Preguntas y Respuestas

Como se realiza el analisis forense en un caso de publicacion de contenidos no consentidos? por ejemplo videos privados de contenido explicito publicados en internet

Se debe obtener directamente del proveedor el archivo de video, o de ser así tipo nacional, solicitarlo a la Autoridad de Servicios Públicos para que se lo proporcionen, todo esto con su respectiva solicitud oficiosa por parte de la entidad investigadora, o con solicitud judicial a la empresa administradora del sitio web que contiene la ifnromación

Cual es la regulacion cuando los servidores o bases de datos estan fuera del pais?

Solicitar la información mediante asistencia judicial con cancillería adjuntando las resoluciones que motivan la solicutd y copia de la autorización de un juez a la entidad administradora de la información.

Las autoridades pueden irrumpir en un datacenter en donde estén la data o servidores de diferentes entesempresas o bancos sin previo aviso a las demás empresas?

Toda diligencia de allanamiento en este sistema penal debe ser autorizado y en el lugar hacer de conocimiento a las partes de lo que se va a realizar, nunca antes se avisa esto hasta tanto no se ecuentren en el punto de la diligencia que es donde se informa de lo que se tiene a bien realizar.

Que requisitos son los necesarios para ser Perito Forense Informático y quien regula esta profesión?

Para ser perito infomático más que un título universitario se debe tener la experiencia en materia de cibercrimen, aunado esto haber ejercido la especialidad por más de dos años en la sección y luego realizar los exámenes de acreditación y legales para que la institución te reconozca como perito forense informático y para el estado seas reconocido.

Como la autoridad competente resguarda toda la información proporcionada como pruebas en un casa de denuncia penal por un Banco (vulnerabilidades, informacion de sistemas, entre otros), para sentir seguridad en denunciar...

Se almacenan en medios digitales que luego son asegurados en embalajes denomindaos cadenade custodia que solo son accesados frente a las partes y mediante una diligencia judicial autorizada, seguridad de denunciar claro que hay solo falta la voluntad de hacerlo y es loque no tienen muchos bancos pr razones de imagen y no les interesa verdaderamente el cliente.

Existe una regulacion bancaria para el analisis continuo de su seguridad?
Nosotros nos basamos en lo que se nos permite realizar contenido en el MANUAL DE SERVICIOS PERICIALES, investigamos casos a solicitud de las partes y no en calidad de titular de la investigación.

Que recomendaciones puede dar como accion adecuadas para la recoleccion de evidencias de forma adecuada?

Primero que nada solo se debe contener la información sin manupulaciones, ni copias ni chekeos, lo apagado queda apagado y lo encendido desconectado de conexiones externas, asegurado hasta tanto no se entregue a las autoirdades, nada de reproducciones arbitrarias porque se violan derechos de los posibles indiciados.

En que punto de la investigacion se rompe la cadena de custodia?

Al momento de realizar cualquier acción sobre el indicios qu eno haya sido autorizada ni reconcida por alguna de las pertes, todos tienen que tener pleno conocimiento de la información y las actividades a realizar, igualmente contener registros de accesos arbitrarios o elementos que puedan poner en tela de duda la calidad del mismo y el principio de mismicidad.

Preguntas y Respuestas

Los oficiales de seguridad informática y administradores de aplicaciones o métodos de pagos como SWIFT y bloomberg deben estar armados para protección de su integridad física?

Este tema en lo personal escapa de mi responsabilidad en materia de informática forense, pero algo si es cierto, mientras estas mirando un sistema de esta clase no creo que tengas la oportunidad de cuidar tu espalda, otro lo puede hacer por ti, así que tanto como que tu tengas que tener un arma encima no te garantiza que te den chance de usarla en una situación confusa.

Haz manejado casos de vulnerabilidades en las IOT (internet de las cosas), de ser asi, como se realiza el analisis forense?

El analisis forense solo es llevado a reconocer la existencia del daño material, a donde recurrir por más detalles e identificar proveedores que puedan obtener más datos del emisor de daño o del cliente afectado, es decir, medir el daño, es la entidad financiera la responsable de subsanar la lesión y evitar que sus clientes estén expuestos.

