La profesión de Graduado o Ingeniero Técnico de Telecomunicación es la única profesión regulada y oficial que puede realizar peritaciones telemáticas, que como pueden suponer son casi el 100% de las periciales tecnológicas, porque, ¿qué es un móvil, tablet u ordenador sin conexión a una red de datos como Internet?, párense a pensarlo…

Perito judicial en el ámbito de la telemática y las telecomunicaciones, preguntas frecuentes y un pequeño ejemplo real

Javier Marqués Pons.

Fco. Javier Marqués Pons. *Ingeniero y Máster en Telemática*
Vicedecano COGITTCV Colegiado Nº 9724
www.javiermarques.com // javiermarques@coitt.es

Muchas preguntas nos surgen a los que poseemos la profesión regulada de Ingeniero Técnico de Telecomunicación cuando decidimos dedicarnos a la peritación judicial, ¿qué necesitamos?, ¿qué tipos de peritación existen?, etc…

Trabajamos básicamente en pericias para empresas, particulares y Administraciones de Justicia, que necesiten conocer o resolver conflictos o fraudes de los diferentes tipos de delitos y estafas telemáticas, recibiendo un informe pericial, una tasación o valoración profesional en procesos particulares, judiciales, extrajudiciales, legales, científicos y forenses, y siempre todo visado por el COGITT.

En este artículo, intentaremos solventar algunas de esas preguntas, con un pequeño ejemplo real al finalizar dichas preguntas. La información del artículo está prestada por material del COGITT y de ANTPJI, con la que el COGITT ha firmado un convenio de colaboración.

Algunos de los trabajos telemáticos que podemos realizar son:

- Informes y Dictámenes Periciales Judiciales o Extrajudiciales Telemáticas.
- Localización, estudio y extracción de evidencias electrónicas en red.
- Auditorias y Seguridad Telemática Forense Corporativa.
- Valoración y Tasación de equipos tecnológicos.
- Auditoria y asesoría de Seguridad Corporativa e Implantación de la LOPD.
- Asesoría legal Telemática para periciales judicial, extrajudicial, denuncias, demandas y otros procedimientos judiciales, así como uso tecnológico por socios o empleados.
- Mediación Tecnológica.
- Protección de datos en la Red, eliminación de datos, reputación en la red.
- Monitorización y presencia en Redes Sociales.
- Delitos telemáticos bancarios de estafas y sustracción.
- Asesoría sobre falsificación de correos, imágenes, violaciones de seguridad, infiltraciones, doble contabilidad, fraude financiero y de sistemas informáticos, robo de claves, información sensible, secretos industriales, errores en la cadena de custodia.

¿Qué es un peritaje telemático y/o de telecomunicación?

El artículo 335.1 de la LEC (Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil) se refiere a la figura del perito y establece que: Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley,

que se emita dictamen por perito designado por el tribunal.

Así pues, un peritaje es un informe en el que un experto contesta a una o más preguntas o da su opinión profesional sobre cuestiones planteadas por el Juez o las partes. Este dictamen pretende ayudar a una persona que, por no tener los conocimientos técnicos necesarios, no puede responder a dichas preguntas por sí misma, o desea presentar el informe como una prueba. El informe debe ser escrito pensando en su lector, y exponer las conclusiones de manera razonada y comprensible para alguien no experto.

¿Qué es un perito judicial telemático y/o de telecomunicación?

Puede que sea esta la pregunta más repetida en las llamadas de consulta realizadas por profesionales y responsables de seguridad de TICs, abogados, detectives, criminólogos, auditores, consultores, licenciados…

El perito judicial es un profesional dotado de conocimientos especializados en telecomunicación forense y pericial, que suministra información u opinión fundada tanto a los tribunales como a las partes. 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.

