HISTORIAS DE UN PERITO INFORMÁTICO FORENSE

Fernando Mairata de Anduiza

Perito Informático Forense

HISTORIAS DE UN PERITO INFORMÁTICO FORENSE

Autor:

Fernando Mairata de Anduiza

Perito Informático Forense

Portada:

Íñigo Mairata Iturmendi

Todo lo que se cuenta en este libro está basado en hechos reales, vividos como Perito Informático Forense. Se han alterado algunos datos para salvaguardar las identidades de las personas y empresas involucradas.

Esta obra está dedicada a mi familia por su apoyo y por todo el tiempo que les robo para dedicarme al apasionante mundo de la Informatica Forense.

Especialmente dedicada a todos los peritos y abogados tecnológicos que viven cada día estas historias y que son un apoyo vital en mi trabajo diario con su ayuda y su aporte de conocimientos.

Mención especial para D. Raúl Elola y D. Ignacio Carrasco compañeros de batallas, y Dª Laura Melgar Martínez por su ayuda en el desarrollo de estas páginas.

ÍNDICE

PRÓLOGO.

Desde hace ya algunos años, la electrónica, la informática y las nuevas tecnologías de la información y la comunicación forman parte de nuestras vidas. Es un camino sin retorno que, sin lugar a dudas, tiene una tendencia creciente. ¿Quién, a día de hoy, no utiliza el correo electrónico, algún sistema de mensajería instantánea, alguna que otra red social, la banca online…?. Las tecnologías de la información y la comunicación han llegado a nuestras vidas para quedarse, y no descubro nada nuevo si digo que no únicamente se han hecho un hueco importante en el ámbito personal o particular, sino también en el ámbito profesional y empresarial, donde, además, si te quedas fuera, estás casi abocado "al fracaso".

Todo esto tiene sus beneficios, no cabe duda, pero también tiene sus riesgos. Cada vez nos encontramos con más supuestos de ciberacoso, de fuga de información, de espionaje, de "robo" de identidad, de ataques a sistemas informáticos…

Para poder denunciar estas situaciones, se hace necesario poderlas demostrar y, para ello, la prueba estrella es la prueba pericial informática o tecnológica. La realización de un informe pericial informático, que sirva de prueba en un

juicio, requiere de profesionales cualificados y específicamente formados en informática forense, ya que, por un lado, existen evidencias digitales que son volátiles, lo que significa que un manejo incorrecto de las mismas las podría hacer desaparecer y, por otro lado, una mala praxis en el procedimiento de recolección y análisis de la evidencia podría dar lugar a una invalidación de la prueba.

No todos los casos llegan a juicio. A veces, los informes periciales son tan concluyentes que la parte contraria acepta anticipadamente "su derrota" y se llega a un acuerdo; otras veces, el cliente solicita el informe pericial no para denunciar, sino para asegurarse de que su dispositivo no está comprometido... En cualquier caso, y por los motivos anteriormente comentados, es necesario que el perito informático forense siga de forma escrupulosa un protocolo de actuación, tanto en el proceso de recolección y análisis de las evidencias digitales, como en la elaboración del informe pericial y, en su caso, en su ratificación ante la autoridad judicial. Por otro lado, y dado el vertiginoso avance de la tecnología, es requisito imprescindible que el profesional no se quede atrás y mantenga una formación continua.

En la obra que el lector tiene entre sus manos se realiza un estudio pormenorizado de la prueba pericial informática, desde un punto de vista eminentemente práctico, y ello, con un lenguaje cercano y fresco que invita a la lectura.

Su autor, Fernando Mairata de Anduiza, tiene una acreditada formación en el ámbito de las redes, la administración de sistemas, la seguridad de la información y de la informática forense.

Además, lleva a sus espaldas una intensa trayectoria como perito judicial informático forense, ha sido profesor del curso "Experto en Ciberseguridad y Peritaje Informático Judicial", ofertado por la Universidad a Distancia de Madrid (UDIMA) y, desde hace más de cinco años, es formador y participa de forma activa en jornadas y ponencias relacionadas con la seguridad de la información y la pericia informática.

A lo anterior se añade su humildad y altruismo, ya que colabora, como cibercooperante, en la divulgación de un uso seguro y responsable de Internet, de los riesgos que las nuevas tecnologías traen consigo y de los mecanismos de ayuda a los que poder recurrir en caso de ser víctima de un ciberacoso o un ciberataque.

En el presente libro podemos distinguir dos partes, ya que el autor comienza haciendo una clara descripción de la figura del perito informático forense para, a continuación, abordar la pericia con un enfoque práctico, explicando, a través de casos reales, el modus operandi de un perito informático forense.

No se limita el autor a hacer una relación de hechos superficial, sino que, de forma hábil, nos adentra en cada historia, convirtiéndonos en observadores privilegiados de diferentes escenarios, vivencias y experiencias, abordando la historia en su completud, desde el momento previo en que el cliente solicita el servicio, pasando por la extracción de las evidencias digitales y su estudio y concluyendo, según los casos, con la ratificación del informe pericial en el juzgado.

Esto da la obra una indiscutible originalidad que permitiría titularla como estudio práctico de la pericia informática a través del análisis de casos.

Por todo ello, el libro que ahora mismo tiene entre sus manos constituye una valiosa guía práctica para adentrarse en el cada vez más recurrido campo de la prueba pericial informática, siendo un instrumento muy útil para todo tipo de público que quiera saber qué es y qué hace un perito informático forense, así como

una herramienta de trabajo de excepcional valor para los peritos informáticos, especialmente para aquellos que se inician en la profesión.

Laura Melgar Martínez

Abogada y fundadora de Digital Crime Abogados

INTRODUCCIÓN.

Cuando empecé hace años en el mundo de la informática Forense no tenía claro donde me estaba metiendo. La gente me plantea problemas de lo más diverso que a menudo acaban en los Tribunales. Firmo informes que pueden cambiar la vida de la gente por ganar o perder un juicio. Muchas veces dependiendo de tu buen trabajo las pruebas sirven o no, y por supuesto como nuestro trabajo es el de analizar las evidencias: las pruebas no siempre dicen lo que quiere nuestro cliente, pero tenemos un compromiso con la justicia. La Ley y nuestro Código Deontológico nos prohíbe manipular las pruebas a favor del que nos paga, las pruebas son como son y no siempre son favorables a los intereses del que nos contrata.

Trabajamos bajo presión en cada actuación, en cada informe que redactamos y en cada ratificación ante un Tribunal, pero nos enfrentamos a esas dificultades convencidos de nuestros conocimientos (que actualizamos constantemente), apoyándonos en nuestros compañeros (que saben lo que estamos pasando), y a la comprensión de nuestras familias que viven nuestras preocupaciones y nuestras jornadas maratonianas sin saber lo que

estamos haciendo porque el Secreto Profesional nos impide dar detalles.

Nuestro trabajo es complejo y variado. Desde la primera entrevista con el cliente, hasta la ratificación de nuestro informe ante un Tribunal, pasamos por distintas fases que debemos dejar perfectamente documentadas para no dar pie a que la prueba pueda ser invalidada. Un trabajo apasionante y meticuloso, al que espero acercaros de la forma más comprensible a través de este libro.

CAPÍTULO I: EL PERITO INFORMÁTICO FORENSE.

Si desglosamos la palabra Perito Informático Forense y buscamos su significado, nos encontramos que, según reza la Wikipedia, atendemos a las siguientes definiciones:

"El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.".

"El perito judicial o perito forense es un profesional dotado de conocimientos especializados y reconocidos, a través de sus estudios superiores, que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen. Existen dos tipos de peritos, los nombrados judicialmente y los propuestos por una o

ambas partes (y luego aceptados por el juez o el fiscal), y ambos ejercen la misma influencia en el juicio."

"Los peritos judiciales son capaces de ejecutar, aplicar y utilizar todas las técnicas y recursos de una forma científica para una adecuada administración de los requerimientos de su campo laboral (recolección de pruebas, aseguramiento, preservación, manejo de la cadena de custodia necesaria para esclarecer la verdad, etc.).".

