UNIVERSIDAD CATOLICA DE SALTA

Tesis para la obtención del Título de Grado de

Licenciada en Criminalística

“Identificación de computadoras, utilizadas para la concreción de delitos informáticos, a partir de su dirección física, en redes de Área Local.”

Autor: Zalazar, Débora Daniela

Director: Ing. Zalazar, Dante Daniel

San Salvador de Jujuy- Argentina 2017

AUTORIDADES

RECTOR

Ing. Rodolfo Gallo Cornejo

VICERECTORA ACADEMICA

Mg. Constanza Diedrich

SECRETARIA GENERAL

Lic. Silvia Álvarez

DECANO DE LA FACULTAD DE CIENCIAS JURIDICAS

Dr. Omar Alberto Carranza

SECRETARIA ACADEMICA

Dra. Virginia Maria Diez Gomez Logarte

JEFE DE CARRERA LICENCIATURA EN CRIMINALISTICA

Lic. Roberto Washinton Gonzalez

DELEGADO RECTORAL- SEDE SAN SALVADOR DE JUJUY

Lic. Sergio Roberto Castanetto

“Identificación de computadoras, utilizadas para la concreción de delitos informáticos, a partir de su dirección física, en redes de Área Local.”

"La privacidad no debe ser una opción,

y no debe ser el precio que aceptamos solo para

conectarnos a Internet"

-Gary Kovacs-

Dedicatoria

A MI FAMILIA

A mis padres, **Dante y Adela**, pilares en mi vida; y a mi pequeña hermana, **Florencia** por haberme formado y preparado para los grandes retos de la vida. Con su forma de ser y educar serán siempre el ejemplo a seguir en el nuevo camino que inicio a recorrer. Les agradezco el apoyo incondicional que me brindaron día a día, inculcándome siempre que con esfuerzo todo es posible.

Atte. Debora Zalazar

Agradecimientos

En este apartado quiero expresar mi gratitud hacia las personas o entidades que hicieron posible el desarrollo del presente trabajo de investigación:

A **IES N°5 "J. E. Tello"**, como también a los alumnos de la carrera Tecnicatura Superior en Seguridad Informática, por su colaboración y ayuda en el paso a paso de la investigación; aportando sus conocimientos y predisposición.

A **Nelson Notario**, que sin sus consultas interpretativas y apoyo hubiera incurrido en diversos errores.

A la Universidad Católica de Salta, en especial al **Lic. Roberto Gonzalez** y al **Lic. Sergio Castanetto**, por el buen trato y gestión que me brindaron; dando siempre soluciones a los inconvenientes presentes en toda investigación.

A mis amigos, en especial **Dana y Daniela**, personas admirables que encontré en el transitar de la vida y que siempre me impulsaron a seguir adelante en mi formación académica, enseñándome siempre a sonreír ante todo.

INDICE GENERAL

1. INTRODUCCION

La necesidad de comunicación, inherente a todo ser humano y que lo destaca como ser social, impulsó y continúa impulsando el desarrollo de múltiples formas para interactuar con sus pares estableciendo relaciones con su entorno que pueden ser de índole laboral, personal o recreativa. Esos entornos, que se encuentran en constante innovación, provocan que las comunicaciones e intercambio de información cambien constantemente.

El cambio más significativo en esta relación de comunicación, es el desarrollo vertiginoso y continuo de la tecnología; lo que estimuló un giro en la vida de las personas al convertirse en permanentes usuarios de las denominadas nuevas tecnologías a partir de la utilización periódica de las computadoras, sin evaluar suficientemente los potenciales riesgos que estas tecnologías pueden contener.

De esta manera el foco de atención de la presente investigación, es la identificación de las computadoras empleadas para cometer delitos informáticos dentro de las redes locales de computadoras, permitiendo posteriormente, llegar a identificar el individuo que ejecutó la maniobra delictiva.

Para lograr este cometido, se utilizara como indicador la “dirección física” de su tarjeta de red complementando la identificación por dirección IP de la computadora ejecutora del delito. La dirección física de una tarjeta de red, también llamada MAC-Address, se la puede definir como un número hexadecimal único grabado en cada tarjeta de red al momento de su fabricación.

Sin embargo, para iniciar el análisis de la mencionada problemática resulta necesario ahondar en sus causas; una de las cuales es el acceso a las nuevas tecnologías y su presencia activa en la vida cotidiana de las personas donde los delitos informáticos pueden, al igual que otros, traducirse en graves daños a las personas como a organizaciones y/o

instituciones. Si bien, se puede decir que el mundo actual se rige por valores monetarios, existe un bien al que muchas veces no se le atribuye el valor que merece: la información.

El hecho de perder parcial o totalmente información privada de las personas o información importante de las empresas, puede significar una pérdida mucho más sustancial que el simple hecho de extraviar una billetera con dinero, por citar un ejemplo.

La característica principal de los delitos informáticos, es que afecta lo que se denomina la identidad "digital" de las personas o instituciones. Este nuevo concepto hace referencia a todo lo que cada persona manifiesta en el espacio digital y el impacto que representa en los demás individuos. (Aparici, 2013)

A partir de lo expresado, todo el planteamiento y desarrollo de la investigación está motivado en el siguiente interrogante: ¿Qué se puede hacer para mejorar la exactitud con la que se identifica una computadora que cometió algún delito?

Si bien, es cierto que este interrogante puede ser respondido por múltiples factores y postulados; el presente trabajo pretende hacer hincapié en el empleo de la dirección MAC –Address como un marcador único que puede servir a la hora de determinar el ordenador desde el cual se perpetuo la acción nociva.

Por ello, la investigación bibliográfica se complementa con el desarrollo de casos simulados de delitos informáticos, cometidos en redes de área local (LAN); donde si bien al inicio de cada uno de ellos, el investigador sabe cuál es la computadora culpable, se desea llegar a la misma a partir del análisis informático de la dirección IP y dirección MAC-Address que esta presenta.

Finalmente, a partir de los datos recolectados con la ejecución de los casos simulados, se desea establecer estadísticamente si este nuevo marcador, la dirección MAC –Address, colabora y/o complementa los procesos de identificación de computadoras que consumaron algún tipo de delito.

CAPITULO I:

DISEÑO DE INVESTIGACION

2. CAPITULO I: DISEÑO DE INVESTIGACION

2.1 Tema

A partir de una extensa búsqueda experimental y bibliográfica con respecto a los grandes "agujeros negros", que aún existen dentro del amplio saber criminalístico; surge la Informática Forense como una de las recientes disciplinas que forman parte de este gran territorio y que avanza al mismo tiempo en que se realizan los nuevo desarrollos del mundo tecnológico en el que estamos inmersos. Sin embargo, con este gran avance también existen grandes riesgos que son los puntos iniciales para los Delitos Informáticos. Por ello, el tema del presente trabajo se traduce en la identificación de computadoras que cometieron algún delito informático, dentro de las redes de área local.

2.2 Planteo del problema de la investigación

La investigación surge de la necesidad que exige toda tarea pericial, en el sentido de la búsqueda imperiosa de la verdad de los hechos que se investigan, a partir del cual se desea reducir el margen de error presente en investigaciones de Delitos Informáticos. Dentro de ellos, el trabajo se centrara en los delitos informáticos cometidos a través de redes de computadoras (más específicamente redes de área local), aplicando una técnica complementaria a la actualmente utilizada al momento de identificar un dispositivo electrónico.

La técnica de identificación que emplea la dirección física (traducción del término en ingles MAC-Address) como indicador de cada computadora tendría gran utilidad en las investigaciones realizadas por Peritos Informáticos o Técnicos en Seguridad Informática, identificando con mayor seguridad la computadora que ha sido el ejecutor o vehículo de un delito informático; en comparación con el método de identificación por

individualización de dirección IP (traducción del termino en ingles IP-Addrees) que se emplea en la actualidad.

2.3 Interrogantes

De esta manera, el único interrogante que se pretende dilucidar será:

¿Cuál de las técnicas de identificación de dispositivos conectados a una red informática produce un menor margen de error en investigaciones realizadas por Peritos Informáticos y/o Técnicos en Seguridad Informática, en la ciudad de San Salvador de Jujuy actualmente?

2.4 Justificación

Con el correr de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida. En la actualidad las empresas pueden desarrollar sus negocios o las personas pueden realizar tareas cotidianas gracias a la presencia de las nuevas tecnologías, las que simplifican y optimizan las cosas.

Esto ha llevado a una dependencia en la cual no todas son ventajas; si nos situamos unos veinte años atrás, podemos imaginar que la perdida de conectividad con Internet o mal funcionamiento de un sistema resultaba solamente algo molesto. Hoy en día, la pérdida de conectividad significa que una empresa o usuario quede prácticamente inoperante.

Por ello, es incuestionable la importancia que día a día adquiere el estudio y el desarrollo de diversas estrategias y/o instrumentos que permitan minimizar o identificar el daño ocasionado a las computadoras, y a la información que estas contienen, a partir de lo que se denomina “Seguridad informática”. La seguridad y la protección de datos serán objetivos fundamentales para esta área, la información pública o privada en muchos casos es invaluable, pero su intangibilidad hace que en ocasiones no sea preservada adecuadamente.

La progresiva informatización de los procesos administrativos y de negocios, el despliegue masivo de redes que permiten poner a disposición de cualquier usuario datos como el desarrollo de nuevos servicios on-line a través de Internet son algunos de los factores que explican la creciente preocupación por mejorar la seguridad en los sistemas de información o en el uso de los servicios de las redes de computadoras.

Al volcar nuestras vidas hacia la tecnología, almacenamos información personal en las redes, desde registros médicos hasta balances de cuenta en sistemas informáticos solo para mencionar algunos ejemplos; y a medida que las organizaciones confían en la tecnología para hacer negocios, establecer comunicaciones y transferir fondos, empiezan a aparecer otras personas, no tan bien intencionadas, que ven en la tecnología una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás. Debido a esto, los datos por robo o pérdida de información crecen a la par de nuestras dependencias tecnológicas, constituyendo lo que se denominan “Delitos Informáticos” que son ni más ni menos, conductas orientadas a causar daños en el hardware o en el software de un sistema.

Si bien, en la actualidad la legislación como las investigaciones que se desarrollan a partir de estos delitos ha avanzado, siguen creciendo, motivando la búsqueda incesante de medios para frenar su accionar o reducir el daño que pudiera ocasionar.

La intención de este tipo de investigación es contribuir a sostener la calidad que debe tener toda prueba pericial al momento de identificar dispositivos que haya sido utilizado para desarrollar conductas ilícitas en las redes, el medio de comunicación y de almacenamiento de datos públicos y personales más utilizado en la actualidad.

