de demostrar, verificar y mantener la singularidad del objeto o proceso que se investiga.

Diversas normas y manuales describen los requisitos para mantener la continuidad y el peso de la evidencia que se relacionan con la gestión de las pruebas. Estos requisitos se resumen en:

IDENTIFICACIÓN DE LA AUTORIDAD – Se determina quien ha tenido acceso a la evidencia, quien ha creado o cambiado algún registro.

AUTORIDAD DE VERIFICACIÓN Y VALIDACIÓN – Se determina verificar la autenticidad de los cambios, el acceso, los registros creados y que la grabación de los procesos es validada y confiable.

DISPONIBILIDAD Y REGISTRO – Se determina que los registros estén disponibles y que se almacenen en un formato que sea utilizable y accesible para ser revisado en cualquier momento.

IDENTIFICADORES

Uno de los primeros puntos cruciales en el diseño en la recolección de la evidencia es que cada elemento de prueba y sus posibles partes puedan identificarse para cada caso. Estas partes pueden adoptar muchas formas dentro de los elementos de la evidencia. Por ejemplo, en un sistema informático puede ser incautado una matriz RAID de ocho discos duros. El registro debe permitir que el RAID pueda ser registrado y examinado como partes físicas (discos duros), así como cualquier parte lógica (particiones, volúmenes) y por supuesto la controladora RAID en sí.

Esto impone la utilización de identificadores extensibles y únicos para la construcción de registros, la elección de los identificadores debe ser dentro del contexto dado. Por ejemplo, si una organización procesa más de mil casos por año, sería ingenuo seleccionar un número de caso de tres dígitos como el identificador de caso único. Asimismo, el uso de un número de caso de ocho dígitos sería excesivo.

Un formato de registro genérico con identificadores aceptables, podría ser:

NÚMERO DE CASO	NÚMERO DE ARTÍCULO	NÚMERO DE PIEZA	DESCRIPCIÓN	MARCA DE TIEMPO	CREADOR
0003	RC001	HD001	Reporte de análisis de disco	200803190944	Juan Pérez
0004	RC002	HD002	Inicio de hashes	200803121821	Pedro López

- **NÚMERO DE CASO**: digito entero incremental
- **NÚMERO DEL ARTÍCULO:** Las dos primeras letras identifican lo que genéricamente es; por ejemplo, un ordenador de escritorio: DT; un ordenador portátil: LT; un RAID: RC; un teléfono móvil: ML. Los tres últimos caracteres son dígitos entre 001- 999
- **NÚMERO DE PIEZA:** Las dos primeras letras identifican la parte genérica; por ejemplo, una unidad de disco duro: HD; una memory stick: MS; una tarjeta SD: SD; una memoria flash MF; un elemento desconocido: ED
- **DESCRIPCIÓN:** Una descripción evidente
- **MARCA DE TIEMPO**: En formato YYYYMMDDHHMM
- **CREADOR**: Las letras iniciales del nombre de la persona que crea el registro. Podría ser un número de servicio, insignia, login de red, o algún otro identificador único.

La nomenclatura para nombrar artículos o la identificación de ellos normalmente está ligada a la producción de los registros de la organización. La parte importante es que el esquema o nomenclatura este diseñado y declarado.

El tiempo y el estampado de la fecha es un tema crítico en la creación, recuperación y almacenamiento de evidencias, en particular en pruebas digitales y registros relacionados al caso. Las marcas de tiempo permiten la reconstrucción exacta de los acontecimientos que se han producido en un punto de interés o en algún registro sobre ellos. Todos los sistemas de computación dentro del laboratorio deben usar un servidor de hora centralizado para sincronizar la hora. El protocolo común para esto es NTP (Network Time Protocol), mediante el cual el servidor principal del laboratorio se mantiene en formato UTC (tiempo universal coordinado) o GMT (Greenwich Mean Time) a través de un reloj atómico. Todas estas interacciones en el servidor principal deben producir un cambio en el tiempo para poder ser registrado y asegurado el registro de información. Una forma de confirmar que el tiempo se sincroniza es asegurarse de que todos los dispositivos en el sistema consulten al servidor central. En el caso de las estaciones de trabajo que no estén conectadas al servidor se tendrá que hacer manualmente.