Creo que todo esto hay que explicarlo en palabras comprensibles para todos, porque cuando alguien te pregunta a qué te dedicas y le dices "soy Perito Judicial Informático Forense" le cambia la cara al que tienes delante porque no sabe cómo cuadrar todas las imágenes que se le vienen a la cabeza, veamos: al oír "perito judicial" la imagen que se proyecta es a una persona en un juzgado, "informático" rápidamente te ven con un ordenador, de momento la imagen que tienen de ti es una persona con un ordenador en un juzgado … hasta ahí todo bien, pero al llegar a la palabra "Forense", la imagen se distorsiona del todo. Rápidamente el que ha preguntado tiene una imagen muy clara, en su cabeza "forense=autopsia=sangre" y ahí ya está liada porque la idea que se proyectan sobre tu trabajo es una persona con un ordenador en un juzgado ensangrentada por todas partes, y eso suena a película de terror, y así lo expresa su cara.

Espero que, a través de este libro, el lector se haga una idea adecuada sobre nuestra profesión y el trabajo que desempeñamos.

Entonces, si el Perito Judicial Informático Forense no es una persona ensangrentada en un Juzgado con un ordenador, ¿qué hace exactamente esta persona y a qué se dedica? Lo cierto es que esa imagen que se proyecta en la gente está muy lejos de la realidad.

Un Perito Judicial Informático Forense es un profesional del mundo de la informática o las telecomunicaciones, con altos conocimientos de alguna rama de su profesión y de las leyes que le competen para el desempeño de su trabajo, que posee la certificación de su profesionalidad otorgada por una Asociación o Colegio reconocidos para tal efecto. Puede intervenir en un Juicio contratado por alguna de las partes o llamado por la autoridad judicial para dar luz sobre algún tema de su competencia. Cabe reseñar que nuestro trabajo no siempre va encaminado a terminar ratificado ante un Tribunal, como comprobaremos más adelante al hablar de algunos casos que contaré de ejemplo.

El Perito Judicial Informático Forense es el encargado de realizar las siguientes acciones cuando hay de por medio evidencias digitales o telemáticas: extracción, conservación y análisis, manteniendo la Cadena de Custodia, para realizar un informe con las conclusiones de la

investigación y asegurar que las evidencias son admisibles, auténticas, completas, confiables y creíbles.

Cuando alguien tiene un problema en el que lo tecnológico juega un papel importante y necesita de nuestros servicios (normalmente asesorado por algún otro profesional: abogado, detective, o por algún conocido que nos ha necesitado), el primer paso es tener una primera reunión cara a cara con el futuro cliente. Esta reunión la empleamos para conocer el alcance del problema y limitar nuestras actuaciones para asegurar el mejor fin posible. En esta fase es cuando explicamos al cliente nuestra forma de trabajar y las posibilidades que existen, siempre buscando asesorar al interesado para centrar el trabajo y optimizar los recursos y los gastos que se le originarán.

Aquí es cuando nos encontramos las mayores sorpresas, con las peticiones del futuro cliente, es cuando averiguamos si realmente saben cuál es nuestro trabajo o si nos siguen viendo como un personaje extraño que hace cosas raras. No es la primera vez que recibo una llamada de un posible cliente y salta una pregunta "maliciosa" del tipo: "¿sabe hacer un bicho para meterlo en un móvil y borrar cierta información?" o "¿Pueden instalarle a XXX algo en el móvil para controlar lo que hace sin que se note?".

Cuando recibes estas preguntas sabes a ciencia cierta que esta persona no tiene nada claro lo que somos y lo que hacemos, por lo que empiezo con las explicaciones y la respuesta es siempre la misma:

"Sí que sabemos hacerlo, pero no hacemos ese tipo de servicios porque van contra la Ley. Debe entender que para poder identificar este tipo de delitos debemos conocer cómo se realizan (técnicas, programas, metodologías,…), pero nosotros somos de los buenos y no nos dedicamos a dar este tipo de servicios. Podemos ayudarle con su problema con los medios que nos permite la legalidad vigente".

Normalmente entran en razón y olvidan el tema o se preocupan de la manera legal de actuar.

Una vez que dejamos claro lo que hacemos, llega la siguiente dificultad, explicar la "Cadena de Custodia" y por lo tanto la necesidad de realizar la extracción de evidencias delante de un Fedatario Público (es decir, un Notario o un Secretario Judicial). Y ¿Por qué es un escollo? Muy fácil, cuando nos llega un cliente, lo que quiere es que le arreglemos el problema de forma rápida y económica, el cliente normalmente no entiende de leyes ni de tecnología, tiene un problema y sabe que se lo podemos solucionar, pero nunca se ha planteado todo el proceso para poder aportar la evidencia como prueba ante un Juez y que éste no la desestime por haber dudas

en el proceso de extracción o en la Cadena de Custodia.

Sí, las evidencias son frágiles en su manejo, y no se pueden conseguir de cualquier forma, ni se pueden conservar como nos apetece. Todo tiene un protocolo para que la prueba no sea contaminada y pueda ser aceptada por el Juez y ser efectiva en un proceso judicial.

Es curioso constatar cómo no se concebiría ver un escenario de un delito en el que los policías que estén recogiendo las pruebas no lleven guantes para no alterar la presencia de huellas, o no fotografiasen el lugar donde las encuentran. Parecería de locos si los policías cogiesen esas pruebas y, en lugar de meterlas etiquetadas en bolsas de pruebas, las metiesen todas juntas en una bolsa de supermercado. Sin embargo, en el caso de las evidencias digitales o telemáticas no se entiende este concepto.

Mi empeño y el de mis compañeros es dejar claros estos matices sobre nuestro protocolo de actuación para que todo el mundo entienda y respete los procedimientos de extracción de evidencias y que puedan ser empleadas en un litigio. Voy a explicarlo con el símil del escenario de un crimen: los Informáticos Forenses llegamos a la escena de un crimen, por ejemplo un ordenador. En esa escena tenemos que buscar las evidencias (si existen) del "problema" que sufre el cliente (fuga de información, espionaje,

comunicaciones, …), para no contaminar las pruebas trabajamos con copias y no con originales y para que no exista duda alguna del entorno y de nuestros trabajos, realizamos el procedimiento de extracción documentando todo lo que hacemos y con un Fedatario Público que levanta acta de todo lo que sucede durante el protocolo (al estilo de los policías judiciales que van fotografiando las pruebas encontradas en la escena del crimen).

Esta parte de nuestra actuación es vital dentro del proceso para poder emplear las evidencias como pruebas en un litigio. Cualquier duda que arroje nuestra actuación podrá dar al traste con la prueba en el juzgado. Por eso es tan importante, para poder demostrar que las cosas están donde están y que no es una invención del perito, que el Fedatario Público levante acta de todo, dando fe de la existencia de las evidencias en el lugar que indicamos, y que las evidencias no son manipuladas durante el proceso de extracción y asegurando la Guarda Custodia de los originales para posibles investigaciones futuras.

Cuando realizamos un protocolo de extracción de evidencias, el material que empleamos para guardarlas debe ser nuevo y estar precintado, de forma que el Fedatario puede asegurar que no se contaminan las evidencias con este material por estar totalmente nuevo y vacío. Al estilo de las evidencias que toma la policía en el escenario de

un crimen metiéndolas en contenedores nuevos y descontaminados, ¿alguien daría credibilidad a una prenda manchada de sangre del presunto agresor que se guarda en una bolsa reutilizada y con sangre de otros procesos? Está claro que no. Debemos ser asépticos en nuestro proceder y en nuestro material.

Una vez extraídas las evidencias, los originales se deben custodiar para posibles investigaciones futuras, asegurando que no se manipulan desde el momento en que se obtienen las evidencias, de tal forma que si en un futuro se vuelven a extraer serán exactamente iguales al momento del inicio de la investigación.

Parece una labor sencilla, pero la realidad dista mucho de la teoría. Es un proceso en el que hay que andar con pies de plomo, en el que hay que ir preparado para todo, porque no nos podemos permitir el privilegio de parar una actuación por no tener el material apropiado para sacar esas copias.