Un Perito Judicial es la persona con conocimientos en TIC, que vierte una opinión técnica objetiva sobre las cuestiones que tengan que ver con algún asunto tecnológico, que le plantea alguna de las partes involucradas en un proceso judicial, es decir, estudia las cuestiones que le plantean y aporta sus conclusiones para ayudar al juez a aclararse sobre un tema en el que no tiene por qué ser especialista (aunque sería deseable), pues en ocasiones ocurre que cada una de las partes aportan sus propios informes técnicos con conclusiones totalmente opuestas sobre algún tema en concreto, por lo que el juez no tiene conocimientos suficientes para decidir cuál de los informes es más acertado.

¿Quién puede ser Perito Judicial telemático y/o de telecomunicación?

Cualquier persona mayor de edad que cumpla al menos uno de los siguientes tres requisitos:

- Cualquier profesional que acredite una capacitación universitaria en materia TICs.
- Acredite una actividad profesional de al menos 3 años (incluyendo profesionales independientes como detectives, criminólogos, licenciados, libre ejercientes).
- Disponer de titulación universitaria que acredite la especialidad escogida como Perito telemático y/o de telecomunicación Forense. Aquí, todos los Ingenieros Técnicos de Telecomunicación estamos plenamente capacitados, es más, somos los únicos capacitados, junto con los Ingenieros de Telecomunicación para la labor pericial telemática.

¿Dónde puedo consultar la normativa jurídica que regula esta profesión?

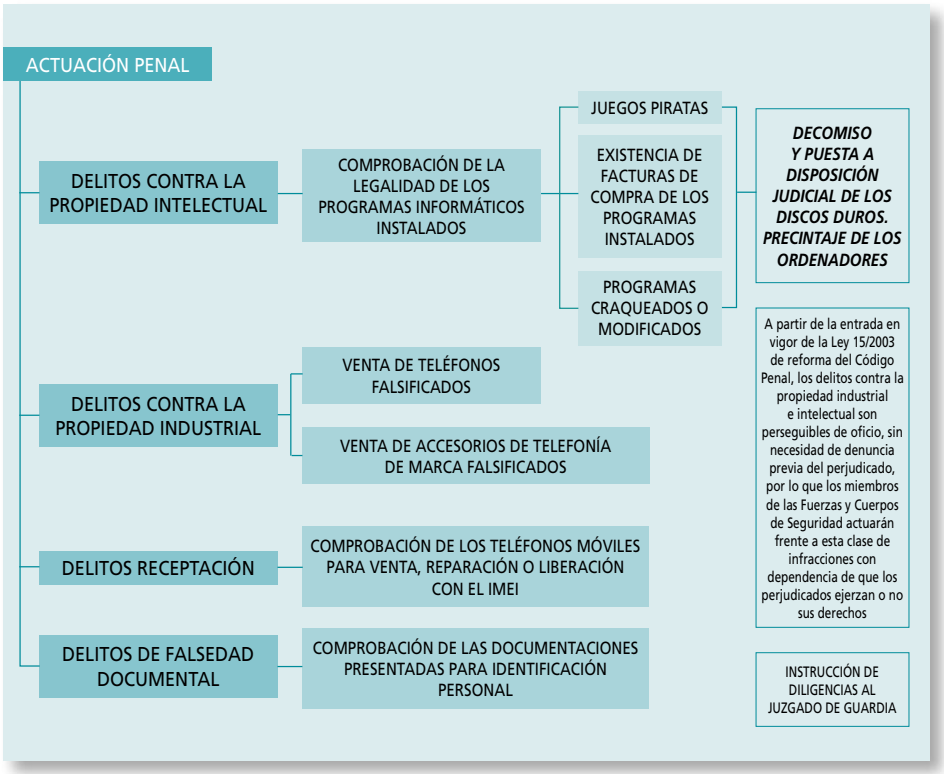
La actividad del Perito Judicial telemático y/o de telecomunicación, se encuentra como en la del resto de los Peritos Judiciales en un limbo jurídico, y existen alguna normativa y legislación que regula esta profesión y que la encontramos en Ley de Enjuiciamiento Civil (L.E.C. 1/2000), que es la que regula los procedimientos judiciales civiles y los medios de prueba, que es al fin y al cabo lo que aporta el perito.