2.5 Objetivos

2.5.1 Objetivo General:

Establecer la efectividad de los mecanismos que permiten identificar la dirección física (MAC- Address) única en dispositivos informáticos, con relación a la reducción del margen de error al momento de identificar computadoras relacionadas con delitos informáticos cometidos en redes de área local.

2.5.2 Objetivos Específicos:

- Indagar, utilizar y evaluar la eficacia del proceso de investigación con relación a los delitos informáticos cometidos en redes de computadoras de área local
- Detallar los mecanismos que hacen posible la identificación de la dirección física de una computadora.
- Analizar los programas de computadoras (software) que se implementan actualmente y los que permiten identificar la dirección física de las computadoras estableciendo las distintas ventajas y desventajas que presentan cada uno de ellos.
- Evaluar el grado de eficacia en la reducción del margen de error en las investigaciones realizadas en situaciones testigos simuladas al compararla con las usadas habitualmente en el tipo de accionar.

2.5.3 Interrogantes:

- ¿Cuál es el lineamiento investigativo que se emplea ante la presencia de delitos informáticos cometidos en redes informáticas de área local actualmente?
- ¿Qué mecanismos permiten individualizar la dirección física (MAC- Address) en una computadora?

- ¿Cuáles son los programas (software) forenses permiten la identificación de la dirección física (MAC- Address)?¿Cómo lo hacen?
- ¿Se reduce el margen de error, en este tipo de investigaciones, si se emplea como indicador la dirección física (MAC-Address)?

2.6 Marco Metodológico

La presente investigación se desarrollara encuadrando los procedimientos a realizar dentro del enfoque cualitativo-cuantitativo, respetando el método científico; con alcance exploratorio-correlacional, cuya finalidad será examinar un tema poco estudiado y conocer la relación que existe entre dos o más conceptos dentro del contexto en particular.

2.6.1 Población/universo y Muestra:

La presente investigación se desarrollara con asiento en la ciudad de San Salvador de Jujuy, provincia de Jujuy, República Argentina. A los fines de reducir el ámbito de estudio dentro de las existentes en la citada ciudad, el asiento de la investigación será en el Colegio Comercial N°2 “Malvinas Argentinas” sede de Instituto de Enseñanza Superior (IES N°5) donde se dicta la carrera “Tecnicatura Superior en Informática con orientación al soporte de infraestructuras IT” y con la correspondiente colaboración de los alumnos de la cátedra “Seguridad Informática”.

La información que se va a analizar será la obtenida a partir del desarrollo de situaciones simuladas, durante el año 2016.

La cantidad de computadoras a lo largo y ancho de la cuidad supera a la cantidad de personas en la misma, y si en materia de redes estructuradas se habla, existen otras muchas. Los datos experimentales recabados serán

en base a computadoras que se encuentren inmersas en Redes de Área Local (LAN), a partir de situaciones testigos simuladas dentro de la ciudad de San Salvador de Jujuy, provincia de Jujuy, Argentina.

2.6.2 Unidad de estudio

La unidad de estudio principal de esta investigación son los individuos que emplean las computadoras u ordenadores conectados entre sí, a través de una Red Informática de Área Local, como instrumentos necesarios para la consumación de acciones ilícitas.

2.6.3 Instrumentos y Técnicas postulados

Las técnicas de carácter metodológica que se van a realizar a los fines de esta investigación son:

- Análisis documental: actividad que realizara el investigador tendiente a conocer la situación actual en materia de identificación de computadoras en red.
- Experimental: el relevamiento de los datos se realizara sobre 15 (quince) situaciones testigos simuladas de delitos informáticos cometidos dentro de redes informáticas testigo de área local (LAN), sobre las cuales se empleara el proceso de identificación a través de la individualización de la Dirección IP y la Dirección física MAC- Addreess.
- Análisis de datos: se hará sobre los datos recolectados en las situaciones empíricas, realizando análisis estadístico descriptivo e inferencial con el fin de determinar cuál de las técnicas empleadas produce menor margen de error.

CAPITULO II:

FUNDAMENTOS DE LA INVESTIGACION

3. CAPITULO II: FUNDAMENTOS DE LA INVESTIGACION

3.1 Estado del Arte

A partir de la búsqueda, análisis y evaluación de información bibliográfica sobre la metodología utilizada para la identificación de computadoras; así como de las investigaciones desarrolladas sobre la problemática, se puede destacar el interés evidenciado en este nuevo objeto de estudio, en virtud de su relevancia en las redes informáticas, por las que circula cuantiosa información.

En la actualidad se puede evidenciar la creciente preocupación sobre la información personal que circula en las redes informáticas; que se hace presente a través de diversas publicaciones, tanto en revistas científicas como diarios de amplia difusión. La revista "USERS", considerada como un referente en el área informática, se ocupo del tema con diversas publicaciones.

La misma "USERS" publico un trabajo titulado "Seguridad Informática", desarrollado por Portantier, F en el año 2012, que expone lo siguiente: "… A medida que las personas volcamos nuestras vidas hacia la tecnología, almacenamos información personal, registros médicos y balances de cuenta en sistemas informáticos. Y a medida que las organizaciones confían en la tecnología para hacer negocios, establecer comunicaciones y transferir fondos, empiezan a aparecer otras personas, no tan bien intencionadas, que ven la tecnología como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás. Debido a esto, los daños por robo o pérdida de información crecen a la par de nuestra dependencia tecnológica. Muchos criminales optan por utilizar la tecnología como herramienta, ya sea para cometer nuevas formas de crimen o para complementar las que ya están difundidas." (p.15). Cabe destacar que en el citado trabajo, el autor destaca la importancia que adquiere, en la actualidad, la Seguridad Informática como medio por el cual se puede contrarrestar la

creciente aparición de ilícitos cometidos a través de computadoras; y a la vez, como la civilización misma fue aventurándose al amplio y a veces "turbulento" mundo de la Informática.

Este nuevo entorno, proporciona facilidades en la vida cotidiana, pero también conlleva riesgos. En la edición N°295 de USERS titulada "El fin de la privacidad" (2015) se afirma que: "..Seguramente hoy en día la mayoría de nosotros poseemos un teléfono inteligente, participamos en al menos una o más redes sociales y utilizamos algunos que otros servicios online. También nos animaríamos a decir que a la mayoría de nosotros nos da flojera leer los "famosos" términos y condiciones cuando nos inscribimos en algún servicio, rellenamos varios formularios sin saber a dónde van a parar nuestros datos y no le prestamos mucha atención a los permisos que las aplicaciones móviles nos solicitan."(p.8).

El articulo prosigue destacando que si bien, ninguno de nosotros pretende dejar al descubierto nuestra información personal, al compartir distintos archivos dentro de la red se generan otros datos que se asocian a la información enviada. Estos datos se los conoce como METADATOS (datos dentro de los datos), los cuales podrían traducirse en una importante fuga de información, tanto personal como de una empresa. Con estos datos, señala el artículo, se puede obtener el Nombre del usuario, Sistema operativo, Software en el que se creó el documento compartido, ubicación dentro del disco duro, *Posición Geográfica*, entre otros. Este último punto es el que se relaciona íntimamente con la presente investigación; ya que, tanto dirección IP y dirección MAC son algunos de los elementos que posibilitan el posicionamiento geográfico de un dispositivo.

La identificación de computadoras se considera como algo tangible y sustancial, al igual que la identificación que se realiza sobre personas. Esto es así, porque a partir de la utilización de diversos tipos de mecanismos y métodos, se puede individualizar la computadora que ha sido ejecutora o

vehículo de acciones nocivas, realizadas con el fin de provocar daño en la vida de las personas físicas o jurídicas.

En la Tesis titulada "Vulnerabilidad de las redes TCP/IP y principales mecanismos de seguridad" realizada por Ing. Riffo Gutiérrez (2009), se define el cerrado mundo de las redes informáticas, su estructura, funcionamiento interno y externo, a partir del que realiza un análisis profundo y exhaustivo de los tipos de vacíos o falencias que pueden presentar las redes de computadora de área local; las cuales pueden ser interceptadas por otras personas que pretenden sacar algún provecho. En el capítulo II, establece las distintas deficiencias que presentan las redes analizadas, dentro de las que realiza la aplicación de software varios (como ventana de comandos "CMD", programa "Whois", "SuperScan", etc.), para localizar la dirección IP (IP Address) de los ordenadores que integran la red informática. Obtuvo, con ello, información sobre el servidor, identificando usuarios, personas, direcciones de correo asociadas a la administración, y también una cantidad de puertos abiertos, entre otros tantos datos de interés. El autor concluye su trabajo, enfatizando sobre la importancia de conocer los factores que pueden vulnerar considerablemente a un sistema de redes informáticas; y de la necesidad de tomar recaudos para la protección de las mismas, y de esa manera de toda la información que circula por ese medio.

Asimismo, en relación al tema se encuentra el trabajo titulado "Aplicación Web para encender y apagar computadoras (con tarjetas de red con opción Wake on Lane)" desarrollado por Ing. Luzuriaga Quichimbo (2008), en el que se utiliza en forma conjunta la dirección IP y MAC como medio de identificación de computadoras.

Si bien, el trabajo tiene como objetivo el desarrollo de un software que permite el inicio remoto de computadoras, utiliza para tal fin elementos que se exponer en esta investigación. A través de la tarjeta de red, el autor, identifica la computadora que se desea encender o apagar de forma remota

utilizando la dirección MAC (MAC-Address), la dirección IP o su nombre de Host dentro del protocolo TCP/IP de Internet, considerándose estas en relación a su nivel de confiabilidad.

El programa o software desarrollado, en palabras simples lo explica el autor, envía una señal (paquete de datos) hacia la dirección MAC de una tarjeta de red específica, la que recibe el paquete, lo identifica y envía la carga de voltaje para producir el encendido de la computadora; cumpliendo así el objeto de su tesis.

En la era de la globalización y las telecomunicaciones en la que vivimos, podemos decir que es de interés común el resguardar los datos e información que, otredad se protegía de forma física en archiveros y escritorios; porque al producirse un hecho ilícito contra estos bienes, resulta de vital importancia lograr identificar, con el mayor grado de confiabilidad al agresor; y es justamente lo que se desea definir en este trabajo

3.2 Marco histórico

Se puede afirmar que la necesidad de transmitir información se remonta hacia los inicios de la humanidad. En un primer momento, dicha comunicación se realizó mediante gestos y sonidos, luego con señales de humo o destellos con espejos; con el transcurso de los años y el avance de las tecnologías, la transmisión de mensajes se pudo realizar mediante cables, utilizando código Morse, luego la propia voz por medio del teléfono; desde ese momento la humanidad no ha parado de crear máquinas y métodos para poder transmitir y procesar la información.

Según la bibliografía consultada, la informática, definida como el tratamiento automático de la información, se remonta a la invención de la primera computadora mecánico-programable diseñada por el ingeniero alemán Konrad Zuse entre los años 1936 y 1938 designada con el nombre de “Z1”.