Sí, sí, ya lo sé, cuando vamos a realizar un protocolo de extracción de evidencias parece que nos vamos de viaje o que nos vamos a mudar a casa del cliente, a la Notaria o al Juzgado.

Debemos llevar toda clase de material para asegurar que podemos afrontar cualquier imprevisto: toda clase de conectores, varios discos nuevos con distinto tipo de conexión y tamaño, pegatinas de evidencias, clonadoras de

alta velocidad, discos externos, usb nuevos de distintas capacidades y precintados, precintos, bolsas de Faraday, bolsas antiestáticas, destornilladores, guantes de látex, portátil, cuaderno, bolígrafo, rotulador indeleble … Cualquier material que pensemos que nos puede sacar de un apuro y que nos evite poner en peligro el protocolo.

Es uno de los momentos de mayor tensión, meter la pata durante el protocolo puede dar con las pruebas en el cubo de la basura y, lo que es peor, inutilizados los originales. Esta es una de las razones por las que es mejor acudir a profesionales contrastados y experimentados y no a cualquiera que diga que puede hacerlo y que es muy barato, ya que, seguramente no esté certificada su profesionalidad y lo que, en principio, sale barato al final puede salir muy caro. No se puede prescindir del Fedatario Público, ni de la Cadena de Custodia, porque todo el trabajo realizado será tirar el dinero del cliente y nuestro prestigio como profesionales quedará por los suelos.

Es muy importante trasladar al cliente el protocolo a seguir y explicarle muy bien las consecuencias de no realizarlo correctamente. Yo, personalmente, si un cliente quiere ahorrarse el dinero del Fedatario Público, no acepto el trabajo. Prefiero no hacer un trabajo a jugármela haciéndolo mal.

Ahora llega el momento de analizar bien las evidencias para elaborar un buen informe. Tiempo de soledad y concentración en el laboratorio. Toca echar horas revisando y analizando las evidencias extraídas, sin dejar pasar por alto ningún detalle. En ocasiones me encierro en la cabina de audio del laboratorio para aislarme del mundo y centrarme en el trabajo. Durante el análisis solo existimos en el mundo esas evidencias y yo, sin móvil que me pueda desconcentrar, sin gente alrededor. Eso sí, cuando entro en la cabina, que está insonorizada, siempre hay alguien enterado de que me encuentro metido y, de vez en cuando, se pasan y ven por el cristal que sigo bien.

Cuando trabajo con algún compañero hacemos el trabajo en paralelo y luego lo comentamos (es la forma de no dejarnos influir en nuestro análisis).

Lógicamente, si ocurriese algo de vital importancia, un compañero me saca de la cabina para que me entere, pero debe ser algo realmente urgente o importante.

Es el momento más íntimo y especial de todo el trabajo, dentro de esa cabina estamos las evidencias y yo, no existe nada más, no existe nadie más.

En ocasiones imagino cómo sería realizar ese trabajo con los niños correteando, el teléfono sonando, las obras del vecino… Está claro que para este trabajo se requiere especial

concentración para evitar fallos o despistes. Nuestro cliente se juega mucho y debemos demostrar nuestra profesionalidad, aunque luego tengamos que escuchar infinidad de veces "eso lo hace cualquiera", "el informático de mi empresa certifica tal o cual y tarda dos minutos en hacerlo", … Sí señor, su informático lo hará en dos minutos, pero dudo mucho que su trabajo tenga validez procesal, porque de tenerla se tomaría tan en serio ese certificado que ya no tardaría dos minutos.

Tras realizar un análisis exhaustivo de las evidencias, interpretando la historia que esconden detrás, buscando encontrar respuestas al trabajo que se nos ha encomendado, es el momento de contrastar el análisis con Raúl, compañero de fatigas y sobre todo buen amigo.

Juntos revisamos y compartimos nuestros análisis y elaboramos el informe con las conclusiones. Es importante precisar que nosotros no juzgamos, analizamos las evidencias y hacemos el informe para que el abogado pueda usarlas como pruebas en un juicio.

Cuando terminamos el informe y, tras revisarlo unas cuantas veces, lo firmamos los dos. Mucha gente nos pregunta por qué firmamos el informe dos peritos aunque sea un trabajo con pocas evidencias con las que trabajar (cuando se trata de un caso muy complicado todo el mundo

entiende que podamos intervenir y firmar el informe varios peritos).

La respuesta es sencilla y es algo que he aprendido con el tiempo: "Nunca dejamos tirado al cliente", es decir, si yo hago un trabajo y solo yo firmo el informe, seré el único que pueda ratificarlo en Sede Judicial. ¿Y si me pasa algo? El cliente habría pagado el trabajo, pero no serviría de nada. Sin embargo, si lo firmamos dos peritos y uno no puede asistir, el otro lo puede ratificar en Sede Judicial y el cliente siempre tiene respuesta.

Antes de entregar el informe y reunirnos con el cliente y el abogado para explicarlo, enviamos el informe a visar por nuestra Asociación. Se trata de un proceso importante porque el comité de expertos revisa el informe para certificar que hemos realizado todos los pasos correctamente, que lo hemos redactado de manera comprensible y que cumplimos con las normativas de calidad y profesionalidad que se nos marcan. Este visado es una garantía de que el perito firmante no ha llegado a unas conclusiones "forzadas" por nadie, sino que es el resultado de su buen hacer y sus conocimientos.

No sería la primera vez que se nos ha ofrecido algún incentivo importante por orientar o cambiar nuestro informe. Con el visado se evitan esas tentaciones y se da una garantía en el proceso. Sobre todo sabiendo que si mientes ante

un Tribunal… se acabó tu carrera y te llevas alguna sorpresita desagradable en forma de querella.

Llegó la hora, hemos extraído las evidencias, realizado el análisis, realizado el informe, preparado con el abogado cómo presentar las pruebas explicándole a fondo el informe, y ahora ya estamos en el Juzgado para ratificar el informe.

Aquí sí que te sientes más sólo que un portero en un penalti. Estás esperando a entrar en la sala y hay un montón de gente que te mira como si fueses un bicho raro. Seguramente no has dormido la noche anterior (porque, por muchas veces que vayas a un juicio, siempre te juegas algo importante), seguramente ni desayunes (para evitar las ganas de ir al baño en un mal momento), y, además, el tiempo pasa muy despacio, ves entrar a los testigos uno a uno y a otros peritos, siendo el perito informático el último en entrar a sala.

Son momentos de recogimiento repasando el informe que realizaste hace meses, de conversar con otras personas que están esperando y explicarles lo que haces para que no te vean como un extraterrestre, momentos de charla con algún compañero que va de apoyo, hasta que, de repente, se abre la puerta y sale el secretario judicial que pronuncia tu nombre. Ha llegado tu momento, te juegas todo el trabajo realizado en

la defensa de tu informe. Es como jugarse el resultado de un partido con un match ball.

Te acercas al secretario para identificarte y, en ese momento, pueden ocurrir dos cosas:

1. Que te diga que te puedes ir, que el informe es claro y no hacen falta aclaraciones (por un lado te sientes aliviado, por otro piensas "¿todo el día aquí para nada?").
2. Que entres a sala y demuestres tu profesionalidad, con seguridad y estilo, teniendo claro lo que hablas y haciéndote entender (cosa complicada si tenemos elementos muy técnicos), dejando los nervios fuera de la sala y seguro de tu trabajo.

Al finalizar el juicio, según sales del Juzgado, buscas el bar más cercano para reponer fuerzas, que llevas mucho tiempo sin comer nada.

Ahora toca esperar de nuevo, esta vez, a que salga la sentencia.

Días o meses después de terminado el juicio llega la llamada del cliente, diciéndote que ya tiene la sentencia y que ha ganado. A ti te hace tanta ilusión como a él y lo celebras con tus compañeros o con tu familia, sin poder dar más datos del trabajo que un simple: "hemos ganado".

En el caso de que la sentencia sea desfavorable te molestará, aunque tu trabajo haya sido excelente y no fuese clave en el proceso.