En concreto, en el artículo 299 se enumeran los medios de prueba de que se podrán hacer uso durante el juicio, entre las que se encuentra en el punto 4 el dictamen de peritos. En el artículo 339 se regula la solicitud de designación de peritos, los honorarios de los peritos y en el artículo 340 se fijan las condiciones que habrán de reunir los peritos.

En resumen, la parte de la Ley de Enjuiciamiento Civil que regula la prueba pericial son los artículos 335 hasta el 352. Del mismo modo debemos recalar en la Ley de Enjuiciamiento Criminal, que regula el informe pericial entre sus artículos 456 a 485.

La diferencia entre las leyes de enjuiciamiento civil y criminal es el ámbito de cada una de ellas. Mientras que la ley de enjuiciamiento criminal se dedica a lo que conocemos como derecho penal, es decir su ámbito de acción es el Código Penal, las faltas y delitos que un individuo puede cometer y que, en última instancia, pueden llevarle a prisión, la Ley de Enjuiciamiento Civil, se dedica por el contrario al ámbito civil, o lo que es lo mismo, a aquellos conflictos entre particulares, ya sean personas físicas o jurídicas, que no constituyen ninguna falta o delito pero que sí pueden conllevar responsabilidades de otro tipo, en especial dinerarias.

Esquema con delitos tecnológicos de actuación penal:



¿Se pueden realizar peritajes estando titulado pero sin estar colegiado?

Sí, si el perito es llamado directamente por las partes y se presenta su informe como prueba o si el peritaje es privado (sin intenciones judiciales) en cuyo caso la entidad puede llamar directamente a cualquier persona.

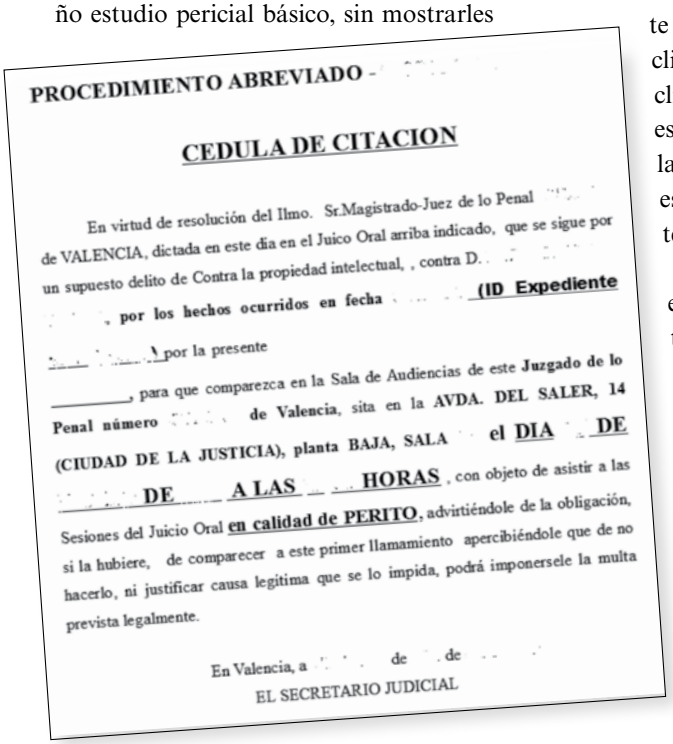
En los peritajes judiciales donde el perito se designe por los Juzgados a partir de la lista aportada por el Colegio Profesional, y también en los peritajes gestionados directamente por el Colegio, es requisito estar colegiado…

Estar colegiado y visar los peritajes nos aporta un seguro de responsabilidad civil que es más que aconsejable.

Aquí os dejamos una citación judicial en calidad de Perito como ejemplo.

EJEMPLO PERITACIÓN DE PARTE: EMPRESA "AAA"

Les mostramos un ejemplo de un pequeño estudio pericial básico, sin mostrarles el informe y quitando todas las partes legales, explicando los pasos dados para el estudio, a modo de ejemplo básico de una pericial telemática.