Como la autoridad resguarda toda la información que es proporcionada (pruebas, información de vulnerabilidad, entre otros) que proporcionan los bancos en una denuncia?

Se almacenan en medios digitales que luego son asegurados en embalajes denomindaos cadenade custodia que solo son accesados frente a las partes y mediante una diligencia judicial autorizada, seguridad de denunciar claro que hay solo falta la voluntad de hacerlo y es loque no tienen muchos bancos pr razones de imagen y no les interesa verdaderamente el cliente.

Como se maneja la intercepcion de correos atravez de la tecnologia DLP internamente en la organizacion la ley permite esta practica o puede ser una especie de pinchazo?

No es pinchazo comenzando, ni es en tiempo real, la entidad administradora proporciona la información y el volcado de los datos por siolicutd de los investigadores, previa autorización legal.

Existen guías/manuales y recomendaciones de recolección de evidencia y análisis forense que puede el Ministerio Público suministrar a los bancos?

El intituto de Medicina Legal y Ciencias Forenses es brazo auxiliar dal Ministerio Público, somos una institución aparte con nuestro propio presupuesto, director y administración, el ministerio público no posee esta información, y si es cierto, este docuemtno existe y es de uso común para todo aquel que quiera conocer como realizar estas précticas.

Porqué es posible la incautación de datos, específicamente chats de WhatsApp, sí según WhatsApp los mensajes son "cifrados de usuario a usuario"?

Si se extraen con herramientas forenses especializadas de alto nivel, CELLEBRITE es la marca, lo exorto a que conozca que en materia pericial forense en ifnromática nada está oculto, las empresas de estos servicios incluso cooperan con los scripts para decifrar la informacion que corre en sus plataformas, de esta forma contribuyen a que no utilicen sus sitemas para crimenen o terroristmo.

Para tener conocimientos en Informática Forense que tanto debemos saber de leyes?

Lo necesario como saber que es delito analizar la mensajería personal, que es delito realizar analisis sin orden de un juez, que es delito eliminar datos y que es delito no ser objetivo.

La información en cualquier dispositivo que le proporcione el banco al colaborador es privada del colablrador. ¿esto aplica para laptops, desktops, movil, usb, etc? Y ¿es esto independiente de las normas internas del banco?

Ninguna norma está por encima de la Constitución, si se requiere investigar las normas bancarias quedan a un lado y la justicia impera para sancionar a los que cometen crimenes, les aconsejo que no se opongan a esto porque estarían obstruyendo la ley.

Preguntas y Respuestas

Los bancos aportan las pruebas, ustedes investigan y el sistema penal libera al delincuente. Como se puede hacer con esté problema ? Al dia siguiente están en otro banco haciendo fraude..

Nosotros no investigamos, investiga el Ministerio Público, nosotros aportamos las pruebas a favor o en contra de cualquiera de las partes, no somos responsables de la detención o no, solo de realizar la práctica de pruebas en busca de la verdad y no favorecemos a nadie.

¿Cuáles son los cursos o temas que se deben incluir en un taller de Informática Forense?

Manejo de la evidencia digital, delitos inforáticos, servicios periciales informáticos.

Se ha visto mucha investigacion de telefono android, que pasa con apple?

Apple está incluido, se omitió mencionarlo pero en general y como tal es teléfono.

Debido a las demoras en los diferentes casos o denuncias presentadas, la institución está capacitando a nuevos investigadores y actualizando a los existentes?

En todo momento, esa línea de capacitación es constante.

Más que una pregunta tengo una recomendación: por favor, mejoren los centros de recepción de denuncias, sobre todo los medio día u hora de almuerzo.

Disculpas, pero nosotros no recibimos denuncias, es un tema con la procuradora, nosotros somos laboratorios forenses y no tenemos nada que ver con denuncias ni recepción, ni medio días ni noches, realizamos PERITAJES y no cerramos medio día la parte operativa, la administrativa solo es administrativa, pero denuncias no recibimos, es una consulta que debe hacerle directamente a la procuradora en el Ministerio público.