A partir de ese momento, muchos científicos se interesaron por la "ciencia naciente", realizando múltiples estudios y avances; dentro de los cuales se debe destacar, en el marco nacional, el desarrollo de la primer computadora para fines científicos llamada "Clementina" la que presto funciones entre los años 1961 y 1971, en la Universidad de Buenos Aires. De allí en más, el desarrollo de nuevas tecnologías no se detuvo.

De manera semejante a los avances tecnológicos surgieron también avances en el ámbito delictual, estos encontraban una nueva oportunidad para obtener beneficios. Surgen así los denominados Delitos Informáticos y su contrapartida la Informática Forense.

El primer caso conocido, de este tipo de delitos, con sentencia efectiva fue el denominado Caso Irán-Contras (IranGate) en agosto de 1986, concerniente a la venta de armamento militar, realizado por el gobierno de los Estados Unidos al gobierno Iraní. El Tte. Coronel Oliver North fue señalado como el principal gestor del dinero obtenido mediante un entramado dudoso de cuentas bancaras en Suiza. Según los registros, el Coronel, escribió correos electrónicos a los fines de efectivizar la transacción, los cuales borro de su computadora sin advertir que se realizaban copias de respaldo, que tiempo después permitieron recuperar el contenido de los correos.

Otro caso resuelto en el ámbito de la Informática Forense es el caso Guttman en el año 1991. Este, se origina a partir de la localización de una nota sin firmar redactada en computadora e impresa por una impresora a matriz de puntos; la cual se hallo junto al cadáver de la esposa del señor Guttman. Al registrar la computadora del domicilio no se logró encontrar vestigios del documento; no obstante con el transcurso de la investigación, se logró determinar que Guttman tenía una relación extramatrimonial. Al allanar la casa de la tercera en discordia, se encontró una unidad de almacenamiento tipo "disket" seccionado en pequeñas piezas. La

reconstrucción del mismo hizo posible la recuperación de la nota mencionada.

Por último, se menciona como otro antecedente, y quizás el más famoso, el caso Mitnick, en alusión a Kevin Mitnick conocido también por ser el primer hacker de la historia, quien en 1995 fue detenido gracias a un trabajo interdisciplinario entre expertos del FBI y académicos en seguridad informática, luego de tres años de persecución. A Mitnick se lo acuso de diversos delitos electrónicos, dentro de los cuales se le imputó el haber ingresado de forma ilegítima a algunas computadoras y redes más seguras de los Estados Unidos.

Si bien estos son solo algunos de los casos más resonantes, y quizás más rudimentarios, ya se puede observar la interrelación que existe entre la tecnología y los ilícitos. Con el correr del tiempo estos han tomado dimensiones colosales.

La tecnología avanza día a día; lo que exige y exigirá que los expertos y encargados de resguardar los derechos de la población se encuentren en la constante búsqueda de nuevas formas de control y protección de lo que hoy en día es llamada la “Identidad Electrónica o Digital”.

CAPITULO III:

MARCO TEORICO

4. CAPITULO III: MARCO TEORICO

4.1 La Criminalística como ciencia

En la actualidad, y a raíz de la creciente delincuencia en todo el mundo, comenzó a tomar importancia la criminalística como una nueva ciencia, que en otros tiempos se encontraba a la sombra de las ciencias clásica. Sin embargo, sus inicios se pueden remontar a los de la propia humanidad, al ocuparse de indagar sobre las huellas que el ser humano va dejando como evidencia de su accionar.

En la bibliografía consultada, expertos en el área, definen a la criminalística de diversas maneras; entre ellos se mencionan los citados por Juan Héctor Raúl en su obra "Introducción a la Criminalística":

Roberto Albarracín y Julio Fortunato la definen como: *"la aplicación de recursos, métodos y procedimientos suministrados por la ciencia a las investigaciones policiales tendientes a constatar la existencia de los delitos y la identificación de sus autores".*

Díaz de Acevedo dice que: *"Criminalística es el conjunto de conocimientos técnico científicos, ajenos a la ciencia médica, aplicados a la resolución del proceso penal y civil".*

Del Picchia Filho afirma que: *"Criminalística es el conjunto de conocimientos técnicos científicos aplicados a la función judiciaria de investigación criminal y del estudio de la prueba indiciaria constituida por los vestigios materiales de naturaleza no biológica".*

López Rey Arrojo indica que*: "Criminalística es la disciplina auxiliar del Derecho Penal y del proceso Penal que se ocupa del descubrimiento y verificación científica del delito y del delincuente"*.

Gaspar Gaspar la define como: *"la disciplina auxiliar del Derecho Penal que se ocupa del descubrimiento y comprobación científica del delito y del delincuente"*

Carlos Guzmán: *"Criminalística es la profesión y disciplina dirigida al reconocimiento, individualización y evaluación de la evidencia física, mediante la aplicación de las ciencias naturales en cuestiones legales".*

Raúl Enrique Zajaczkowski: *"Criminalística es la disciplina autónoma que concurre al auxilio del proceso judicial utilizando técnicas, procedimientos y métodos brindados por las ciencias auxiliares, que le permiten identificar y esclarecer los distintos indicios que conectan, a través de ellos, al autor con el hecho en sí".*

Sin embargo, en el presente trabajo se adhiere a la definición expresada por el doctor **Moreno González** (2001), que establece a la criminalística como *"…la ciencia que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen del material sensible significativo, relacionado con un presunto hecho delictuoso con el fin de determinar en el auxilio de los órganos encargados de administrar justicia, su existencia o bien reconstruirlo, o bien señalar o precisar la intervención de uno o varios sujetos en el mismo".* La elección se basa en que, esta definición, logra especificar las diversas actividades que permiten cumplir los objetivos de la ciencia Criminalística, que a continuación se detallan.

4.1.1 Objetivos de la Criminalística:

Al igual que las demás ciencias, según Montiel Sosa (2003), la Criminalística posee objetivos claros y específicos que se dividen en dos:

4.1.1.1 Objetivo Material: estudiar las evidencias materiales o indicios que se utilizan y que se producen en la comisión de hechos.

4.1.1.2 Objetivo Formal: es auxiliar, con los resultados de la aplicación científica de sus conocimientos, metodología y tecnología, a los órganos que procuran y administran justicia a efecto de darle elementos probatorios que permitan conocer la verdad técnica e histórica de los hechos que investigan.

4.1.2 Áreas y disciplinas auxiliares

Asimismo, y para poder cumplir su cometido, la Criminalística cuenta con el auxilio de las ciencias clásicas, que aportan los saberes que pudieran requerir algunos casos; como las matemáticas, estadística, física, química, ingenierías, entre otras.

Por otro lado, y debido a la gran variedad y variabilidad de los hechos delictuosos que se presentan en la realidad, la Criminalística, a su vez, se divide en distintas áreas de estudio. Según Allan A. V.:

1. Criminalística de campo: aplica los conocimientos, métodos y técnicas con el objeto de proteger, observar y fijar el lugar de los hechos, así como para coleccionar y suministrar las evidencias materiales asociadas al hecho al laboratorio de criminalística.
2. Balística forense: aplica los conocimientos, métodos y técnicas con el objeto de investigar con sus ramas: interior, exterior y de efectos los fenómenos, formas y mecanismos de hechos originados con armas de fuego cortas y largas.
3. Documentología: aplica los conocimientos, métodos y técnicas con el objeto de estudiar y establecer la autenticidad o falsedad de todo tipo de documentos como escritura cursiva, de molde, mecanografiadas o de imprenta, haciendo probable la identificación de los falsarios.
4. Explosivos e incendios: aplica los conocimientos, métodos y técnicas en la investigación de siniestros producidos por explosivos o

incendios, a fin de localizar cráteres, focos y demás evidencias para determinar sus orígenes, formas y manifestaciones.

5. Fotografía forense: aplica los conocimientos, métodos y técnicas a fin de imprimir y revelar las gráficas necesarias en auxilio de las investigaciones que aplican a todas las disciplinas de la criminalística.
6. Accidentología Vial: aplica los conocimientos, métodos y técnicas a fin de investigar los fenómenos, formas, orígenes y manifestaciones de los siniestros viales; como ser atropellamientos, colisiones entre dos o más vehículos, volcaduras, proyecciones sobre objetos fijos y caídas de personas, todas ellas producidas por vehículos automotores.
7. Sistemas de identificación: aplica los conocimientos, métodos y técnicas a fin de identificar inequívocamente a personas vivas o muertas, putrefactas, descarnadas o quemadas.
8. Técnicas forenses de laboratorio: aplica los conocimientos, métodos y técnicas de las ciencias naturales química, física y biología a fin de realizar los análisis y manejo propio del instrumental científico, para identificar y comparar las evidencias materiales asociadas a hechos presuntamente delictuosos.
9. **Informática Forense**: estudio y análisis de los delitos digitales para los cuales fueron empleados dispositivos tecnológicos como: computadoras, medios electrónicos, tecnologías de la información y la comunicación o Tecnologías de Información; procura preservar e identificar datos que sean válidos dentro de un proceso legal o hecho punible.

4.2 Informática forense: la disciplina a la orden del día

Al momento de definir a esta nueva disciplina investigativa resulta ser una tarea algo compleja. Esto, debido a la unión de disciplinas que presenta en su esencia, por un lado "Informática" y por otro "Forensia". Por ello, y a fin de lograr mayor compresión con respecto a los términos, se analizara uno por uno hasta llegar a un concepto unificado.

En principio, el Diccionario Pericial, define el termino Informática de la siguiente manera: *"Ciencia que estudia el procesamiento de la información, es decir, la adquisición de datos o informaciones a tratar, como se introducen en una computadora, estructura y funcionamiento de estas y obtención de resultados." (*Machado, 1992).

En lo que respecta al término "Forense", Álvaro Gómez Vietes (2007) establece:

"La Ciencia Forense nos proporciona los principios y técnicas que facilitan la investigación de los delitos criminales, mediante la identificación, captura, reconstrucción y análisis de las evidencias." Esta, a su vez, requiere la aplicación del método científico por excelencia, para lograr su cometido y, el mismo autor, continua diciendo: *"…se basa en el "Principio de Transferencia de Locard", según el cual cualquier persona u objeto que entra en la escena del crimen deja un rastro en la escena o en la propia víctima y viceversa, es decir, también se lleva consigo algún rastro de la escena del crimen".*

Ahora bien, si direccionamos el ámbito de las Ciencias Forenses hacia la Informática, se logra obtener una idea vaga de lo que podría significar la Informática Forense; ciencia que se encarga de investigar los delitos realizados a través de computadoras. El mismo Álvaro Gómez Vietes (2007), citando la definición propuesta por el FBI establece que: ***"La Informática Forense se encarga de adquirir, preservar, obtener y***

presentar datos que han sido procesados electrónicamente y guardados en un medio computacional."