En el caso de verificar todos los puntos de interés de la evidencia digital, los algoritmos hash criptográficos son el método comúnmente utilizado para verificar e identificar la evidencia digital. El uso de una sola función de hash no es la mejor práctica, se deben usar dos algoritmos hash bastante fuertes como MD5 y SHA256. Este proceso es necesario para asegurar que los temas de interés se verifican y se identifican de forma única. Para elementos físicos se requiere que el almacenamiento dentro de un receptáculo sea apropiado y que pueda ser sellado, también se debe tener una hoja de registro o etiqueta física asociado con él. Adicionalmente en la actualidad se aplican algoritmos criptográficos como MD5 y SHA1.

En el proceso de la identificación y la autenticación de un usuario puede ser a través de una contraseña segura, un PIN (número de identificación personal), un identificador biométrico, una tarjeta inteligente, una firma digital, o la autenticación múltiple que es una combinación de dos o más técnicas para proporcionar acceso. La autenticación múltiple es la mejor práctica, y es fácil de lograr con los sistemas informáticos modernos. La clave es que la autenticación no se convierta tan engorrosa y que afecte la productividad de los procesos.

El sistema debe tener suficientes niveles de granularidad para registrar la causa de los cambios en el estado de un registro. Siempre que sea posible el uso de un sistema de autenticación debe ser corroborado, por ejemplo, con imágenes de vigilancia en el área de laboratorio. Por otra parte, el

sistema de archivos o el sistema en el que se almacenan las actas deberán ser capaces de identificar quien creó el archivo y también quien ha accedido al archivo. En la mayoría de los sistemas operativos para servidores de archivos, como Windows Server o Novell Server, la auditoria de archivos debe estar habilitada. La auditoría de archivos dentro de estos sistemas de seguimiento manejan todas las interacciones con los archivos. Del mismo modo, si se lleva a cabo el registro basado en una estructura de base de datos, por ejemplo, en un servidor de base de datos (SQL), la auditoría igualmente debe estar habilitado con la aplicación. Uno de los problemas principales en el uso de estas herramientas son los privilegios de acceso.

AUTORIDAD, VERIFICACIÓN Y VALIDACIÓN

Uno de los conceptos más importantes es la verificación de la autoridad dentro de la cadena de custodia y la continuidad de la evidencia. En un proceso o registro se debe de demostrar quien creó el registro inicial, así como que personas han accedido o modificado los registros iniciales. Por otra parte, los procesos que hacen esto deben ser validados y probados para asegurar la integridad del proceso y del registro.

El registro debe ser almacenado en un sistema que sea difícil de modificar, cambiar, borrar y ver un registro sin causar un registro o grabación de esta actividad. Esto se puede lograr por el bloqueo de archivos rigurosos; es decir, cuando un archivo se reescribe en el disco un registro se produce que almacena el nuevo nombre del archivo. Como se mencionó antes, los sistemas operativos modernos tienen la capacidad de documentar el seguimiento y los cambios. Es obligatorio que los sistemas que crean, almacenan y mantienen los registros no sean capaces de cambiar o modificar los registros de auditoría; estos deben ser almacenados de forma segura en el dispositivo de origen y también en un sistema de registro o dispositivo independiente. Estos métodos de sellado de tiempo, auditoría y control deben estar establecidos en los sistemas que están conectados a la red. Sin embargo, gran parte de la adquisición inicial de las posibles evidencias se emprenden fuera del sitio.

ARCHIVING DE DATOS Y DISPONIBILIDAD

Este es un proceso cada vez más complejo y difícil en el dominio de TI. No sólo es el volumen de información, sino también el aumento de la multitud de dispositivos y formatos en los que se almacena. La evidencia en algunas jurisdicciones tiene que ser preservado por un período de hasta 75 años. No obstante todo dependerá de la naturaleza de la investigación que se esté realizando, se debe definir el periodo de retención y establecer procedimientos de devolución como por ejemplo wiping (técnica de borrado seguro) o relocalización de la evidencia.