A fecha de escritura de este libro, puedo decir que solo he conocido el caso de la victoria de todos mis clientes, llevándome grandes alegrías, pero soy consciente que llegará el día en el que la sentencia sea desfavorable, no debiendo nunca bajar la guardia para evitar que eso ocurra.

En este libro, quiero compartir unos casos de éxito explicando el trabajo realizado desde el punto de vista del Perito Informático Forense, con la intención de dar un poco de luz sobre nuestro trabajo y que se nos empiece a ver como un elemento más de la compleja maquinaria de la Justicia y no como un bicho raro que hace "magia tecnológica".

Las historias que comparto a continuación son el fruto de la experiencia y de muchas horas metido en la cabina de audio, aislado del mundo, analizando evidencias y descubriendo la historia que esconden.

CAPÍTULO II: EL ARCHIVO DE AUDIO.

En los tiempos que vivimos es cada vez más común que, en el mundo laboral, tanto empresarios, como empleados, busquen guardarse las espaldas por lo que pudiera ocurrir. En este escenario, un cliente solicitó mis servicios para certificar un audio grabado con su móvil, con el que podía demostrar que la causa de su despido era falsa y que, por lo tanto, su despido era nulo.

Veamos el procedimiento realizado en este caso. Lo primero, cuando recibí el encargo, fue concertar una entrevista con el futuro cliente para delimitar los objetivos del trabajo.

Durante la entrevista me detalló las circunstancias: había sido despedido de su empresa alegando que realiza unos trabajos por su cuenta y sin informar previamente a sus jefes.

Sospechando que querían despedirle y buscaban algún motivo, decidió grabar la reunión de seguimiento de proyectos que tenían en la empresa cada dos meses. Para la grabación empleó la aplicación de grabación del móvil, que lo dejó discretamente sobre la mesa de la reunión.

El trabajo consistía en hacer una certificación del archivo de audio para emplearlo como prueba y demostrar que, en esa reunión, el despedido no

sólo informó a sus jefes, sino que también había puesto de manifiesto los riesgos del proyecto.

Antes de aceptar el caso, consulté con mi compañera Laura (Abogado Tecnológico) sobre la legislación vigente en cuanto a grabaciones realizadas sin informar de su realización y la posibilidad de aportar éstas como pruebas en un litigio. Aunque los peritos estudiamos Derecho y procuramos estar al día en cuanto a lo que la legislación se refiere, para evitar sustos, es preferible contrastar la información con un abogado experto en estos temas.

Efectivamente, al ser una grabación de una conversación donde participaba el despedido y, al tratarse de un juicio de laboral, se podría emplear la grabación como prueba. Por lo que, una vez recibido el visto bueno por parte de mi asesora legal, comencé con el protocolo.

Tras firmar los documentos de confidencialidad y aceptación del presupuesto por el cliente, quedamos en el Notario para hacer la extracción de evidencias, asegurando la Cadena de Custodia y la Guarda Custodia de las mismas.

Nos personamos en la Notaria y, tras preparar todo el material y verificar la firma de los acuerdos de confidencialidad y de consentimiento de acceso, comenzamos el protocolo de extracción: tomando los datos de todos los elementos que intervienen en el proceso y cada paso que se da. En este caso,

además, realicé una grabación de prueba posterior con el terminal del cliente, para tener una muestra con la que comparar, lo que me ayudaría en el posterior análisis.

Tras la extracción, calculo el HASH de los archivos extraídos. El HASH es un código numérico que se calcula en base a una fórmula matemática, de tal forma que si se calcula varias veces sobre un mismo archivo siempre da el mismo resultado, a menos que el archivo se modifique, lo que produciría que el resultado de la formula cambie. Es decir, una vez calculado, si se vuelve a calcular y no da el mismo resultado, podemos asegurar que el archivo se ha modificado. Guardo una copia de las evidencias con un fichero de texto con los HASH correspondientes a cada una de ellas en un pendrive, perfectamente precintado y etiquetado con los datos del caso, tipo de prueba, perito y fecha de extracción, para su depósito en la caja fuerte del Notario hasta la finalización del proceso judicial.

Por supuesto, no abandono el despacho del Notario sin tener firmado el registro de la Cadena de Custodia.

Es el momento de preparar todo el material para empezar el encierro en la cabina de audio y realizar el análisis en el laboratorio.

El fichero es de una hora y cuarto. El cliente me dijo que lo útil eran solo cinco minutos y que se

podía cortar para reducir. En ese momento ya le expliqué cómo funcionan las evidencias digitales: si las manipulas no son válidas, hay que entregarlas exactamente como son; además, tal y como digo en las charlas que imparto en los colegios, cuando sacas algo de contexto cambia totalmente su significado.

En el caso de un audio: imaginemos que estamos grabando una función de teatro amateur; durante la actuación y, siguiendo el guión, un actor amenaza a otro.

Si escuchamos toda la grabación, nos hacemos una idea de la obra de teatro, pero ¿qué ocurriría si solo escuchásemos la parte en la que un actor amenaza a otro? Con el audio de ese trozo de la obra, fuera de contexto, nos haríamos una idea equivocada del contenido de la grabación, pasando de ser una obra de teatro a ser una amenaza de una persona a otra.

Teniendo claro este supuesto, una de las cosas que debemos descartar en el análisis es que el audio haya sido editado, que no tenga cortes, que tenga coherencia. Buscamos cualquier pista que nos ofrezca indicios de manipulación del audio, empleamos distintos programas para estudiar los metadatos (datos ocultos que dan información de los ficheros), el espectro de onda, los ruidos que puedan existir, la existencia de capas ocultas. Una vez que lo he escuchado tantas veces que casi me lo sé de memoria, que he

analizado el fichero de audio de evidencia comparándolo con el audio de test que grabamos de muestra en la Notaría, tras realizar los múltiples procedimientos para validación de audios que tenemos y de tener claro que puedo certificar el audio sin lugar a dudas, empiezo a elaborar el informe.

Durante todo el proceso de análisis he ido documentando cada paso, siguiendo los protocolos correspondientes. Toda esta documentación la emplearé al redactar el informe, para explicar todo el proceso de análisis y dejar claro cómo llego a las conclusiones finales, para que no exista ningún tipo de dudas sobre las mismas.

Los informes que realizamos cumplen con la UNE197001:2011 en su estructura. Plasmamos todo el proceso del trabajo desde el principio hasta las conclusiones que se presentan ante el Tribunal, de tal forma que explicamos el encargo, el procedimiento de extracción ante el Fedatario público, el análisis y terminamos con las conclusiones, que deben ser claras, concisas, y responder a las preguntas planteadas al comenzar el trabajo.

En el caso que nos ocupa, las preguntas planteadas al comenzar el trabajo eran claras:

- ¿El fichero de audio es auténtico? es decir, ¿se grabó con ese terminal identificado, en

el lugar y fecha que se celebró la reunión grabada?.

- ¿El fichero de audio ha podido ser manipulado desde su grabación?

El análisis fue complejo, el fichero había sido grabado casi un año antes de la pericial, por suerte el teléfono no había sufrido ningún percance y el archivo permanecía con todas sus propiedades.

Me puse en contacto con el fabricante del terminal para solicitar información sobre los metadatos asociados a los ficheros en sus grabaciones, sistema de grabación empleada, compresión de información, así como sobre el registro de algún tipo de marca oculta (lo mismo que en balística, en que se estudian las marcas que el cañón del arma, por sus imperfecciones, puedan causar a los proyectiles, sirviendo, de ese modo, para poder asociar un proyectil con un arma concreta).

Una vez que me facilitaron toda la información, empecé mi encierro en la cabina de audio que tenemos en el laboratorio forense.

Fueron días muy intensos porque, aunque normalmente tenemos tiempo sin agobios para realizar el trabajo, hay ocasiones, como ésta, en que tenía solo 10 días para realizar todo el

trabajo y que el abogado del cliente presentase el informe junto con la prueba.

Cuando recibes un encargo de este tipo, siempre está presente la sombra de la duda, ¿tendré tiempo suficiente? ¿Podré descubrir la realidad de la evidencia? ¿Será real la evidencia? Debes planteártelo todo y dar mil vueltas a cada protocolo que ejecutas, tienes que asegurarte que no te la están colando y que no vas a llevar a un Tribunal una prueba como real si no estás al cien por cien seguro de que realmente lo es.