PROCEDIMIENTO ABREVIADO -

CEDULA DE CITACION

En virtud de resolución del Ilmo. Sr.Magistrado-Juez de lo Penal de VALENCIA, dictada en este dia en el Juico Oral arriba indicado, que se sigue por un supuesto delito de Contra la propiedad intelectual, , contra D. , **por los hechos ocurridos en fecha (ID Expediente** por la presente

, para que comparezca en la Sala de Audiencias de este **Juzgado de lo Penal número** de Valencia, sita en la **AVDA. DEL SALER, 14 (CIUDAD DE LA JUSTICIA), planta BAJA, SALA el DIA DE DE A LAS HORAS**, con objeto de asistir a las Sesiones del Juicio Oral **en calidad de PERITO**, advirtiéndole de la obligación, si la hubiere, de comparecer a este primer llamamiento apercibiéndole que de no hacerlo, ni justificar causa legitima que se lo impida, podrá imponersele la multa prevista legalmente.

En Valencia, a de de

EL SECRETARIO JUDICIAL

Introducción

La empresa "AAA", se puso en contacto con el perito telemático, en este caso yo mismo, para que les realizara un informe pericial de su red telemática, ya que según ellos se les ha acusado de un delito telemático que ellos no realizaron. Las leyes vigentes me obligan a proteger la identidad de mi cliente y de todo el proceso, por lo que he omitido y/o variado datos personales o direcciones.

Hay que decir, que el cliente junto con su abogado me dieron toda la información de la denuncia, donde el denunciante decía que mi cliente le había realizado amenazas e insultos por las redes sociales. En la denuncia venia un informe de Telefónica en el que indicaba que las amenazas e insultos venían efectivamente desde la IP Pública de mi cliente. Lo que indigna a mi cliente es que el denunciante es vecino puerta con puerta de la Clínica de Fisioterapia que es desde donde presuntamente se realizó el delito.

Mi trabajo ha sido el de estudiar la red de datos y los tres ordenadores que existen en la clínica e intentar buscar indicios sobre la demanda que han presentado a mi cliente, indicando, con sus respectivos estudios, que no se puede demostrar que ha sido desde ningún ordenador de la empresa AAA la infracción, ya que como veremos en el informe, poseen una red MUY MAL PROTEGIDA CONTRA INTRUSIONES. Lo que sí es cierto es que la IP Pública que se demanda es la de mi cliente, como yo pude observar en los documentos aportados por la operadora en la denuncia.

Hay que reseñar que en dicha empresa AAA, yo, como perito telemático, manifiesto que no incurro en causa de recusación, según lo regulado en el artículo 124 de la Ley de Enjuiciamiento Civil, ni en tacha según el artículo 343 de la citada Ley. Se detalla esto para indicar que no sabía que nos encontraríamos al estudiar la red y los ordenadores, tanto en cuanto a seguridad, a sistemas operativos, a software antivirus, antitroyanos, etc...

Estudio y desarrollo del informe pericial

Red telemática de la empresa AAA

Para entender muchas cosas del informe pericial que se presentó para este caso se necesitan conocimientos específicos de telemática, pero se deben omitir todos esos aspectos más técnicos para que el juez pueda entenderlo sin casi tener nociones de telemática. Para la redacción de este artículo, y que los lectores puedan tener una visión coherente de la explicación que se realizó en la pericial, se intenta explicar todo lo necesario para que todos (clientes, abogados…) lo pudiesen entender. En definitiva, no esperen ningún artículo técnico, es un artículo mucho más docente. Se redactó lo que sigue:

Para empezar, y de manera simplificada, sin nomenclátor técnico, explicamos el direccionamiento IP y las direcciones MAC que después nos servirán en las conclusiones.