RECOLECCIÓN DE LA EVIDENCIA

En las secciones anteriores se trataron los sistemas necesarios y sistemas de requisitos de diseño para la obtención de evidencia. Esta sección tratará sobre la colección física de los elementos de interés que se espera que se conviertan en pruebas. El proceso de recolección se lleva a cabo en varias etapas, estas son conocidos como:

- Lugar de priorización
- La evidencia en tránsito
- Recepción de la evidencia
- Artículos de reconciliación

LUGAR DE PRIORIZACIÓN

En el lugar de priorización se involucra directamente con la obtención de pruebas en la escena del crimen o incidente. Uno de los principales métodos para documentar las acciones tomadas es conocido formalmente como notas contemporáneas. Las notas contemporáneas es la grabación completa, sistemática y cronológica de todas las acciones en los registros electrónicos originales o en las copias. Las personas deben tomar notas contemporáneas de cualquier proceso, como toma de decisiones, información disponible, personas consultadas, las autoridades inmersas en el caso y las razones de las decisiones tomadas. Estas notas deben registrar sólo los hechos y no opiniones o conjeturas; que debe ser un registro verdadero y exacto de lo que ha ocurrido. Estas notas pueden estar en forma de papel o en formato electrónico. El hecho importante es que la autenticidad y la autoridad del registro puedan ser probadas. En el lugar de priorización, el papel y la fotografía sigue siendo una forma efectiva de grabación de evidencia de una forma rápida y eficiente. Los documentos en papel y fotografías resultantes de la escena luego pueden ser utilizados como datos de pruebas.

La recolección del material debe hacerse en formularios de papel consistentes con el registro electrónico de lo que se va a introducir. Por ejemplo, sería poco aconsejable omitir elementos críticos que identifican de forma única la evidencia recogida. Del mismo modo también se requiere el uso correcto de la fotografía, debe incluir los números que identifican cada elemento de interés. Las fotografías tomadas también deben estar vinculadas al tema de interés en el formulario.

Todos los elementos de interés se deben almacenar en un recipiente o medios de transporte adecuadamente etiquetado o identificado que clasifique el elemento de interés claramente, la persona que crea el registro debe colocar un sello de unión que protege el elemento de interés. El propósito es asegurar y demostrar que el elemento de interés no ha sido contaminado o dañado

durante el transporte o el almacenamiento, y de esta manera se cumple con el mantenimiento de la continuidad o cadena de custodia.

El recipiente o medio de transporte debe ser lo suficientemente robusto como para proteger el elemento de extremos ambientales, daños físicos o cualquier otro problema en tránsito. Además se debe almacenar lejos de fuertes corrientes eléctricas, emanaciones de radio frecuencia o fuentes de magnetismo.

El daño físico es un tema que debe ser mitigado. Los discos duros y muchos otros componentes digitales son susceptibles al daño por golpes. Siempre que sea posible cualquier unidad o dispositivo que está siendo administrado por un investigador debe garantizar en todo momento la colocación y la fijación a una superficie estable.

LA EVIDENCIA EN TRÁNSITO

Este es un proceso importante, el estado de cualquier artículo de interés es uno de los casos comunes donde la continuidad de la evidencia es fácil de incumplir. Es importante que en ningún momento durante el tránsito la intercesión de un tercero sea posible. En todo momento los artículos de interés deben estar suficientemente supervisados. Como se mencionó anteriormente los artículos de interés deben ser asegurados para no permitir colisiones o movimiento bruscos que puedan afectar la evidencia incautada, se debe garantizar que estén protegidos de las corrientes de alta energía eléctrica, los campos de radiofrecuencia, campos magnéticos y sobre todo contar con controles ambientales apropiados para regular la temperatura.

En algunos casos, puede ser necesario que el dispositivo esté conectado a una fuente externa de energía (por ejemplo, un teléfono móvil, PDA o un dispositivo móvil que requiera carga). En este tipo de casos, esto puede significar que el vehículo de transporte debe estar preparado para tratar este tipo de casos. La alimentación del dispositivo debe hacerse debidamente y no interferir con los elementos de interés, se debe evitar la emanación eléctrica o magnética, y se debe tener cuidado de que cualquier dispositivo móvil que se active no puede recibir una frecuencia de radio señal.

RECEPCIÓN DE LA EVIDENCIA

La recepción de los artículos de interés es una de las actividades más importantes que se llevan a cabo. La recepción incorrecta o imprecisa de artículos de interés en esta etapa puede invalidar la presentación de la evidencia.

Se supone que el edificio cuenta con un área de recepción de evidencia por separado. La zona de recepción se describe mejor como el DMZ de la organización (zona desmilitarizada) en el cual se recibe la evidencia original de entrada. Es importante que esta frontera organizacional está estrictamente

protegido y separado en el sentido físico y lógico. Esta separación forzada permite un mayor control de la continuidad de la evidencia y reduce el margen de error. Si las circunstancias o eventos se convierten en temas de conflicto, la auditoría y la resolución de problemas de continuidad la evidencia deben de superar este tipo de impases.