Lo que sí quiero dejar claro es que mi trabajo no consiste en dar la razón a mi cliente pase lo que pase. Mi trabajo es analizar evidencias para certificar su autenticidad y trabajar con ellas, siguiendo unos protocolos efectivos para poder presentarlas como prueba, sin dejar lugar a dudas acerca del procedimiento seguido, lo que podría suponer una prueba inválida que no tendría ningún efecto en el proceso. En algún caso el resultado de las investigaciones no es el que quiere el cliente, pero siempre es lo que cuentan las evidencias.

Por suerte, hasta la fecha, no han tratado de colarnos muchas pruebas manipuladas y, cuando lo han intentado, lo hemos detectado, evitando su presentación en un proceso judicial.

En este caso, tras varios días de encierro y trabajo a conciencia, el resultado de las preguntas era el esperado por el cliente:

- El fichero de audio era auténtico y se había grabado con el terminal aportado en fecha, hora y lugar en que se celebró la reunión grabada.
- El fichero de audio no había sido manipulado desde su grabación.

Una vez redactado el informe y revisado unas cuantas veces para asegurarse que está bien escrito y que me expreso de forma perfectamente comprensible por alguien que no tenga conocimientos de la materia, lo envío a visar a la Asociación, abstrayéndose del fondo del asunto.

El proceso de visado consiste en una revisión por parte de un grupo de expertos que certifica la correcta realización de los protocolos y la estructura del informe para comprobar que cumplen con las normativas vigentes.

Tras el visado, entrega al cliente y a esperar la citación para ratificar el informe en sede judicial.

Y llegó el día de la ratificación. Llego tempano al juzgado repasando el informe para contestar a las preguntas que puedan hacerme tanto los letrados como el magistrado y a esperar en la sala de espera, junto a testigos, peritos y abogados de esa causa y de otras que comparten la misma sala de espera.

El juicio es a las 10:00; a las 13:30 aproximadamente deciden que hay que ampliar demanda y se suspende la sesión hasta dentro de

un mes. En ese momento, recoges tus cosas, te despides y esperas la nueva citación, sabiendo el cliente que te deberá abonar la nueva jornada.

En la segunda citación para el juicio, mismo procedimiento, llegada temprano al juzgado con una copia del informe para repasarlo (aunque antes de ratificarme en sala se me facilitará el informe para revisar que es el mío) y a esperar a que me llamen.

En esta ocasión pasan unas nueve horas de juicio y veo entrar a cada testigo, a los peritos de otras especialidades, nueve horas departiendo con la gente que está en la sala e intercambiando tarjetas con otros profesionales, y por fin a las 19:45 sale el secretario y me llama: *"¿el perito informático?"*, "sí, soy yo" (mientras saco mi carnet para acreditárselo), *"muchas gracias por venir, no hace falta que entre a ratificar su informe, está muy claro y las partes lo han admitido sin presentar dudas, puede irse".*

Trabajo bien hecho y terminado. Espero en la sala a que salgan todos para despedirme del cliente y a esperar el día que reciba la sentencia y me llame para contármelo.

Unos meses después recibí la llamada. El cliente estaba contentísimo, ya tiene la sentencia: despido nulo, reincorporación a su puesto de trabajo y recibirá una indemnización por el tiempo transcurrido. El hombre está feliz y ahora ya sabe él y todo su círculo quienes somos y lo

que hacemos. Él recupera su vida y nosotros a seguir con nuevos casos, pero por muchos casos que lleve, puedo asegurar que me acuerdo de cada cliente, cómo llegaron agobiados por la situación y un poco escépticos de nuestra figura en el proceso.

CAPÍTULO III: FUGA DE INFORMACIÓN.

Este caso resultó muy interesante en cuanto a la actuación y el análisis. Estaba tranquilamente leyendo un libro y recibo la llamada de mi Asociación, un trabajo pericial de urgencia y sin muchos detalles.

Cojo el maletín de periciales (que lleva todo lo necesario para evitar sorpresas en la actuación) y el portátil, me subo al coche y llamo a la Asociación para recibir las coordenadas y más información.

El trabajo consiste en asistir a una empresa en la que hay dos trabajadores de los que se sospecha que están sacando información confidencial corporativa, clonar los discos de los equipos ante el Notario y realizar la investigación oportuna. Es un viernes a mediodía y sabemos que cada usuario tiene dos o tres equipos con los que trabaja, así que llamo a mi compañero Raúl como refuerzo y quedamos en la empresa del cliente.

De camino, el cliente me informa que el Notario de zona no puede acercarse. Esto nos genera un pequeño problema porque no podremos hacer las clonaciones asegurando la Cadena de Custodia. Solución: precintar los equipos para su traslado a la notaria y realizar allí los clonados de los equipos asegurando la Cadena de Custodia y el protocolo de salvaguarda de las evidencias.

Una vez explicado el procedimiento al cliente, y tras asegurarnos que los empleados tienen firmadas las políticas de uso de los equipos corporativos, nos reunimos en la sala del Consejo de Administración de la empresa con los dos trabajadores afectados, sus representantes sindicales, representantes de la empresa, los abogados de la empresa y tres testigos. Explicamos el proceso a seguir a todos los asistentes y se levanta acta de la reunión que se firma por todos los presentes. Acto seguido, procedemos a identificar los equipos de los trabajadores y los precintamos, levantando acta de cada equipo precintado (acta que firmamos todos los involucrados en el proceso). Una vez precintados, trasladamos los equipos a las oficinas del Notario, donde quitamos el precinto y llevamos a cabo el protocolo de clonación de los discos de los equipos. Una vez terminada la clonación, precintamos los discos originales para su custodia por parte del Notario.

Para el protocolo de clonado de los discos, llevamos dos clonadoras de alta velocidad de nuestro laboratorio y discos nuevos precintados. Realizamos el clonado de los discos en unas siete horas, calculamos los HASH de los discos para comprobar que los clones son exactos y precintamos cada original. Durante todo el proceso (desde nuestra llegada a la empresa) vamos documentando todo el proceso gráficamente.

Al abandonar la Notaria, los discos originales se quedan precintados en la caja fuerte del Notario para su custodia, los discos clonados nos los llevamos para su análisis y los equipos (sin disco duro) se los llevan de vuelta a la empresa.

La parte más desagradable del trabajo ya ha pasado. Ahora Raúl y yo nos vamos al laboratorio para empezar con el análisis de los discos.

Para el análisis de estas evidencias empleamos varios programas de informática forense con los que sacamos toda la información que necesitamos. Realmente sacamos muchísima información, por lo que debemos filtrarla y analizar aquello que nos puede servir para el trabajo que estamos realizando.

Una vez analizados los discos y la actividad de los usuarios en esos equipos, y que de toda la información hemos separado el grano de la paja, nos reunimos (que hemos realizado el análisis por separado) y analizamos juntos los resultados para ver si alguno nos hemos saltado algo. En este trabajo, si se parte del mismo origen y se emplean los mismos métodos, el resultado debe ser el mismo.

Tras el análisis conjunto, empezamos a desarrollar el informe, dejando muy detallado en la parte de análisis la información relevante para el caso y cómo la hemos extraído.

CAPÍTULO IV: SECUESTRO TECNOLÓGICO.

Es curioso ver cómo las empresas se gastan miles de euros en sistemas de seguridad y luego dejan todo el poder en las manos de un solo individuo.

Este caso comenzó cuando me llamaron de una empresa que, tras despedir a una de las trabajadoras del departamento de Informática, se dieron cuenta de que era la única que tenía las claves de administración de los sistemas y la documentación de cómo estaban montados todos los sistemas de información corporativos. En el momento del despido nadie se había percatado de este problema en la empresa y, posteriormente, se encontraron con la negativa de la ex trabajadora para facilitar esta información.