De esta manera y para hacer posible las investigaciones que requieren conocimientos, tanto la Informática como la Criminalística, es necesario contar con un equipo interdisciplinario de profesionales capacitados a tal fin y proveerles las herramientas necesarias para desarrollar las distintas etapas del análisis forense informático.

4.2.1 Fundamento

La Informática forense, como disciplina derivada de la Informática y avocada a la tarea investigativa, resulta ser un saber muy reciente.

Si bien existen infinidad de ámbitos informáticos que aún siguen siendo "oscuros", en la actualidad para los peritos especializados en el tema; esta nueva ciencia surge de la cantidad de delitos de índole informático que se empezaron a producir a partir de la década de los 80' con los primeros "virus informáticos" lanzados a las redes.

La denominada "Era Digital o Informática", que comenzó a principios del siglo XX y en la cual aún estamos inmersos, es el periodo de la humanidad que permitió a través de los distintos avances tecnológicos, que van desde los primeros medios de comunicación hasta el desarrollo de la informática e Internet, facilitar en gran medida la vida cotidiana de las personas.

Si bien, esta "ciber-dependencia" se acrecentó mucho más con el desarrollo integro de Internet y las redes informáticas, fue intercediendo cada vez más en el hacer cotidiano. Desde realizar alguna consulta o usarlo como medio de comunicación que interconecta distintas partes del mundo, la vida y las relaciones humanas se fueron viendo cada vez más ligada a un

computador; interpretandolo como recipiente contenedor de información, tanto pública como reservada.

Este es el gran tesoro que circula constantemente en las redes de computadoras y es, a partir de allí, donde empiezan a aparecer los problemas y peligros que son visibles hoy en día.

"…*La progresiva informatización de los procesos administrativos y de negocio, el despliegue de redes privadas de datos y el desarrollo de nuevos servicios on-line a través de Internet son algunos de los factores que explican la creciente preocupación por mejorar la seguridad en los sistemas de información y en el uso de los servicios de las redes de ordenadores…" (*Gómez Vietes, 2007).-

4.2.2 Objetivos de la Informática Forense

Como se planteó anteriormente, esta disciplina representa un gran avance en materia de investigación de delitos; permitiendo llegar hasta la esfera de la información intangible, como lo es el mundo informático.

Presenta tres objetivos principales, según lo plantean Giovanni Zucardi y Juan David Gutiérrez en su publicación "Informática Forense" (2006), a saber:

1) La persecución y procesamiento judicial de los responsables.
2) La compensación de los daños causados por los criminales o intrusos
3) La creación y aplicación de medidas para prevenir casos similares.

4.2.3 Sub- ramas de la Informática Forense

Dentro del amplio espectro que investiga esta ciencia, Giovanni Zucardi (2006), menciona como sub-disciplinas de la Informática Forense a:

- Computación Forense: disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia,

procura descubrir e interpretar la información en los medios informáticos para establecer el hecho y formular las hipótesis relacionadas con el caso.

- **Forensia en redes**: escenario en el cual se requiere comprender la manera como los protocolos, configuraciones e infraestructura, de comunicación se conjugan para dar como resultado un momento específico en el tiempo y lugar. Ello hace que el profesional, entendiendo las operaciones de las redes de computadoras; sea capaz, siguiendo los protocolos y formación criminalística, establecer los rastros, los movimientos y acciones que un intruso ha desarrollado en las redes de computadoras.
- Forensia digital: forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de la justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos.

4.3 Delitos Informáticos: delincuencia del siglo XXI

4.3.1 Definición

Los Delitos Informáticos son la razón de ser y el objeto de estudio principal de la Informática Forense.

En este sentido, al igual que con el termino Informática Forense, para poder llegar a una definición acertada es necesario desglosar la frase; haciendo distinción entre "Delito" e "Informático".

El Derecho tradicional instaura diversas definiciones acerca del tema. El Diccionario Jurídico, desarrollado por el poder judicial del NOA (2015), define delito como la:

"…Acción típica, antijurídica y culpable. Acto tipificado como tal en la ley, contrario al derecho y en el que el agente ha tenido dominio sobre las circunstancias, es decir, que por voluntad no ha desarrollado una conducta diferente…"

Ya teniendo el conocimiento de la definición de informática antes expuesto, se puede unir ambos términos obteniendo como resultado una definición simplificada acerca de lo que representan los Delitos Informáticos: conductas antijurídicas realizadas atreves de medios informáticos. Efectivamente dicha idea planteada no se encuentra tan alejada de la realidad, ya que a los llamados "Delitos Informáticos" se los define como: ***"…cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos"*** (definición propuesta por un Grupo de Expertos de la OCDE en 1993).

4.3.2 Jurisprudencia sobre Delitos Informáticos

La Legislación vigente con respecto a esta temática en la República Argentina, está representada por la Ley Nacional N° 26.388 "Sobre

regulación de Delitos Informáticos", sancionada el 4 de Junio de 2008; por medio de la cual se modificaron distintos artículos del Código Penal Argentino. El Dr. Arocena, Gustavo, en su publicación "Introducción a la Ley Nacional N°26.388" propone como definición la siguiente:

"…El **delito informático o ciberdelito** es el injusto determinado en sus elementos por el **tipo de la ley penal**, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los **sistemas informáticos** como **medio masivo** o teniendo aquellos, en parte o en todo, como su **objeto**, se vinculan con el **tratamiento automático de datos…**"

4.3.3 Tipos de Delitos Informáticos

Al ser el campo de la Informática tan amplio como el espacio mismo, los delitos susceptibles de ser cometidos son también la infinidad misma.

Si nos centramos en la clasificación de los delitos informáticos que son reconocidos por la ONU (Organización de las Naciones Unidas- 2001) se obtiene la siguiente distinción:

1) Fraudes cometidos mediante manipulación de computadoras
    - Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
    - Manipulación de Programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación. Este delito consiste en modificar los programas

existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- Manipulación de los Datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
- Fraude efectuado por Manipulación Informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "salami" o "técnica del salchichón" en la que "rodajas muy finas", apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2) Falsificaciones Informáticas

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: la computadora también puede utilizarse para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos laser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y

los documentos que produce son de tal calidad que solo un experto puede diferenciarlo de los documentos auténticos.

3) Daños o modificaciones de programas o datos computarizados:
   - Sabotaje Informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadoras con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
     - ❖ Virus: serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.
     - ❖ Gusanos: análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir datos pero no puede regenerarse a diferencia del virus.
     - ❖ Bomba lógica o cronológica: exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de los datos en un momento dado a futuro. Ahora bien, al revés de los virus y gusanos, las bombas lógicas son difíciles de detectar antes que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño.
   - Acceso no autorizado a servicios y sistemas informáticos: estos accesos se pueden realizar por distintos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
     - ❖ Piratas informáticos o Hackers: este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones. recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir

deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

- Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Dentro de esta clasificación rudimentaria de los delitos informáticos, los que son de interés, a los fines de la presente investigación, son los que están contemplados dentro de la sección “Acceso no autorizado a servicios y sistemas informáticos”, y dentro de esta los **delitos cometidos dentro de redes computacionales**.

4.4 Investigaciones Criminalísticas- Informáticas

4.4.1 Evidencia Digital

El termino evidencia invariablemente designara a todo elemento material susceptible de ser analizado por personal capacitado, cuyos

resultados pueden constituir pruebas de gran relevancia a la hora de resolver procesos judiciales.

Este término, aplicado a los elementos de orden informático, es lo que denominamos como “evidencia digital”.

Casey (2004) define la evidencia digital como *“cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor”*.

A diferencia de la evidencia documental o tradicional, la evidencia digital o computacional es frágil y fácilmente adulterable. De esta manera, otra característica de dicho material probatorio es la posibilidad de realizar copias no autorizadas de la información que puede contener, poniendo en riesgo la validez e integridad de la misma. Es por esto que los peritos informáticos tienen la obligación de realizar “copias forense” (copia exacta bit a bit de la evidencia recolectada) sobre la que se va a realizar los análisis correspondientes para asi no comprometer la evidencia original recolectada en el lugar de los hechos; como así también sacar de cada evidencia una numeración única que demuestra la integridad e inmutabilidad de la misma denominado HASH.

4.4.1.1 Clasificación de la Evidencia Digital

Si bien, existe tanta diversidad de evidencia digital como tecnología desarrollada en la actualidad; Cano Martínez (2005) en su libro “Evidencia Digital: Contexto, Situación e implicaciones nacionales” clasifica la evidencia en tres categoría:

- Registros generados por computadoras: estos registros son aquellos, que como dicen su nombre son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son

llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que género el registro.

- Registros no generados sino simplemente almacenados por o en computadores: estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras (Word, block de notas, entre otros). En estos registros es importante lograr demostrar la identidad del generador y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.
- Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

4.4.2 Protocolo general de actuación de peritaje ante la justicia a nivel nacional

Si bien, en el marco nacional, no existe un reglamento establecido y unificado con respecto a la elaboración de pericias informáticas, se encontró la confección de un Protocolo de Actuación de Peritajes Informáticos desarrollado originalmente por el Poder Judicial de la Provincia de Neuquén (2015). Este, detalla de forma minuciosa la modalidad de trabajo que se debe realizar para él envió y análisis del material tecnológico correspondiente a un proceso judicial (ver Anexo N°1).

4.4.3. Herramientas de Investigación Forense

Se debe tener en cuenta que, en materia de tecnología, cada nuevo amanecer puede ser el marco para un nuevo descubrimiento y lanzamiento de nuevas técnicas, tanto en el ámbito investigativo como en el delictual. La tecnología es un área de crecimiento desmedido día a día, imposible de delimitar o restringir.

Es por ello que el perito informático debe ser una persona en constante y frecuente investigación de los nuevos "productos" disponibles en el mercado de las redes, ya que con esa misma rapidez, los ciberdelincuentes pueden encontrar nuevas formas de producir las acciones nocivas que desean.

El uso de la herramienta adecuada va a posibilitar un pronto esclarecimiento de los ilícitos debido a, según Lopez et. al. (2002):

- La gran cantidad de datos que se pueden almacenar en un computador en la actualidad; sin estas herramientas la búsqueda de las mismas sería muy tediosa y poco eficiente.
- La variedad de formatos de archivos. Las herramientas de recolección de evidencia ayuda a la identificación de los diferentes tipos de archivos que se recuperan, facilitando de la misma manera el análisis de los datos.
- La necesidad de recopilar información de una manera exacta. Las herramientas asisten en la recuperación de la evidencia digital sin alterarla o borrarla del disco duro.
- La necesidad de verificar que la copia es exacta. Las herramientas de recolección de evidencias pueden obtener un HASH de la imagen del disco para verificar que la copia es exacta bit a bit al momento del análisis forense, esto sería imposible de realizar de forma manual.