Todos los artículos de interés deben ser registrados y recibidos en esta frontera lógica y física. Los artículos incautados no deben moverse a través de cualquier otra parte del proceso del negocio hasta que se produzca la correcta recepción de los artículos. Para una buena gestión de la recolección de evidencias se debe incluir la tramitación de un expediente o un elemento para producir una copia de la evidencia. La recepción se completa cuando hay una copia forense de trabajo viable de un elemento para su uso en el laboratorio que cuente con una pista de auditoría completa y con una cadena de custodia con autoridad.

En algún momento se deben comprobar los valores hash y aplicar los procesos forenses para verificar la integridad de los elementos antes de aceptar los artículos de interés; sin embargo, esto no es simplemente práctico o conveniente en la realidad. Sin embargo, se puede controlar el proceso por el cual la evidencia cruza la "frontera" de una entidad a otra. El siguiente es un resumen de los procesos que deben ocurrir para garantizar la continuidad de la evidencia y la ordenada recolección de artículos de interés. En este punto se asume que los artículos de interés han cruzado el umbral físico de la organización y se encuentran en el edificio en la zona de recepción física.

VERIFICACIÓN DE LA PROPIEDAD

Este proceso se refiere a la verificación y validación de la identidad de la persona. Este proceso debería, como mínimo, utilizar una forma de identidad con fotográfica y la firma del presente. Si los artículos están siendo enviados por correo, se debe asegurar de que se identifique al mensajero por el nombre completo y la empresa de mensajería. Los artículos deben tener un número de seguimiento para su registro. El proceso debe garantizar la correcta identificación y verificación cada vez que se recibe un artículo de interés.

VERIFICACIÓN DE ARTÍCULOS

La justificación y la comprobación de los elementos presentados es de vital importancia para asegurar de que se está tomando la recepción del número correcto de artículos y que se identifican individualmente y de manera apropiada. El aseguramiento debe llevarse a cabo para verificar que las descripciones proporcionadas son un registro fiel y exacto de los elementos presentados. Esto debe estar contenido en la documentación sobre los artículos en cuestión. Los sellos de la continuidad de la evidencia deben ser revisados para la integridad; cualquier rotura o anomalía deben registrarse y

documentarse a través de fotografías y notas contemporáneas. En caso de una rotura en un sello o cualquier otra anomalía, el asunto debe ser escalado con carácter de urgencia al gerente del laboratorio o el administrador de casos relevantes.

ARTÍCULOS DE RECONCILIACIÓN

Este es el proceso de introducción de los elementos en el sistema interno, donde se registran los detalles de los elementos en el sistema para su uso por la organización receptora. Si los artículos son de la propia organización, un simple proceso de verificación debe llevarse a cabo para asegurar que se registran todos los detalles necesarios. En el caso de los formularios de registro deben ser utilizados como punto de referencia para todos los registros. Si los artículos son de una organización externa, tiene que haber una reconciliación del registro externo con los detalles de los registros internos y sus requisitos. Las organizaciones que intercambian este tipo de información a menudo se basan en un formato estándar. Por tanto, es una buena idea desarrollar un proceso estándar y hojas de procedimiento a fin de que este proceso de reconciliación se produzca de una manera coherente y ordenada.

PROCESAMIENTO DE ARTÍCULOS

Esto requiere que los artículos de interés deben ser procesados inicialmente donde se crean y se verifican a través de las prácticas forenses estándar, tales como las imágenes de disco, copias de archivos, reproducción fotográfica, copias forenses de los elementos originales, entre otros. Tras la verificación y registro de una copia forense, el elemento original se registra, vuelve al depósito de empaque, y se fija en el área de almacenamiento de evidencias. Las copias forenses se pueden introducir en los procesos de investigación normales del laboratorio.

DOCUMENTACIÓN DE PROCEDIMIENTO

Por último, el procedimiento juega un papel importante en asegurar que no se realice ningún error u omisión. Los procedimientos operativos estandarizados deben ser desarrollados para cada instancia en la recolección de la evidencia. El uso de procedimientos estandarizados reduce la posibilidad de que ocurra un error a través del refuerzo y la repetición del proceso constante; es decir, que es menos propenso olvidar u omitir pasos en el proceso. Los siguientes son los procedimientos o formularios necesarios para la recolección ordenada y adecuada de las pruebas básicas.