Dirección IP

Una dirección IP es un número que identifica a un ordenador conectado a Internet. Esto no significa que exista una IP por ordenador, un grupo de ordenadores de una misma red puede tener la misma IP. Esta dirección puede cambiar al reconectar, si es así, se denomina una dirección IP dinámica. En caso contrario, se determina como dirección IP fija. En la empresa AAA tenemos IP dinámica Pública asignada por la empresa Telefónica.

Una IP pública es aquella que tenemos en Internet. Sin embargo, la IP privada es la que tenemos en nuestra propia

red local, es decir, desde nuestro dispositivo (router).

En nuestro caso, la empresa AAA no posee IP Fija, por lo que, en el momento de la denuncia la dirección IP Pública era 79.145.40.241, pero a día de hoy es diferente. La IP Privada ha sido y sigue siendo la misma, ya que ésta sí es fija o estática, 192.168.1.1.

Dirección MAC

MAC son las siglas de Media Access Control y se refiere al control de acceso al medio físico. O sea que la dirección MAC es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware: cada tarjeta Ethernet viene de fábrica con un número MAC distinto y único en el mundo.

Windows la menciona como Dirección del adaptador. Esto es lo que finalmente permite las transmisiones de datos entre ordenadores de la red, puesto que cada ordenador es reconocido mediante esa dirección MAC, de forma inequívoca.

Por lo tanto, cada equipo conectado a una red de datos Ethernet, como la que estamos estudiando, posee una dirección MAC única en el mundo. En los datos incluidos por el denunciante, nos aporta identificación de usuarios IP de la empresa Movistar (Telefónica), pero no nos indica la dirección MAC de ningún equipo conectado en dicho router en la fecha indicada, por lo que es IMPOSIBLE saber desde qué ordenador se realizó la conexión denunciada, pero sí queda claro por los informes del operador que fue desde la empresa AAA, ya que la IP Pública es la de ellos. Más adelante explicaremos por qué no se puede demostrar que haya sido realizado desde ningún ordenador de la empresa AAA, por culpa de la conexión WIFI.

La dirección MAC está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (cada pareja se separa de otra mediante dos puntos ":" o mediante guiones "-"). Por ejemplo, una dirección MAC podría ser F0:E1:D2:C3:B4:A5.

Para poder entender el informe, primero tenemos que explicar un poco como funciona su red telemática propia, de ordenadores y de redes de datos.

La red telemática de la empresa AAA es una red muy simple. Tiene un router inalámbrico de la empresa Movistar SA, tres ordenadores (1 fijo y dos portátiles) y una cámara de seguridad, todos ellos conectados a dicha red. Los dos portátiles y el equipo de sobremesa de forma inalámbrica y la cámara con cable de red.

Para entender mejor la red, con IPs y configuraciones les he dejado el siguiente esquema:

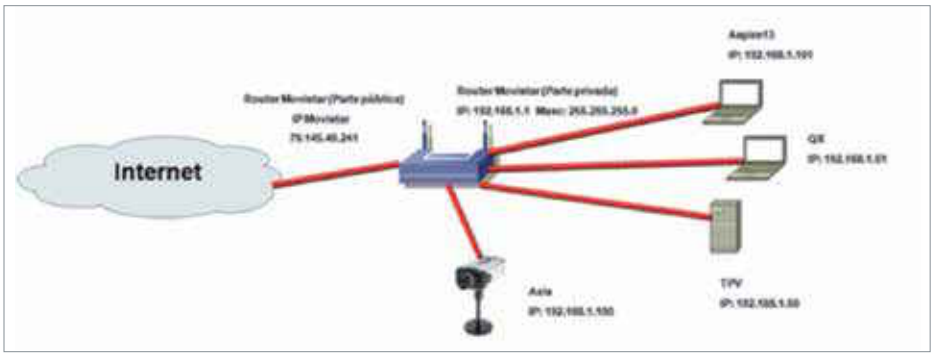


Figura 1. *Red empresa AAA*

Como vemos hay tres equipos, dos portátiles, y uno fijo. También existe una cámara de vigilancia IP conectada a la red, concretamente conectada al Router.