- Limitaciones de tiempo para analizar toda la información. Las herramientas forenses agilizan el proceso de análisis permitiendo búsqueda de palabras claves dentro de un gran conjunto de datos, entre otras características que hacen que el proceso investigativo sea más rápido.
- Facilidad para borrar archivos de computadoras. Las herramientas de recolección de evidencia asisten en la recuperación de archivos y/o directorios borrados en el sistema.

4.4.4 Tipos de herramientas

Una clasificación primaria que se puede realizar, atento al aspecto económico, distingue las herramientas en:

- Herramientas Comerciales: existen herramientas comerciales no gratuitas desarrolladas por empresas privadas que solicitan el pago de una licencia (mensual o anual) para poder utilizar el software en pericias judiciales.
- Herramientas de Código Abierto: también denominadas “Open Source”, son las de uso gratuito y se pueden descargar libremente desde las páginas de sus correspondientes autores o miembros del proyecto.

Las ultimas mencionadas son las más empleadas a lo hora de realizar el análisis de datos de una evidencia digital. Si bien las herramientas comerciales pueden tener mayor cantidad de prestaciones, las herramientas Open Source abarcan un amplio espectro de funciones, con un alto grado de exactitud y confiabilidad; como así también, la posibilidad de saber el funcionamiento interno del programa.

4.5 Redes de computadoras

4.5.1 Concepto

En la actualidad, las redes informáticas son el mayor medio de almacenamiento y transmisión de información entre computadoras de todo el mundo; permitiendo la intercomunicación instantánea entre computadoras cercanas o entre países alejados, que antiguamente se hubiese traducido en tiempos mucho más prolongados.

Matías Katz (2013), en su libro titulado "Redes y Seguridad", se refiere al tema de la siguiente manera:

"…A fines prácticos, una red no es más que un conjunto de componentes de hardware, conectados físicamente mediante cables u ondas, y configurados de una manera homogénea y sincronizada, que permiten establecer comunicaciones entre sí".

4.5.2 Tipos de redes

Existen distintos tipos de redes informáticas en la actualidad y cada una de ellas presenta diversas características. Según la amplitud de cobertura, en el mismo libro Matías Katz (2013) las clasifica en:

4.5.2.1 Redes Cableadas

- **LAN**: (Local Área Network, red de área local) constituye el tipo de redes que se utilizan cuando se desea interconectar un entorno local limitado y no muy abarcativo.
  Se usan comúnmente para conectar espacios privados, ya sea un hogar o una organización en donde las comunicaciones establecidas permanecen en el perímetro interno que se desea interconectar.
- MAN: (Metropolitan Área Network, red de área metropolitana) muy relacionadas con las anteriores y su principal diferencia es

únicamente el hecho de poseer un área de cobertura geográfica significativamente mayor.

Son utilizadas para interconectar diferentes edificios o complejos que se encuentren físicamente cercanos. En síntesis, una red MAN constituye un conjunto de redes LAN interconectadas.

- WAN: (Wide Área Network, red de área amplia) son redes de gran amplitud, generalmente utilizadas para conectar sitios geográficos significativamente alejados, por ejemplo, continentes apartados por océanos.

  Es el tipo de red utilizado para interconectar a nuestro planeta por completo, permitiéndonos comunicarnos con nuestros pares a miles de kilómetros de distancia en cuestión de segundos. La red WAN más popular es Internet, que nos permite acceder a contenido publicado en cualquier parte del mundo, instantáneamente.

4.5.2.2 Redes Inalámbricas

- WPAN: (Wireless Personal Área Network) es una red inalámbrica de cobertura más bien personal, mínima, y está basada en tecnologías de transferencia de información inalámbrica mediante ondas de corto alcance. En esta categoría se puede encontrar RFID (Identificación por Radio Frecuencia), IR (Radiación Infrarroja) y Bluetooth.
- **WLAN**: (Wireless Local Área Network) representan la norma más popular, ya que es la que se utiliza normalmente en las populares redes Wi-Fi, mediante la cual establecemos las comunicaciones inalámbricas en hogares y en empresas, y en la cual podemos conectar cualquier dispositivo, ya sea una computadora, una impresora, un televisor o un teléfono celular

a una red LAN con la posible salida a Internet sin el uso de ningún cable.

- WMAN: (Wireless Metropolitan Área Network) comprende un área de cobertura extensa, de índices kilométricos en la cual cualquier dispositivo que esté conectado, en cualquier parte de la cobertura de la antena principal que emita las ondas y que centralice las comunicaciones, tendrá acceso a los recursos que estén disponibles en dicha red.
- WWAN: (Wireless Wide Área Network) están formadas por emisores generalmente satelitales mediante los cuales se logra cubrir un rango de señal absoluto en espacios geográficos grandes.

En un ambiente donde hay más de un computador, conectarlos en una red es la manera más económica y eficaz de distribuir y compartir adecuadamente los recursos (datos o información en distintos formatos). Es por eso que la poblacion está interesada en las redes de computadores.

Además programas, equipos e informacion están disponibles para cualquier computadora dentro de la red sin importar donde se encuentren, afirmando lo que dice al respecto Jorge Eloy Luzuriaga Quichimbo (2008) : *"El hecho de que un usuario este a 1000 Km. de distancia de sus datos no deberá impedirle usar sus datos como si fuesen locales".*

4.5.3 Redes LAN

Como ya se expresó, las redes de tipo LAN son redes que poseen una extensión dimensional reducida, que puede ir desde algunos metros hasta unos pocos kilómetros, siempre teniendo en cuenta que se considera como una Red de Área Local. Resulta importante destacar que, por esta última condición, es exactamente sobre este tipo de redes que se van a realizar las situaciones simuladas tendientes a identificar e individualizar a

una computadora; ya que, trabajar con redes de más alto calibre se traduciría en años y años de investigación.

Toranso (2004), en su publicación "Redes de Área Local" establece su funcionalidad diciendo:

"…*Se usan para conectar computadoras personales o estaciones de trabajo, con objetos de compartir recursos e intercambiar información…*"

En términos generales, la red LAN puede desarrollarse empleando tecnología de difusión mediante cable sencillo al que están conectados todas las computadoras que participan en la misma. Sin embargo, las redes más empleadas en la actualidad, debido al gran avance en materia tecnologíca, son las que emplean medios inalámbricos para efectivizar sus conexiones y las redes LAN no se quedan atrás. De esta manera se obtienen las redes "Wireless Local Área Network" o WLAN de las que se habló anteriormente.

4.5.3.1 Componentes de una Red LAN

Si vemos las redes computacionales como maquinas que fueron creadas con un fin determinado, resultan aún más sencillos de entender. Para que el fin que se propuso pueda realizarse, cada una de las partes que integran la misma, deben cumplir su función específica.

De esta manera, si lo que se desea es compartir recursos e información dentro de un grupo reducido de computadoras, Alvarez y Monzalvez (2008) afirma que los componentes principales que integraran la red son:

- Computadoras: denominadas "Hosts" en el entorno, son las que inician y procesan la información proveniente de sus pares.
- Concentrador: denominado "Hub", es un dispositivo inteligente encargado de conectar entre si los equipos y retransmitir la

información que recibe desde cualquiera de ellos a todos los demás, actualmente en desuso.

- Conmutador: denominado "Switch" cuya tarea es entregar los datos de acuerdo a la dirección de destino.
- Enrutador: denominado "Router", interconecta trozos o redes enteras entre sí, decidiendo la mejor ruta para el envió de paquetes de datos a través de la red.

4.5.4 Protocolos de Red

Jorge Eloy Luzuriaga Quichimbo (2008), en su tesis titulada "Aplicación web para encender y apagar computadoras (con tarjeta de red con opción Wake on Lane) define como protocolos de red: *"… el conjunto de reglas, normas, convenciones y procedimientos que especifican el intercambio de datos u órdenes durante la comunicación entre los dispositivos que forman parte de una red.*"

Estos protocolos regulan la conexión, la comunicación y la transferencia de datos entre dos sistemas. Dentro de ellos existen dos modelos principales: el modelo OSI (en inglés, Open System Interconnection) y el modelo TCP/IP que se desarrolló sobre las bases sentadas del modelo anterior; siendo este último el aplicado actualmente.

4.5.4.1 Modelo TCP/IP

*"Este modelo es la base del Internet que sirve para interconectar equipos computacionales que utilizan diferentes sistemas operativos, teléfonos del tipo IP y todo dispositivo que tenga una Tarjeta de Red, ya sea de forma alámbrica, inalámbrica, de área extensa o de área local". (*Riffo Gutiérrez, 2009).

El modelo TCP/IP se desarrolló en el año 1972 por el Departamento de Defensa de los Estados Unidos como una simplificación del modelo OSI.

Este, forma parte de un protocolo DARPA (sigla en inglés de Agencia del Departamento de Defensa de los Estados Unidos) cuyo objetivo es proporcionar una trasmisión segura de “paquetes de datos” (bloques en que se divide la información para ser enviada) en las distintas redes computacionales.

Adquiere su nombre a partir de las iniciales de los protocolos que lo componen, Protocolo de Control de Transferencia (TCP) y el Protocolo de Internet (IP):

- Protocolo de Control de Transmisión (TCP): este protocolo permite a las aplicaciones ejecutarse transparentemente sobre diferentes redes conectadas.
- Protocolo de Internet (IP): permite el desarrollo y transporte de *datagramas* (paquetes de datos).

4.5.4.1.1 Capas del Modelo TCP/IP

Con relación a la arquitectura, es decir, como se encuentra compuesto el modelo TCP/IP, surgen cuatro etapas o “capas” principales; pudiendo diferenciarse del Modelo OSI que, si bien, legaba al mismo resultado estaba constituido en 7 capas. Las capas del modelo TCP/IP son:

1) Capa de Red: o de acceso a la red, específica la forma en la que los datos deben enrutarse y transmitirse hacia una red específica destino. Por norma general, está formado por una red LAN o WAN homogénea.
2) Capa de Internet: maneja la comunicación de una maquina a otra, confiriendo unidad a todos los miembros de la red, independientemente del medio por el cual ingresan a la red. El

direccionamiento y la asignación de direcciones a los paquetes de datos constituye su principal función.

3) Capa de Transporte: regula el flujo de la información que circula por la red, proporcionando una comunicación confiable y asegurando que los datos lleguen sin errores a destino. Para hacer esto debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel; donde a cada paquete de datos se le añade información incluyendo códigos que identifican que programa de aplicación envía y que programa debe recibir.
4) Capa de Aplicación: es la capa que se encuentra en la parte superior del modelo TCP/IP, que contiene a su vez las aplicaciones de la red que permite la comunicación mediante las capas inferiores.