En medio del caos y del pánico que se generó entre los directivos, y como uno de ellos me conocía por referencias, me llamaron para que estudiásemos la situación y les ayudásemos a securizar la empresa, tomando todas las evidencias necesarias para poder presentarlas en el posible Juicio.

En la primera reunión, acotamos el alcance del trabajo y de los recursos necesarios. Se trataba de una empresa con tres sedes en España, con conexiones entre ellas y con los clientes de cada zona. Pero a nivel técnico ninguna información.

Lo primero fue contactar con compañeros de las ciudades donde se encontraban las otras sedes para ponerles al día del trabajo a realizar y sincronizar nuestros trabajos (es la ventaja de pertenecer a una Asociación con presencia en toda España).

En menos de 24 horas, nos presentamos cada equipo en una sede de la empresa acompañados de un Notario, lo primero que hicimos fue identificar cada equipo y clonar los discos. En esta ocasión realizamos dos copias de cada disco: cada original, tras el clonado, se precintó y etiquetó para su salvaguarda por el Notario. Después, una copia la dejamos para que el equipo siguiese funcionando y, la otra copia, la empleamos para nuestras investigaciones.

Para no perder evidencias de accesos, dejamos encendidos los routers y firewalls, pero desconectados de la red; pusimos unos nuevos con las configuraciones necesarias para que la empresa pudiese seguir trabajando con normalidad; cambiamos todas las contraseñas, y securizamos cada sede. Fue un trabajo arduo que nos llevó a estar encerrados en las sedes 32 horas seguidas.

Una vez terminado el trabajo de campo, cada equipo nos dedicamos a analizar los discos clonados buscando evidencias de actividades que pudieran ser sospechosas.

En la sede principal encontramos evidencias de fuga de información a través de correo electrónico y dispositivos de almacenamiento masivo tipo USB desde el equipo de la persona despedida. También se encontraron varios equipos con software espía que enviaba la información a un equipo de la tercera sede.

En la segunda sede, encontramos varios equipos con software espía que enviaba la información a un equipo de la tercera sede.

En la tercera sede, encontramos: el repositorio de los sistemas espía y varios equipos con software espía que enviaba los datos al repositorio encontrado anteriormente.

En los servidores de correo encontramos accesos indebidos a distintas cuentas de correo corporativo. En los servidores de archivos encontramos accesos indebidos a los repositorios de Dirección.

De los discos de las impresoras y los servidores de impresión sacamos evidencias de impresiones masivas de documentación confidencial en horarios extraños.

Finalmente, tras reunirnos todos los equipos, atamos cabos con todas las evidencias encontradas y pudimos demostrar que la persona despedida no era la única que estaba realizando trabajos sospechosos, en cada sede tenía un colaborador. Entre los tres se estaban dedicando a sacar toda la información

corporativa confidencial: clientes, proyectos, diseños de soluciones y todo el I+D de la empresa.

El objetivo final era vender toda la información a empresas de la competencia para acabar trabajando en una de ellas, pero las evidencias les delataron y nuestro cliente pudo contener la fuga de información y tomar las medidas legales oportunas contra esos trabajadores desleales.

CAPÍTULO V: PROBLEMAS ESCOLARES.

Una de mis actividades es la de difundir el uso seguro y responsable de las Tecnologías de la Información (TICs) en los centros escolares, impartiendo charlas a los alumnos, padres y profesores sobre los distintos tipos de peligros que se esconden en Internet y sobre el uso responsable de las TICs que tanto se emplean hoy en día.

Fruto de esas charlas, un día me llaman de un centro en el que tenían posibles problemas de ciberacoso, el tema de las TICs les desbordaba y querían saber qué estaba ocurriendo exactamente antes de proceder a poner una denuncia.

Al tratarse de un centro escolar, las implicaciones legales de cada paso que se da pueden ser muy diversas, así que me presenté en el centro con mi compañera Laura (Abogado tecnológico) para asegurar legalmente cada acción y evitar problemas.

Lo primero fue reunirnos con el equipo de Dirección del centro para hacer una toma de datos del posible problema y acotar nuestra actuación.

Una vez que recopilamos toda la información necesaria, acordamos organizar unas charlas para familias del centro y para los chavales del ciclo afectado para poder hablar con ellos y

analizar sus hábitos con las TICs y las Redes Sociales (RRSS).

Mientras yo impartía las charlas, Laura se entrevistaba con los profesores y el personal del centro en busca de más información.

Las actuaciones comenzaron a dar resultados. En una de las charlas unos alumnos hablaron de una niña de otra clase que tenía problemas con las RRSS. Nos pusimos en contacto con los padres y mantuvimos una reunión con ellos y con la niña.

Conseguimos, tras firmar todos los contratos de confidencialidad y de consentimiento de acceso, conectarnos a sus perfiles de RRSS y al móvil de la joven para analizar lo que estaba ocurriendo.

Encontramos una imagen publicada por un "amigo" en la que la chica salía en una postura un tanto ridícula y que es la que estaba produciendo que se convirtiese en el objetivo de las risas de grupo de compañeros.

Analizando la imagen, descubrimos que era un recorte de otra imagen. En la original se apreciaba en primer plano a varios alumnos en una excursión y, en segundo plano, a esta alumna en una posición rara.

Seguimos investigando y encontramos que esa imagen fue tomada por un padre en una excursión y que su hijo es el que había publicado la foto a su grupo en las RRSS.

Una vez que teníamos claro cómo había aparecido la foto en las RRSS y sabiendo que era un recorte de otra foto (no era una foto hecha con mala intención), los padres de la alumna afectada nos pidieron que se lo explicásemos al alumno que había publicado la foto y a sus padres. Querían arreglarlo sin tener que denunciar.

El colegio convocó una reunión con todos los afectados y les explicamos todo lo que había sucedido: "El padre hace unas fotos en una excursión, el niño ve una parte de una imagen que le parece graciosa, la recorta y la pública a su grupo de compañeros, y ahí empieza el acoso".

Tras la explicación de los hechos, aclaran la situación entre los padres, el niño se ve totalmente sobrepasado por los acontecimientos y comprende lo que ha hecho: una acción que empezó como un juego y que terminó haciendo daño a una amiga.

Los padres de la víctima y la propia niña deciden que, una vez aclarado el tema, lo mejor es que se borre todo y aceptar las disculpas de los padres contrarios.

Desde el colegio nos solicitaron charlas de concienciación para familias y alumnos a los efectos de evitar casos de estos por falta de conocimiento.

Por suerte en este caso salió todo bien y no hubo que lamentar males mayores.

CAPÍTULO VI: USO INDEBIDO DE LAS TIC CORPORATIVAS.

Cada día nos encontramos con nuevos desafíos para las empresas y para los empleados a la hora de controlar la actividad realizada en horario de trabajo y con los sistemas corporativos. Las empresas buscan controlar el buen uso de los sistemas y la optimización del trabajo de sus empleados, pero en ocasiones no tienen muy claro cómo hacerlo, se fían de lo que les cuentan, de lo que leen, pero no asisten a un profesional que les asesore en estos menesteres.

En esta ocasión, acudieron en busca de nuestros servicios dos personas que habían echado de su empresa por uso indebido de Internet. En la carta de despido se adjuntaban unas gráficas justificando ese mal uso: navegación por páginas no necesarias para su trabajo como Facebook, Linkedin, Vibbo, … De modo que la empresa justificó la procedencia del despido de los dos trabajadores en base a esta navegación indebida.

En esta ocasión, el trabajo consistía en hacer un informe que aclarase que los motivos de despido alegados en las cartas no eran atribuibles a los empleados y que los datos empleados para justificar los despidos podían haber sido manipulados.

Al tener que realizar un contra informe y no tener que analizar ninguna evidencia, en esta ocasión

no hubo visita al Notario (no necesitábamos cadena de custodia de evidencias).

Analizando las hojas adjuntas no se encontraba por ningún sitio de dónde se estaban sacando los datos, ni nombre de usuario, ni máquina, ni dirección ip. Tampoco se dejaba constancia de qué software se empleaba para controlar la navegación por Internet en la empresa, o si por el contrario se controlaba por hardware, ningún dato técnico, simplemente adjuntaban unas gráficas en las que aparecía navegación por Facebook, Linkedin y Vibbo en horarios de trabajo.