Equipo	Nombre en la red	Dirección IP	Dirección MAC	Características
Router Movistar	Router	192.168.1.1 (IP Privada) 79.145.40.241 (IP Pública el día del posible delito)	00:03:0D:35:1E:AA	Router Marca Comtrend inalámbrico modelo CT-5365 con P/N: 755555557-02222
Portátil	Aspire13	192.168.1.101	00:25:86:EF:89:DD	Equipo portátil modelo Acer Aspire 1310 con procesador AMD Athlon XP 1800, 512Mb de RAM, un disco duro de 20Gb, y sistema Operativo Windows XP Home Edition SP3.
Portátil	QX	192.168.1.51	00:27:19:B8:78:DD	Equipo portátil modelo Fujitsu Siemens Amilo con procesador Intel Pentium M 1,86Mhz, 1Gb de RAM, dos discos duros de 80Gb, y sistema Operativo Windows XP Home Edition SP3.
Sobremesa	TPV	192.168.1.50	00:03:0D:35:1E:AA	Equipo de sobremesa con procesador Celeron E3300 a 2,5Ghz. 2 Gb RAM, 2 discos duros, uno de 150Gb y otro de 100Gb. Sistema Operativo Windows XP Profesional SP3.
Cámara	Axis	192.168.1.100	00:40:8C:9F:02:66	Cámara IP con servidor integrado y marca AXIS.

Tabla 1. *Información equipos empresa AAA*

Después de explicar cómo está estructurada la red de datos o telemática de la empresa AAA, vamos a ver cómo está configurada la red inalámbrica de la empresa, que aquí es donde radica la cuestión del problema.

Red inalámbrica WIFI de la empresa AAA

El router de Telefónica nos da acceso a Internet y a la red de datos interna mediante cable o acceso inalámbrico WIFI.
El propietario de la empresa AAA, decidió dar acceso inalámbrico a sus clientes para el acceso a Internet proporcionando las claves de su acceso WIFI. Él no pensó en los problemas de este acto.
Como vemos en la fotografía tomada, tiene las claves colgadas en la sala de espera. Hay una fotografía para que se ubique el cartel citado, y una fotografía del router donde se puede apreciar que el propietario no cambio las claves del WIFI desde que Telefónica instalo el router. Ahora hablaremos de los problemas que esto puede ocasionar.

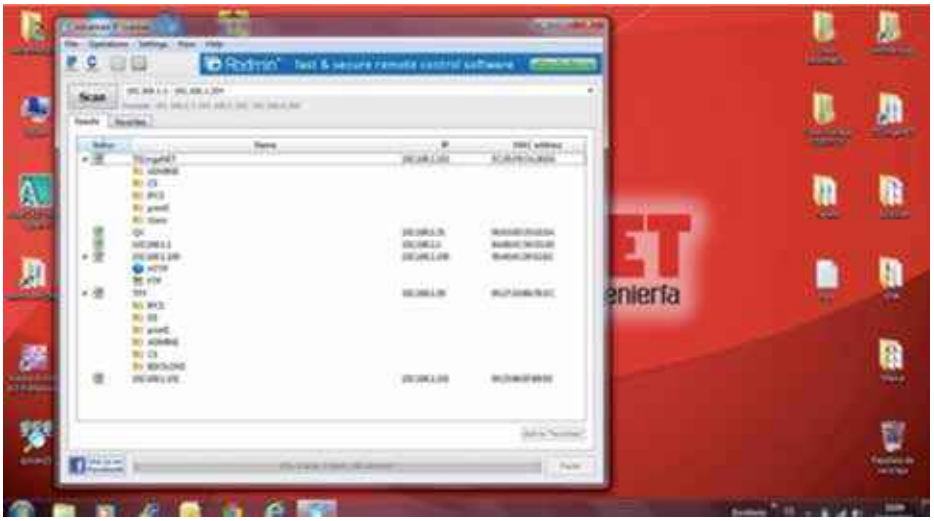
Imagen de la sala de espera con la información WIFI, y foto de la configuración del router