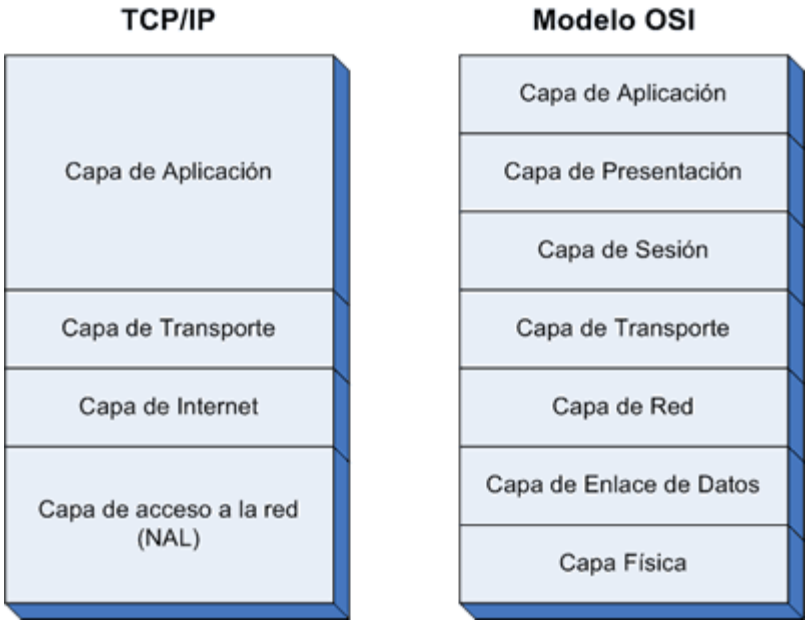


Figura N° 1 - Modelo OSI y modelo TCP/IP

4.5.4.1.2 Familia de protocolos Modelo TCP/IP

Dentro de cada una de las capas que se desarrollaron con anterioridad, para hacer posible el funcionamiento efectivo de la red, trabajan arduamente un conjunto de protocolos con tareas específicas. Es en este punto donde podemos empezar a apreciar los términos "IP" y "Tarjeta de red" en profundidad, temas claves en el desarrollo de la presente investigación.

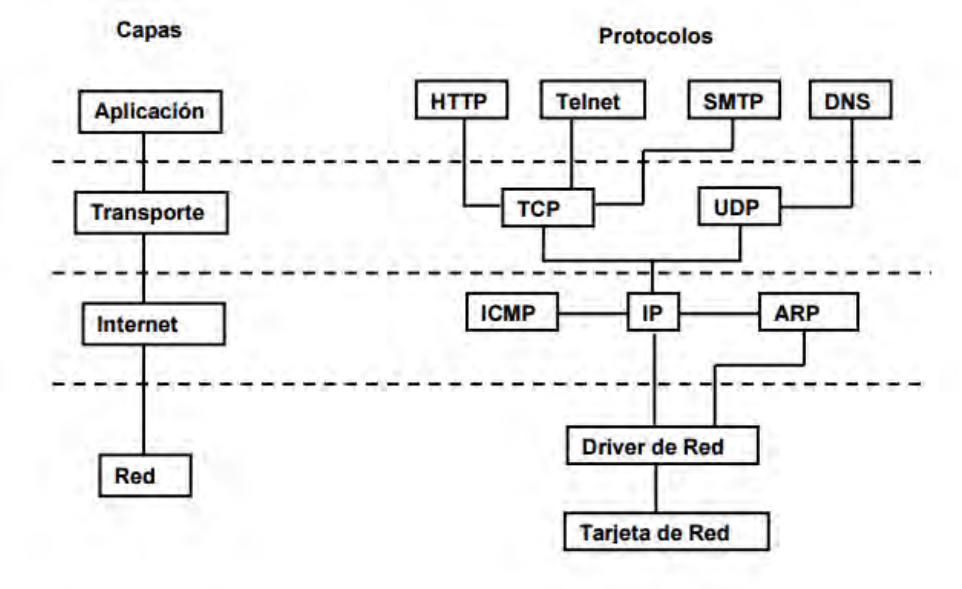


Figura N° 2– Capas y Protocolos del Modelo TCP/IP. (Riffo Gutierrez, 2009)

A continuación se detallaran las funciones principales de los protocolos de cada una de las capas del Modelo en cuestión:

- Capa de acceso a la Red:
  - Tarjeta de Red: o tarjeta de interfaz de red, es un Hardware (componente físico de la computadora) que hace posible la comunicación entre 2 o más equipos, pudiendo ser para conexiones alámbricas o inalámbricas. Su función primordial es la de preparar, enviar y controlar los datos de la red

- Driver de Red: es el Software (componente intangible de la computadora) que permite la interacción del Hardware (Tarjeta de Red) y el sistema operativo interno de la computadora.

- Capa de Internet:
  - **Protocolo ARP:** Protocolo de Resolución de Dirección (ARP) es una de las bases más importantes de este trabajo, ya que permite que se conozca la dirección física de la Tarjeta de Red por medio de una dirección IP.
  - **Protocolo IP:** Protocolo de Internet (IP) es otra de los cimientos de este trabajo, que se más adelante se desarrollara en profundidad.
  - Protocolo ICMP: Protocolo de Control de Mensajes de Internet (ICMP) se encarga de hacer un control de flujo de paquetes de datos que circulan por la red, tratando de localizar posibles errores y situaciones anormales que puedan surgir en el envió o recepción de información.
- Capa de Transporte:
  - Protocolo UDP: Protocolo de Datagramas de Usuarios (UDP) permite crear una interfaz en las aplicaciones IP existentes.
  - Protocolo TCP: Protocolo de Control de Transmisión (TCP) el cual garantiza que los datos serán entregados en sus destinos sin errores y en el orden en el cual fueron enviados.
- Capa de Aplicación:
  - Protocolo HTTP: Protocolo de Transferencia de Hyper Texto (HTTP) permitir las transferencia de archivos de lenguaje de marcación de Hyper Texto (HTML) entre el navegador y un servidor web. Este protocolo se encarga

que una página web pueda proyectar los elementos del texto, imágenes, enlaces, inserciones multimedia, etc.

- Protocolo Telnet: Protocolo de Comunicaciones de red (Telnet) es un protocolo que permite conectar terminales y aplicación en Internet.
- Protocolo SMTP: Protocolo Simple de Transferencia de Correo (SMTP) permite la transferencia en línea de correos desde un servidor a otro.
- DNS: Servidor de Dominios (DNS) de nombres que permite traducir el nombre de un dominio determinado a dirección IP. En esencia, es una base de datos donde se encuentran relacionados los dominios de Internet y su dirección IP, así cuando un usuario necesita llegar a una Pagina X el servidor traduce la orden a la dirección IP de la Página.

4.5.4.2 Protocolo IP

Como ya se explicó, tanto el protocolo TCP y el protocolo IP se encuentra íntimamente relacionado entre sí; posibilitando la comunicación entre computadoras, tanto cercanas como lejanas.

El termino Protocolo IP se puede definir como: *"… El IP es un protocolo de interconexión de red orientada a la emisión y recepción de datagramas".* (Ordina et. al., 2004)

4.5.4.2.1 Direcciones IP

En el libro "Redes de Computadoras" de autores varios, se define a las direcciones como:

"…Las direcciones IP son únicas para cada máquina. Para ser precisos, cada dirección es única para cada una de las interfaces de red IP de cada máquina." (Ordina et. al., 2004)

La dirección IP está representada mediante un número de 32 bits (la palabra “bit” es definida como unidad mínima de información) expresada en números decimales, dividiendo los 32 bits en 4 octetos, separados por un punto, cada octeto puede estar comprendido entre 0 y 255.

Actualmente existen dos versiones de este protocolo, la versión 4 (IPv4) y la versión 6 (IPv6). IPv4 es la que actualmente se encuentra en uso y todos los dispositivos de red están configurados para funcionar con esta versión.

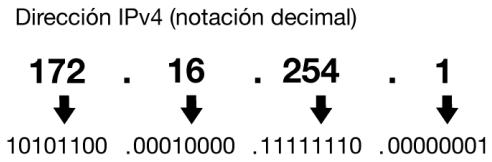


Figura N°3 – Direccion IP

4.5.4.2.2 IP fija y dinámica

Existen dos tipos de direcciones IP en la actualidad, distinción que posibilita el planteo de la presente investigación. Cuando un dispositivo se conecta a una red de tipo TCP/IP puede obtener:

- IP Fija: dirección IP que no varía con cambios o desconexión de red. Dicho dispositivo siempre va a ser reconocido con la dirección IP que haya sido asignada por el usuario o por el proveedor de Internet.

  Las IP fijas actualmente en el mercado de acceso a Internet tienen un costo adicional mensual. Esto permite al usuario crear páginas web, correos, entre otras; teniendo cada página su dirección IP fija.
- IP dinámica: si bien, la que se mencionó anteriormente es de importancia para la localización de páginas web; la IP dinámica es

de uso general para todos los dispositivos conectados a una red; que ademas no posee costo alguno. Consiste en una dirección IP asignada por un programa denominado DHCP (Dynamic Host Configuration Protocol) que permite a, tanto router como switch poder otorgar las direcciones IP correspondientes a cada uno de los dispositivos que se encuentran conectados a la red en tiempo real.

Cuando nos referimos a ciberdelincuencia, y específicamente a delincuentes en red; es lógico afirmar que lo que desean es no ser identificados y poder cometer los ilícitos de forma impune. Sería absurdo suponer que dichos delincuentes podrían contar con el servicio de IP fija, porque esto facilitaría su individualización y consiguiente ubicación.

De forma general, los ciberdelincuentes van a emplear direcciones IP dinámicas, las cuales van a cambiar cada vez que el usuario reconecta por cualquier causa su dispositivo a la red; como así también, existen delincuentes más especializados en el área informática que utilizan distintos programas o softwares que les permite cambiar su dirección IP repetidas veces en un periodo corto de tiempo.

4.5.4.2.3 Clases de direcciones IP

Para poder reconocer el tamaño y el tipo de red con la cual se está trabajando, basta con visualizar en cada computadora la dirección IP que es direccionada. De esta manera las direcciones IP según el rango numérico y la cantidad de computadoras que agrupe en una red, pueden dividirse en:

- Clase A: corresponden a las redes que pueden direccionar hasta 16.777.214 máquinas cada una. El rango va:

  1.0.0.0 – 127.255.255.255

- Clase B: permiten direccionar 65.53 máquinas cada una.

  128.0.0.0- 191.255.255.255

- **Clase C**: permiten direccionar 254 máquinas, correspondiente a redes LAN.

  192.0.0.0- 223.255.255.255.

4.6 Identificación de computadoras conectadas a una red

Si bien, la era de la modernización posee en su mayoría ventajas para todas las personas que tienen la imperiosa necesidad de comunicarse, como se resaltó en el presente trabajo, existen personas que ven en esta una gran puerta de acceso hacia nuevas formas de cometer delitos. Es ante estas situaciones que los profesionales en el ámbito deben llegar a poder identificar con el menor margen de error a la/s computadora/s implicadas en el accionar delictivo.