Siguiendo con el análisis, me encuentro, que la empresa se dedica a la venta de coches y ... ¡Sorpresa!. La empresa tiene página de Facebook donde anuncia sus coches en venta, perfil de linkedin donde publican las ofertas a clientes y emplean el portal de vibbo para consultar precios de otros coches similares a los que venden en el mercado de segunda mano.

Otra peculiaridad que me encuentro en esas gráficas es que, a pesar de que los trabajadores despedidos solo trabajan de lunes a viernes, muestran también en fin de semana, siendo relevante, en ese sentido, el dato de que solo trabajan en fin de semana los empleados del área comercial de su empresa.

Llegados a este punto, realicé un informe explicando todos los indicios que suponían que no se pudiese acusar a los despedidos de uso indebido de los sistemas corporativos con esos informes que les habían entregado. Básicamente se dejaba claro:

1. No estaban identificados los equipos de los trabajadores despedidos, por lo que la información aportada podía ser de cualquier equipo, e incluso de otra empresa.
2. No existían evidencias digitales y, por lo tanto, tampoco había Cadena de Custodia que asegurase su guarda y custodia.
3. En el caso de que los empleados hubiesen navegado por las páginas mencionadas: Facebook, Linkedin y Vibbo, al tener anuncios de coches en venta publicados, se podría haber estado navegando de forma "debida" para asuntos y trabajos corporativos.

En definitiva, en el informe se dejaba claro que, aunque se pudiese vincular a los empleados con esa navegación, no se podía asegurar que esa navegación no se realizase con fines corporativos.

En la defensa del informe ante el Tribunal, el Juez lo entendió perfectamente gracias al aporte

gráfico que llevaba el informe y a la explicación realizada en Sala.

Finalmente, el despido fue declarado NULO por el Juez por falta de evidencias y la empresa fue condenada en costas.

CAPÍTULO VII: TRANSFERENCIA PERDIDA.

Una de las comodidades que tenemos hoy en día es la Banca Online, que nos permite realizar todo tipo de operaciones sin pasar por el Banco (por eso es importante en las empresas tener el mayor número de sistemas de seguridad para la realización de estas operaciones).

Me encontraba en una reunión cuando sonó el teléfono de emergencias, un antiguo cliente, propietario de una empresa, estaba muy nervioso porque había detectado que le estaban "robando" o, por lo menos, que lo estaban intentando.

Tras intentar calmarle, conseguí que me explicase lo que estaba ocurriendo: "alguien había enviado un correo desde su cuenta a la del departamento financiero para hacer una transferencia". Este era el método que utilizaba habitualmente nuestro cliente para realizar las transferencias, por suerte, ese día el hombre se cruzó por el pasillo con el financiero, que le dijo que "ya tenía hecha la transferencia solicitada".

Esta situación hizo saltar las alarmas y pudieron dar marcha atrás a la transferencia y recuperar el dinero, pero vieron que tenían la seguridad de la

empresa comprometida y necesitaban nuestra actuación rápida.

Como la empresa era de 50 trabajadores y necesitaba ayuda para efectuar la investigación de los equipos, rápidamente solicité ayuda a mis compañeros de Asociación y, en cuestión de 10 minutos, ya había seis peritos preparados para ayudarme. Le indiqué al cliente que nos personaríamos en la sede de la empresa con un Notario para clonar todos los discos de los equipos y hacer la extracción de evidencias, salvaguardando, de este modo, la Cadena de Custodia.

Una vez en la empresa, el Notario identificó cada equipo y cada usuario, clonamos los discos de los ordenadores y realizamos la extracción de los correos sospechosos del servidor, los logs de los firewalls,…

Una vez con toda la información adquirida nos lo llevamos al laboratorio para su análisis.

La extracción la realizamos para asegurar que teníamos copia con Cadena de Custodia de las posibles evidencias. Pero empezamos a realizar el análisis de los correos fraudulentos, desde que detectaron el caso del correo falso empezaron a revisar todas las transferencias y vieron que en la

última semana había tres solicitudes de transferencia de distintas cantidades.

Al analizar las cabeceras vimos que el engaño estaba muy elaborado, pero al final siempre se deja rastro del delito y se acaba localizando el fraude.

Analizamos también las trazas de los firewalls y de los servidores de correo. Hicimos una correlación de los eventos de ambos sistemas y finalmente llegamos a una ip que pudimos localizar, un lugar donde curiosamente tenía la oficina el exjefe de ciberseguridad, que había abandonado la empresa dos meses atrás. Rastreamos también las cuentas donde se solicitaban las transferencias.

Finalmente hicimos un informe judicial que el cliente empleó para demandar al avispado exempleado.

CAPÍTULO VIII: ROBO DE IDENTIDAD.

Vivimos en una época en la que la gente vive permanentemente conectada. Se vive más en el cibermundo que en el mundo físico. En cualquier restaurante ves a la personas sentadas en la misma mesa, pero mirando cada uno su móvil y viviendo su propio momento, físicamente en el mismo lugar pero mentalmente a muchos kilómetros de distancia.

Subimos mucha información a la nube, subimos fotos sin pensar si debemos o podemos legalmente hacerlo, exponemos constantemente a nuestros seres queridos en las RRSS sin su consentimiento y, sobre todo, sin su conocimiento. Tenemos una identidad digital que no controlamos y que nos puede llevar a tener grandes alegrías, pero también nos puede llevar a grandes disgustos.

En esta ocasión, me llamaron de la Asociación de Madres y Padres de Alumnos (AMPA) de un colegio donde había estado dando charlas de concienciación sobre el uso responsable de las Nuevas Tecnologías (NTIC). Había un padre que se dedicaba a amedrentar y amenazar a otros padres, llegando incluso a intentar extorsionar a una madre de la Asociación.

El tema era complicado, porque el presunto ciberacosador negaba cualquier actividad de este tipo.

Así que decidimos reunirnos con los afectados y delimitar el contexto y alcance de la pericial (algo especialmente importante en nuestro trabajo para dejar claro hasta donde llegaremos en nuestro análisis, evitando que nuestro servicio se convierta en una especie de modelo de barra libre que una vez contratado pido y pido).

Una vez delimitado el alcance y aceptado el presupuesto, nos reunimos con los afectados que tenían las evidencias para extraerlas ante Notario y después poder realizar el análisis y posterior informe.

Comenzamos a realizar el análisis de las evidencias y el seguimiento de los perfiles de RRSS del presunto ciberacosador (con su consentimiento). Además dio la casualidad de que durante el proceso de extracción de evidencias, en el que estábamos todos presentes, incluso el presunto culpable, una de las víctimas recibió un mensaje.

En esos momentos piensas de todo, los afectados empezaron a decir que con lo que acababan de ver estaba claro que el acusado era inocente, pero también pensaba que podía tratarse de una treta

para parecer inocente sabiendo que todos los afectados estarían de testigos (un mensaje programado, otra persona conectada a tu perfil,…).

Estamos acostumbrados a que lo que vemos no siempre es real en este cibermundo. Ante el júbilo presente de la gente les pedí que guardasen cautela hasta finalizar el análisis de las evidencias y tener unas conclusiones técnicamente claras de lo que estaba ocurriendo.

Una vez con las evidencias y con los seguimientos en RRSS que realizamos, empezamos a sacar conclusiones y vimos que todos los mensajes salían desde su terminal móvil y desde la ip de su casa. En este momento es cuando decidí ampliar el contexto del trabajo y hacer una nueva extracción de evidencias: clonado del disco duro del ordenador personal del presunto ciberacosador y análisis de su terminal móvil en el laboratorio con la Cellebrite (lógicamente, todo ello con el consentimiento de acceso firmado).

Tras mucho análisis, pude aislar el tráfico que se generaba desde esos equipos hacia los perfiles de las RRSS: cada 26 minutos el tráfico se establecía a través de un programilla oculto en el terminal móvil y, cada 53 minutos, desde el equipo de casa.