1. **LUGAR DE PRIORIZACIÓN/ESCENA DEL CRIMEN**

- **DOCUMENTACION INICIAL EN LA ESCENA:** El procedimiento que se debe iniciar en el lugar de la escena es la documentación, esto implica el uso de notas contemporáneas, vídeos y fotografías para documentar la escena.

- **ETIQUETADO DE ARTÍCULOS**: Es el procedimiento para etiquetar e identificar los artículos del interés. Esto implica la producción de un procedimiento que identifique los elementos para ser etiquetados de una manera que sea consistente y se relacione directamente con los sistemas en uso en el laboratorio.
- **PROCESAMIENTO INICIAL:** Son los procedimientos para permitir la retirada ordenada de los elementos de la escena. Estos serán diferentes para cada dispositivo genérico encontrado, como por ejemplo:
    - Computadora de escritorio
    - Ordenador portátil
    - Teléfono móvil
    - PDA
    - Dispositivos de memoria USB
    - Dispositivos incorporados (iPod, reproductores MP3, routers)

      Esto debe incluir el procedimiento para empaquetar de forma segura cada uno de los dispositivos para el transporte.
- **PROTOCOLOS DE TRANSPORTE**: Son los procedimientos para el transporte de los artículos de la escena del crimen a las instalaciones del laboratorio. Esto debe cubrir los requisitos mínimos obligatorios para el transporte seguro de regreso al laboratorio para mantener la continuidad de la evidencia.

2. **PROCEDIMIENTOS DEL LABORATORIO**

- **RECEPCIÓN Y RECIBO**: Procedimientos para garantizar la recepción correcta de los elementos del sitio o partes externas.
- **RECONCILIACIÓN**: Esto debe hacerse como un proceso independiente de conciliar los elementos en el sistema interno.
- **CREACIÓN DE COPIAS Y EL ALMACENAMIENTO DE ELEMENTOS ORIGINALES FORENSES**: Estos procedimientos es de cómo tratar a cada elemento para crear una copia forense y que sea utilizada en laboratorio. Una vez más, como mínimo, lo siguiente debe ser cubierto, como por ejemplo:
    - Computadora de escritorio
    - Ordenador portátil
    - Teléfono móvil
    - PDA
    - Dispositivos de memoria USB
    - Dispositivos incorporados (iPod, reproductores MP3, routers)

Esto debe incluir el procedimiento para empaquetar de forma segura cada uno de los dispositivos para el transporte.

La fase final es el almacenamiento seguro del elemento original en una sala de evidencia segura.

RESUMEN

La recolección y gestión de los elementos que eventualmente se convierten en pruebas es una tarea compleja y exigente. El principio básico de la ciencia forense es la preservación de la evidencia original con un cambio mínimo o nulo a su estado. Es obligatorio que todos los procedimientos o procesos desarrollados para manejar las posibles pruebas deben asegurarse de que cada evento, proceso o cambio que se haya producido para poder ser auditado, autenticado y establecido. Estos procesos y procedimientos también deben ser capaces de ser contabilizados dentro de una cronología exacta de los acontecimientos en el contexto del caso y más allá de toda duda razonable. El incumplimiento de lo antes mencionado puede que la evidencia sea desechada en una corte.

Aunque el personal dentro del laboratorio debe estar involucrado en la producción de las políticas y los procedimientos apropiados, el director del laboratorio debe promoverlas. El gerente debe decidir cuáles de las opciones (y habrá normalmente varias) es la mejor para que todo el personal siga la políticas y los procedimientos establecidos. Si no se tiene una política o procedimientos establecidos el laboratorio no mantendrá la credibilidad por mucho tiempo.

BIBLIOGRAFÍA

27001:2005, ISO/IEC. (2005). *Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos.*

27037, ISO/IEC. (2012). *Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence.*

Andy Jones & Craig Valli. (2009). *Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility.* USA: Elsevier.

Association of Chief Police Officers (ACPO). (n.d.). *http://www.acpo.police.uk*. Retrieved 10 24, 2014, from http://www.acpo.police.uk

Brian Deering. (n.d.). *http://www.forensics-intl.com/*. Retrieved 10 28, 2014, from http://www.forensics-intl.com/art12.html

Cano, Jeimy J. (2011). *Computación Forense. Descubriendo los Rastros Informáticos.* Alfaomega grupo Editor, S.A. de C.V., México.