4.6.1 Indicadores para la identificación

Referente al tema, Jorge Eloy Luzuriaga Quichimbo (2008) en su trabajo académico afirma:

"*Un computador conectado a una red, puede ser identificado mediante:*

- *su dirección MAC*
- *su dirección IP, o mediante*
- *su Nombre de Host o alias."*

4.6.1.1 Dirección MAC (Media Access Control Address)

La dirección física de la tarjeta de red o dirección MAC es un identificador hexadecimal de 48 bits de longitud que se corresponde de

forma única con una tarjeta o interfaz de red. Este índice es el más seguro de los nombrados debido a que es único para cada dispositivo que posea una tarjeta de red.

Cada dispositivo tiene su propia dirección MAC determinada y configurada por el fabricante y el IEEE (Estándares de los Ingenieros Eléctricos y Electrónicos). Se expresa utilizando 12 dígitos hexadecimales. Los primeros 6 dígitos (de la izquierda) identifican a la empresa o institución fabricante de la interfaz o tarjeta de red y los últimos 6 dígitos (de la derecha) representan el número de serie único de la interfaz.

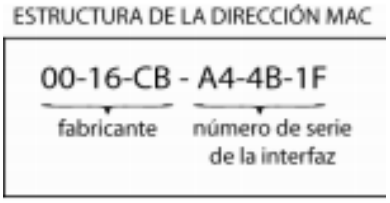


Figura N°4 – Direccion MAC - Address

4.6.1.2 Dirección IP (IP Address)

Detallada en capítulos anteriores, se define a la dirección IP como número que permite identificar la interfaz de un dispositivo, en nuestro caso nos permite identificar mediante números un computador conectado a la red, de manera lógica y jerárquica.

Se puede afirmar que la identificación por este tipo de indicador presenta cierta debilidad, si en materia de Derecho se refiere; ya que, como afirma Barbini (2015):

"…Además debe tenerse presente, que el IP identifica al usuario-cliente con una numeración especifica desde el momento que se conecta a la red, el cual no será modificado en la medida que esa conexión se prolongue en el tiempo, sin que existan interrupciones, suspensiones y/o bajas del servicio acordado con el proveedor de Internet. De darse alguno de

estos supuestos, cuando el usuario-cliente efectué una nueva conexión a la red, se le asignara un numero IP distinto del anterior, circunstancia que dificulta aún más la ubicación en tiempo y forma del sitio de donde se efectuó la conexión."

4.6.1.3 Nombre de Equipo (Hostname)

Otra de las formas de identificar a un computador dentro de la red es por el nombre que le ha asignado el administrador de la misma, debe ser único (no pueden estar conectados a la red dos computadores con el mismo nombre) y es totalmente informal.

Este indicador es el comúnmente utilizado en redes pequeñas, ya que no requiere conocimientos específicos de identificación; análogamente a la individualización que se realiza sobre las personas a partir del nombre civil que es otorgado por sus progenitores.

4.6.2 Herramientas informáticas empleadas

En la actualidad existe una amplia gama de software y herramientas básicas que permita poder conocer tanto las Direcciones IP y Direcciones MAC, al momento de realizar investigaciones informáticas-forenses sobre delitos en redes.

4.6.2.1 Ventana de Comandos de sistema operativo (Windows)

Una de las herramientas básicas para poder conocer esta información es utilizar la ventana de comandos de la propia computadora, empleando comandos especiales a este fin. Los más utilizados y efectivos son los comandos: "ipconfig /all", "ipconfig", "ping", "tracert" y "getmac" (el uso de estos comandos se realiza bajo la ejecución de CMD en la ventana INICIO de la computadora).

Empleando el comando “ipconfig /all” antes mencionado, se puede observar la dirección IP que presenta la computadora que se está empleando asociada a su Dirección física o dirección MAC; como se aprecia en la siguiente figura.

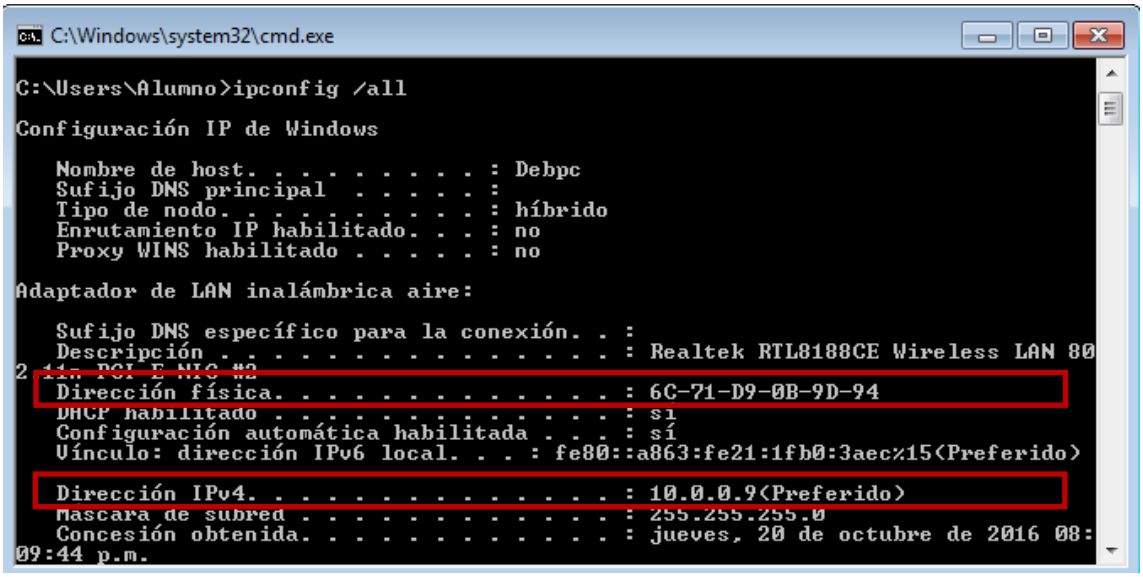


Figura N° 5 – Comando “ipconfig /all”

4.6.2.2 Herramientas específicas

En este punto se encuentran englobados todos los sofisticados softwares que fueron desarrollados para poder obtener la información requerida, tanto direcciones IP como direcciones MAC asociadas de otros computadores. Entre estos, los más útiles y que serán empleados en la presente investigación son los siguientes:

4.6.2.2.1 Advanced IP Scanner

Herramienta de exploración de redes fácil de utilizar, rápida y gratuita. Es un Escáner de red fiable para analizar redes LAN. El programa escanea todos los dispositivos de red, encontrando y sincronizando direcciones IP y MAC.

Otorga acceso a las carpetas compartidas, le proporciona control remoto de las computadoras (mediante RDP y Radmin) e incluso puede apagar las computadoras de manera remota. Es fácil de usar y se ejecuta como una edición portátil, como se puede observar en la siguiente imagen.

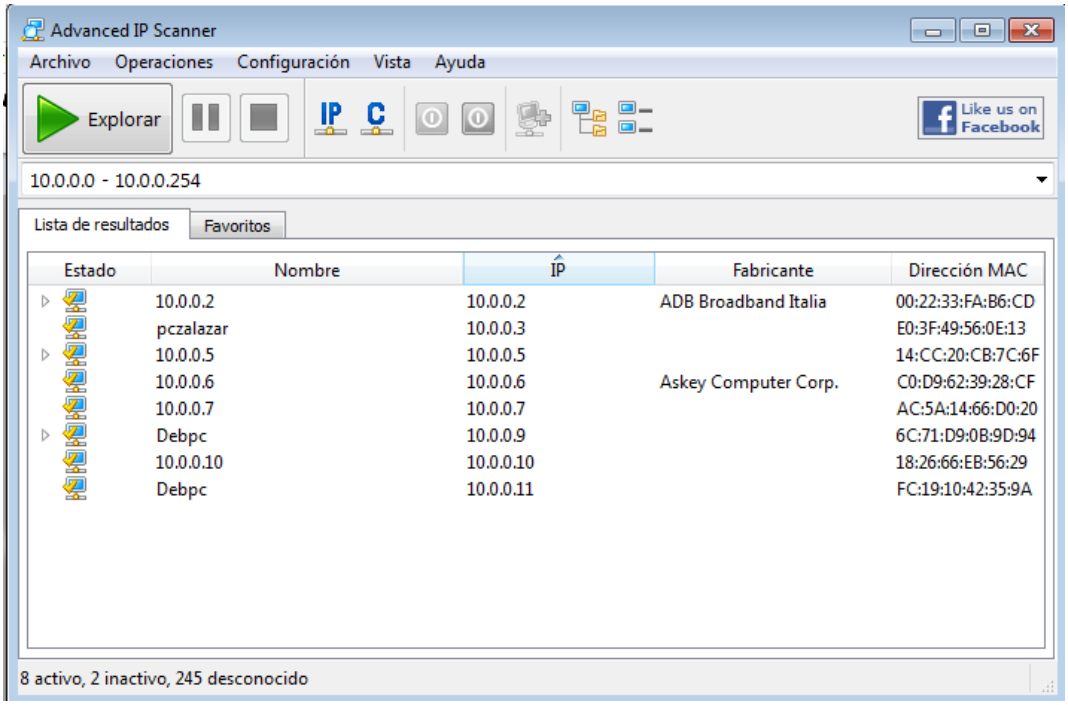


Figura N° 6 – Programa Advanced IP Scanner

4.6.2.1.2 Wireshark

Es una herramienta multiplataforma utilizada para realizar análisis sobre paquetes de red en tiempo real. La utilización de esta herramienta puede parecer compleja en un principio, pero es de gran utilidad una vez conocida su interfaz y su forma de operar. Existen diferentes usos para los cuales puede aplicarse Wireshark como detectar mensajes maliciosos, monitoreo de redes, entre otros.