Tanto el terminal móvil como el equipo estaban infectados con virus que permitían el acceso a las cuentas de RRSS y su control desde otros dispositivos remotos. Las evidencias demostraban que se estaba accediendo a sus perfiles de RRSS desde ips de fuera de España.

Una vez localizado el problema, procedí a limpiar y securizar el terminal móvil y el equipo de casa, y cambiamos las password de todas las RRSS.

Tuve una reunión con el AMPA para explicar lo que había ocurrido y cómo poder evitarlo para el futuro. Finalmente, acabé ese año dando charlas sobre seguridad informática y los peligros de internet a alumnos, familias y profesores. Porque no debemos olvidar que la Seguridad es cosa de todos.

CAPÍTULO IX: LLAMADO POR EL JUZGADO.

En nuestro trabajo, hay ocasiones que son los juzgados los que requieren de nuestros servicios. En este caso me llamaron para un proceso en el que había dos informes periciales (cada parte había aportado uno) y el Juez necesitaba ayuda para dilucidar cuál era el bueno, en el caso de que alguno lo fuera.

En esta ocasión, recibí la comunicación del juzgado por mail y tuve que personarme en el mismo para informarme del encargo y aceptarlo. Cuando fui me entregaron los dos informes fotocopiados y me dieron un mes de plazo para entregar el mío.

En estos casos lo que hacemos es coger cada informe y analizarlo al detalle, saber qué es lo que se pide a cada informe y qué resultado nos aporta. Es muy importante analizar la metodología, cadena de custodia,…

Lo primero que hice con cada informe fue analizar la formación de cada perito firmante, ya que si el perito que firma no tiene la cualificación adecuada para ejercer como tal, el informe no es válido.

En este proceso ambos peritos tenían la cualificación adecuada por lo que, en principio, los dos informes podían ser válidos, así que empecé a analizar cada informe.

En el primer informe no se aportaban las evidencias en digital, por lo que se trastocaba su naturaleza y no se podía realizar un nuevo análisis sobre ellas. Es decir, se trataba de un correo electrónico que se aportaba en papel y no en digital. Un correo electrónico en papel no se puede analizar puesto que es muy fácil su manipulación y no tenemos la información de las cabeceras y los metadatos correspondientes. En definitiva, este informe ya no era válido por no aportar las evidencias en su propia naturaleza "digital" y por basarse en un análisis a un documento impreso fácilmente manipulable y que no nos aporta ningún tipo de garantía digital.

En el segundo informe lo que me encontré era un informe de un correo electrónico "enviado", se aportaba la prueba en su naturaleza digital y respetaba la cadena de custodia. En el análisis del informe se mostraban las cabeceras, pero estas carecían de información relevante. Tras evaluar este informe, no tuve más remedio que darlo por inválido también. En este caso a pesar de cumplir con los requisitos establecidos para los informes periciales y tener las evidencias con Cadena de

Custodia y en formato digital, respetando su naturaleza, el correo electrónico que estaba certificando no se podía certificar por carecer de los metadatos de cabecera necesarios (por ser un correo cogido de la carpeta de correos enviados).

El correo electrónico es como escribir una carta y meterla en un sobre. Si una copia de esa carta la guardo en un cajón (sería como si estuviese en la bandeja de enviados), se puede certificar que se ha escrito, pero no que se ha franqueado y se ha echado al correo, y mucho menos que se ha recibido.

En el caso de una carta que envío, le he tenido que poner un sello y meterla en un buzón, ha pasado por distintas oficinas de correos que le han puesto un sello (en el caso de un email, estos sellos son metadatos que se meten en las cabeceras y que nos permiten certificar su procedencia, envío y recepción), es decir, queda trazabilidad del envío, sin embargo la misma carta que metí en el cajón no dispone de esos sellos porque es una "copia" de lo que "presuntamente" he enviado.

Así que, una vez analizado el informe, también lo tengo que dar por inválido.

Tras realizar el informe explicando los fallos encontrados, lo entregué en el juzgado y, tras

explicarlo en Sede Judicial, el Juez decidió invalidar las pruebas aportadas con los informes periciales por no resultar concluyentes.

Para evitar este tipo de casos, debemos informar al futuro cliente de que no todo vale y hay cosas que no se pueden certificar. Antes de entregar un informe a un cliente, lo enviamos a un grupo de Expertos que analizan la metodología empleada y la forma, pasando todos los filtros de calidad exigidos por las leyes vigentes, sin entrar en el contenido del asunto ni en los datos de los afectados. En este proceso se subsanan los errores que se detectan hasta cumplir los requisitos para obtener el visado, lo que da una garantía extra.

EPÍLOGO.

A través de estas páginas he querido acercar el mundo de las periciales informáticas al lector, un mundo aún muy desconocido pero muy necesario por el avance de las tecnologías y su incursión en la mayoría de los aspectos de nuestro día a día.

Llevamos nuestras vidas en dispositivos móviles, compartimos fotos, vídeos e información de toda clase. Tenemos una identidad digital que no controlamos.

Las nuevas generaciones ven como normal las cosas que hace 10 años nos parecían ciencia ficción.

Y los problemas que teníamos sin la mediación de la tecnología han ido evolucionando y multiplicando sus efectos de manera devastadora: en los colegios siempre han existido casos de acoso que se quedaban en el ámbito escolar y se podían controlar y erradicar desde el claustro, hoy en día el ciberacoso extiende esta problemática más allá del ámbito escolar, dificultando su control con el supuesto "anonimato" que otorgan las redes.

Los delitos, aprovechando también ese supuesto "anonimato" se han incrementado sustancialmente, aprovechando los vacíos

legales, el desconocimiento del usuario, y la proliferación de servicios online.

En estas páginas aprovecho algunos casos para mostrar el trabajo que realizamos. No todos los casos que tratamos terminan en los Tribunales de Justicia. He recogido unos cuantos por su variedad, pero a menudo nos encontramos casos de muy distinto índole por la cantidad de especialidades que puede alcanzar la Informática Forense.

Pero lo más importante de esta obra es dar a conocer la figura del Perito Judicial Informático Forense, un asistente de la Justicia en los casos que dependen de evidencias informáticas o telemáticas.

Una profesión apasionante y muy dura en la que debemos realizar el trabajo con absoluta precisión e imparcialidad, sin atajos, conforme a las leyes vigentes y siempre respetando la Cadena de Custodia para asegurar la guarda custodia de las evidencias para que puedan ser aportadas como prueba en un juicio.

Los Peritos Informáticos Forenses debemos trabajar siempre con absoluta discreción y guardando secreto profesional.

Extraemos las evidencias de los dispositivos de cada caso, nunca nos las inventamos. Llegamos a

conclusiones basadas en el estudio de éstas, no basándonos en la imaginación o en presiones.

Palabras como “pienso” o “creo” no están en nuestro vocabulario, cuando llegamos a una conclusión debemos estar cien por cien seguros de la misma, sin ningún lugar para las dudas.

Pero somos humanos y podemos fallar, por eso tenemos un seguro de responsabilidad civil como lo tienen en tantas profesiones, para trabajar seguros, no para cubrir negligencias.

Quiero terminar esta obra con una frase que forma parte de nuestra profesión y que entre compañeros tenemos muy presente:

“Nunca más caminarás sólo”

Fernando Mairata de Anduiza

Consultor de Ciberseguridad

Cuenta con una larga trayectoria en TICs, habiendo desempeñado puestos de trabajo de responsabilidad en empresas como AIRTEL/VODAFONE, Canal METRO en Madrid y Barcelona, ABALIA CONSULTING. Compagina estudios y docencia, es autor de libros y artículos relacionados con la problemática de las TICs y los menores.

Emprendedor proactivo de la cultura de Ciberseguridad y la docencia de TICs. Implicado activamente: realiza charlas, talleres y formación a profesores, menores, colectivos víctimas de la brecha digital, ofreciendo soluciones de Ciberbullying, Violencia de género digital y otros incidentes en redes sociales y telecomunicaciones.

Cuenta con varias certificaciones en Ciberseguridad, Master de Informática Forense y Pericial por la UDIMA.

Ejerciente como Perito Judicial Informático Forense.