Cano, Jeimy J. (n.d.). *Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis.*

Cano, Jeimy J. (n.d.). *http://www.acis.org.co/*. Retrieved 10 22, 2014, from http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

Casey Eoghan. (n.d.). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. In C. Eoghan.

Checkpoint. (n.d.). *http://www.checkpoint.com/*. Retrieved 10 23, 2014, from http://www.checkpoint.com/campaigns/2014-security-report/#

Corporation, RAND. (n.d.). *http://www.rand.org/*. Retrieved 10 23, 2014, from http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Infosec Institute. (n.d.). *http://www.infosecinstitute.com*. Retrieved 10 24, 2014, from http://www.infosecinstitute.com/jobs/computer-crime-investigator.html

International Organization on Computer Evidence (IOCE). (n.d.). *http://www.ioce.org*. Retrieved 10 23, 2014, from http://www.ioce.org

ISO/IEC27037. (2012). *ISO/IEC 27037:2012.*

Jeimy J. Cano. (n.d.). *Evidencia Digital: Contexto, situación e implicaciones nacionales.*

Juan David Gutiérrez Giovanni Zuccardi. (n.d.). *http://pegasus.javeriana.edu.co/*. Retrieved 10 23, 2014, from http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Listado de Herramientas Forenses. (n.d.). *http://conexioninversa.blogspot.com/*. Retrieved 10 27, 2014, from http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html

López, Javier Pagés. (n.d.). *http://www.criptored.upm.es/*. Retrieved 10 28, 2014, from http://www.criptored.upm.es/descarga/ConferenciaJavierPagesTASSI2013.pdf

Manuel Castells. (n.d.). *http://www.uoc.edu/portal/ca/index.html*. Retrieved 10 24, 2014, from http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html

Marcella, A. J., Greenfield, R. S., Abraham, A., Brent, D., Rado, J. W., Sampias, W. J., et al. (2002). *"Cyber Forensics—A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes.* Estados Unidos: Auerbach Publications (CRC Press). 2002. ISBN 0−8493−0955−7.

Marcelo Alfredo Riquert. (n.d.). *http://www.pensamientopenal.com.ar/*. Retrieved 10 24, 2014, from http://www.pensamientopenal.com.ar/node/27142

Movimiento Medio Lleno. (n.d.). *http://www.mediolleno.com.sv/*. Retrieved 10 27, 2014, from http://mediolleno.com.sv/editorial/el-salvador-necesita-que-se-aprueben-leyes-eficientes

National Institute of Justice. (n.d.). *http://www.nij.gov*. Retrieved 10 23, 2014, from http://www.nij.gov

Óscar López, Haver Amaya, Ricardo León. (n.d.). *http://www.aic.gob.au/*. Retrieved 10 23, 2014, from http://www.aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf

Periódico La Página. (n.d.). *http://lapagina.com.sv/*. Retrieved 10 27, 2014, from http://www.lapagina.com.sv/ampliar.php?id=58659

Phil Williams, Electronic Journal of the U.S. Department of State. (n.d.). *https://www.ncjrs.gov/*. Retrieved 10 24, 2014, from https://www.ncjrs.gov/App/abstractdb/AbstractDBDetails.aspx?id=191389

RFC 3227. (n.d.). *http://www.rfc-editor.org/*. Retrieved 10 24, 2014, from http://www.faqs.org/rfcs/rfc3227.html

Rodney McKemmish. (n.d.). *http://www.aic.gob.au/*. Retrieved 10 23, 2014, from http://www.aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf

SARZANA, C. e. (2000). Delitos Informáticos AD-HOC. Buenos Aires.

Stephenson, D. P. (2014). *Certified Cyber Forensics Professional.* CRC Press.

Symantec. (n.d.). *http://www.symantec.com*. Retrieved 10 24, 2014, from Tendencias de Seguridad Cibernética en América Latina y El Caribe. Publicado por La Organización de Estados Americanos OEA en colaboración de Symantec:

http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Symantec. (n.d.). *http://www.symantec.com/*. Retrieved 10 23, 2014, from http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Transparencia Activa. (n.d.). *http://www.transparenciaactiva.gob.sv*. Retrieved 10 27, 2014, from http://www.transparenciaactiva.gob.sv/analizan-propuesta-de-ley-contra-delitos-ciberneticos/