Cuando nos conectamos a una red WIFI como la que estamos estudiando, el ordenador busca la red (en nuestro caso la red posee el nombre WLAN_D1E0). Una vez encontrada le pedimos que se conecte. Si posee contraseña como la red que nos ocupa la colocamos. En ese momento el ordenador y el router empiezan a "hablar" para poder establecer comunicación. El ordenador le envía la clave, y si ésta es correcta el router establece la comunicación asignando una dirección IP al ordenador. Así es la forma que tiene de conectarse un equipo a una red WIFI.

Tres cosas a resaltar que mi cliente no sabía por sus conocimientos limitados de telemática.

La primera es que una vez el equipo posee una red WIFI conectada, el Sistema Operativo Windows, da igual que sea la versión XP, la versión Vista o la versión 7 u 8, cuando encuentra la red se conecta automáticamente, ya que se queda en la memoria cache del ordenador la contraseña. Por eso, si vuelvo otro día a la empresa AAA o tengo cobertura por estar cerca, mi ordenador al encontrar la red WLAN_D1E0, se conectara automáticamente, sin pedirme contraseñas ni nada.

La segunda es que es una imprudencia dejar que los clientes se conecten a una red WIFI como ésta sin proteger los equipos de trabajo de la empresa AAA, ya que al acceder a la red de datos, también puedo acceder a las carpetas compartidas que posean los ordenadores y con conocimientos avanzados de telemática, no solamente a las carpetas compartidas, sino a todos los sistemas. Como vemos en la captura de abajo, donde también está incluido mi ordenador desde donde realice el estudio, vemos las carpetas compartidas de algunos equipos.



Captura de pantalla donde se ve el software Advanced IP Scanner

La tercera es que encima de tener acceso a todo el sistema, también se puede acceder a la configuración del router de Telefónica, ya que como pude comprobar está con las claves por defecto de fábrica y sin proteger, por lo que cualquiera que se conecte a la red puede acceder a la configuración del router. El usuario es 1234 y el password es 1234.

Accediendo al router puedo cambiar toda la información, o redireccionar el tráfico a una dirección IP, o todo lo que uno quiera o sepa hacer.

Resumiendo lo visto hasta el momento en el informe. Ya sabemos lo que es una dirección IP y las que posee la empresa que estamos estudiando. Ya sabemos lo que es una dirección MAC y las que posee cada máquina de las que estamos estudiando. Ya sabemos cómo está configurada la red WIFI para que se conecten los clientes de la empresa. Ya sabemos que teniendo configurada la red WIFI una vez ésta queda configurada por defecto en el equipo. Ya sabemos que la red WIFI no es segura para los datos de la empresa AAA. Ya sabemos que todos los que se conecten a la red WIFI también tiene acceso a la configuración del router. Ahora solo nos falta saber una cosa relacionada con las conexiones WIFI, la cobertura.

Cobertura WIFI de la red WLAN_D1E0

Los routers WIFI poseen una cobertura máxima alcanzable. Yo me propuse estudiar hasta donde llegaba la red WIFI de mi cliente, la WLAN_D1E0. Sin aparatos de medida reseñables, solo con mi equipo portátil desde donde realice la conexión para el estudio, y con una técnica tan básica como ver en el Microsoft Windows si la conexión era excelente, buena o mala, y con un test de velocidad por Internet, como veis en algunas capturas de pantalla, he podido comprobar en el mapa adjunto la cobertura aproximada desde donde se puede conectar un equipo a la red.

Aquí os dejo la captura y foto de la conexión en la recepción de la empresa AAA. He marcado con un círculo rojo los datos que son reseñables, el círculo pequeño es la cobertura de la antena, y el círculo grande es la velocidad a la que llega en cada sitio según la cobertura.

Captura de pantalla de un test de velocidad de Internet y el WIFI

Después de estudiar la cobertura a la que se llega en la calle del establecimiento citado, en el siguiente mapa vemos el mapa de abajo, siendo el círculo rojo la cobertura a la que llega el router WIFI y el cuadrado rojo la empresa aproximadamente.

Cobertura WIFI del router de la empresa AAA

Conclusiones

Como conclusión, si algún cliente se ha conectado a la red WIFI de la empresa AAA, podrá acceder a Internet y a la red de datos interna de la empresa AAA desde todos los lugares indicados, ya que la contraseña se queda almacenada en el equipo y este al encontrar la señal se conecta automáticamente.

Por este motivo, sabiendo que un día en concreto, a una hora determinada ha habido conexiones malintencionadas desde la IP Pública de la empresa AAA, no se puede demostrar que hayan sido los ordenadores de la empresa, nos falta saber desde qué MAC ha sido para poder saber si ha sido desde algún ordenador de la empresa, ya que cualquiera que se haya conectado anteriormente puede volverse a conectar a la red y todo lo que se realice queda registrado la IP Pública de mi cliente, aunque no haya sido el mismo ni los trabajadores de la empresa.

Después de estas investigaciones, intente averiguar si la fecha denunciada se podría acceder a ver que MACs estaban conectadas, pero es imposible ya que el router al reiniciarse pierde dicha información, y se ha reiniciado multitud de veces desde dicha fecha. Vemos una captura de pantalla de como muestra el router la información de los equipos conectados en ese momento.

Captura de pantalla con información de las MACs conectadas al router.

Por lo tanto, la conclusión final es que sabiendo que en la denuncia se ha demostrado por la empresa suministradora de Internet, Telefónica, que la IP Pública ha sido la de mi cliente, no se puede demostrar científicamente desde qué ordenador se ha realizado la conexión, a no ser que Telefónica también posea en su base de datos las direcciones MAC desde donde se realizó dicha conexión.

Aparte de no poderse demostrar tal hecho, hemos demostrado que la red WIFI posee bastante cobertura hacia los domicilios de alrededor, llegando incluso a la dirección del denunciante sin problemas.

También hemos demostrado que una vez conectados a la red WIFI de la empresa, cualquiera dentro de la cobertura puede volverse a conectar automáticamente, y todo lo que se realiza queda registrado en el IP Pública de la empresa AAA; esto es, si alguien entra en el WIFI, entra en Internet, y realiza un robo, Telefónica podrá indicar desde que IP Pública se ha realizado, pero no quien ha sido, ya que no posee la dirección MAC, que es la única que puede demostrar que ha sido un ordenador en concreto.

Por lo tanto, y como conclusión final, no se puede demostrar que un equipo de mi cliente haya accedido a un página web un día y una hora determinada, pero que si se puede acusar a una conexión, en este caso la de la empresa AAA, de haberse conectado un día y una hora en concreto.

Esta pericial no llego a juzgado, ya que la parte denunciante vio que mi informe era claro y que evidentemente no se podía demostrar lo que ellos intentaban, y llegaron a un acuerdo las dos partes antes de entrar a juicio.

BIBLIOGRAFÍA

COGITTCV (Colegio Oficial de Graduados e Ingenieros Técnicos de Telecomunicación de la Comunidad Valenciana)
o http://www.cogittcv.com

COGITT (Colegio Oficial de Graduados e Ingenieros Tecnicos de Telecomunicación)
o http://www.cogitt.com

ANTPJI (Asociación Nacional de Tasadores y Peritos Judiciales Informáticos)
o www.antpji.com

Policía Local de Valencia. Distrito Marítimo
o http://www.policialocalvalencia.es/

Grupo de Delitos Telemáticos de la Guardia Civil.
o https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Colegio Oficial de Detectives Privados de la Comunidad Valenciana
o https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Colegio Notarial Valencia
o http://www.cnotarial-valencia.com/

Colegio Procuradores Valencia
o https://www.icpv.com/

Colegio de Abogados de Valencia
o http://www.icav.es/