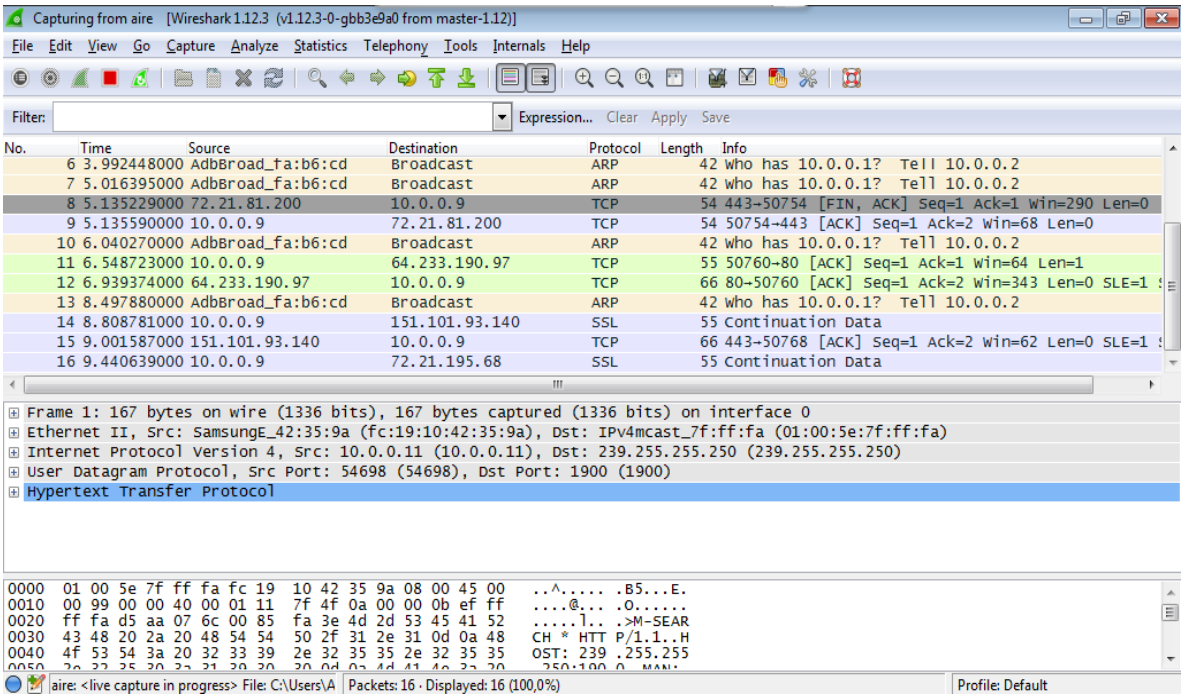


Figura N° 7 – Interfaz del programa Wireshark

Este programa es reconocido a nivel informático como un programa “Sniffer” (termino que se le asigna a las aplicaciones especializadas que permiten capturar los paquetes de datos que viajan por una red); donde, entre otras cosas, permite conocer que direcciones IP se encuentran en intercomunicación en tiempo real; función que será empleada como indicador en las situaciones simuladas que se realizaran a posteriori.

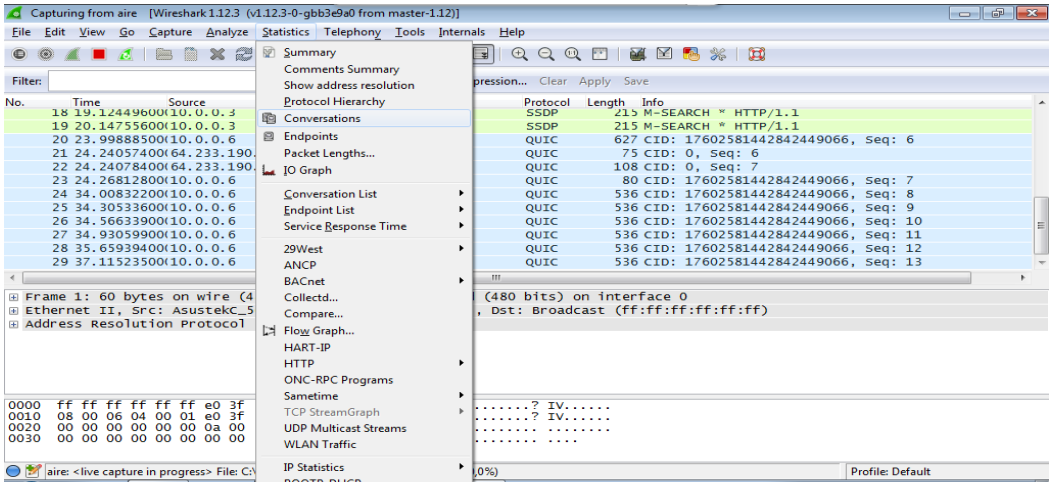


Figura N° 8 – Ingreso a la viñeta “Conversations” del programa Wireshark

Al hacer clic en la opción “Conversations” se abrirá automáticamente una segunda ventana, donde a partir de distintas viñetas permite conocer la conversación que existe entre direcciones IP.

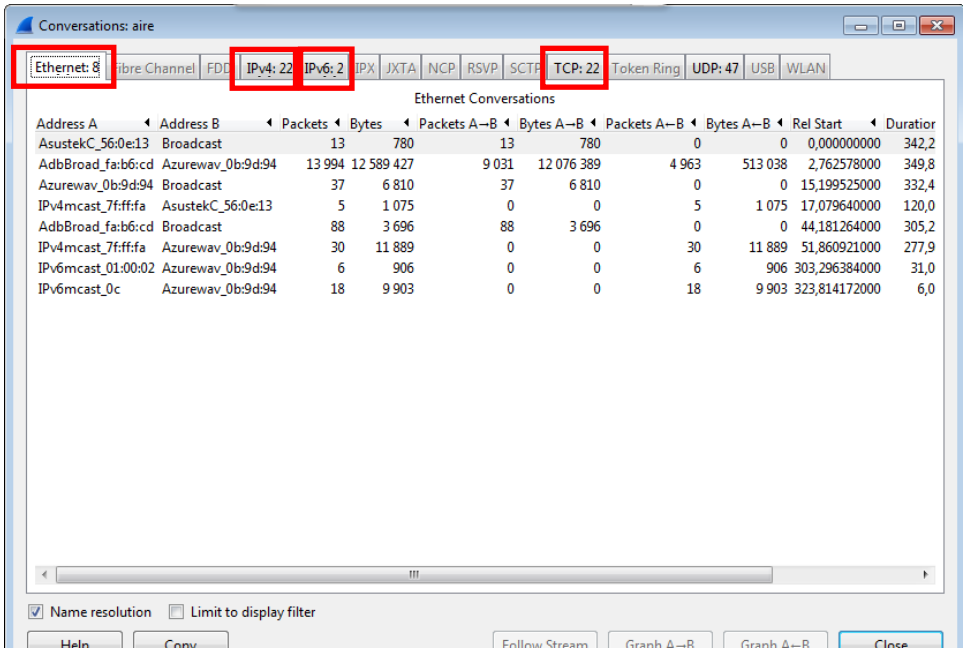


Figura N° 9 – Ventana “Conversations” del programa Wireshark

CAPITULO IV:

DESARROLLO

5. CAPITULO IV: DESARROLLO

Complementando los saberes incorporados a partir de la revisión teórica y bibliográfica, se procedió a la toma de datos empíricos en el campo, que se obtuvieron a partir de la ejecución de situaciones simuladas de delitos informáticos producidas en redes de computadoras de área local (LAN).

A los fines de la investigación, se estableció como caso hipotético la denuncia de supuestas amenazas dirigidas hacia una computadora perteneciente a una misma red. En otros términos, se propuso la situación hipotética en la que existe una computadora, dentro de una empresa X, que envía recurrentemente material de carácter extorsivo hacia la computadora ubicada en la oficina del gerente de la empresa.

Las simulaciones pretenden identificar la computadora vehículo de la acción extorsiva, considerando la dirección física (MAC- Address) conjuntamente con la dirección IP.

5.1 Redes de trabajo

Para la realización de las situaciones simuladas, se seleccionaron cuatro (4) redes de área local ubicadas en la ciudad de San Salvador de Jujuy; Ellas son:

- Red Inalambrica "*Tecinfo*": situado en barrio Ciudad de Nieva, específicamente en el Colegio Comercial N°2 "Armada Argentina" sede de Instituto de Enseñanza Superior (IES N°5)
- Red inalámbrica "*Cockie*": situado en barrio Alto Comedero de la cuidad capital.
- Red inalámbrica "*ALVAREZ WIFI*": situado en barrio Gorriti de la cuidad capital.

- Red inalámbrica: "*ZyXEL*": situado en barrio Alto Comedero, exactamente en el Colegio Secundario N° 1 "Crucero Gral. Belgrano".

5.2 Esquema de Casos simulados

El desarrollo de cada caso simulado en particular se realizó en base a los lineamientos del siguiente esquema metodológico:

1) Establecer conexión a una red de área local con un rango de IP clase C (192.168.0.X).
2) Realizar relevamiento en tiempo real de los dispositivos electrónicos conectados a dicha red con el software **Advanced IP Scanner**.
3) Ejecutar el software **Wireshark**, con el fin de monitorear los paquetes de datos que circulan en la red y las comunicaciones que se efectúan con la computadora "VictimaPC".
4) Localizar la dirección IP de la cual proviene el material extorsivo y relacionarlo con su dirección MAC.
5) Realizar la desconexión de la computadora emisora, del contenido dudoso, y luego, transcurrido un lapso temporal variable restablecer una nueva conexión.
6) Repetir lo expuesto en los puntos 2) y 3)
7) Identificar la IP de la computadora sospechada, estableciendo relación con su dirección MAC.
8) Realizar análisis comparativo de la dirección IP y la dirección MAC, que presentaba dicha computadora en el primer momento, antes de la desconexión, con la vigente en el segundo momento.

En necesario aclarar que, todos los casos desarrollados a continuación fueron realizados en tiempo real. Es decir; teniendo como premisa que la comisión del hecho delictivo está siendo ejecutado en el

mismo momento en el que el investigador está analizando el tráfico circundante en la red de estudio.

5.3 Descripción de casos simulados

Se realizaron quince (15) casos simulados distribuidos en las redes mencionadas en el apartado 5.1; los que se desarrollaron entre los meses de Noviembre y Diciembre del año 2016, a razón de dos (2) casos por día de trabajo. De cada uno de los casos simulados, se tomaron las correspondientes capturas de pantalla como evidencias de todo lo realizado y obtenido, pero a fines de simplificación se destacarán a continuación los aspectos relevantes; pudiendo encontrar el registro completo de cada uno de los casos simulados en el Anexo N°2 titulado "Registro de Casos Simulados":

Caso N°1:

El día 17 de Noviembre del 2016 a horas 19:55 p.m. se realizó la conexión a la red Tecinfo de la computadora de nombre "VictimaPC" (Anexo N° 2: Captura de pantalla N° 1.1 a 1.10).

Seguidamente, se ejecutó el programa Advanced IP Scanner, el que realizó un relevamiento en tiempo real, de todos los dispositivos que se encontraban conectados a la red. Dicho análisis, arrojó como resultado que en la presente red se encontraban 24 dispositivos activos, 1 dispositivo inactivo y 226 dispositivos desconocidos (ejemplos impresoras, celulares, etcétera). Cabe destacar, además, que se obtuvo la dirección IP y la dirección MAC correspondiente a "VictimaPC", de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.135	6C71D90B9D94

Posteriormente, se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento, arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente: 192.168.0.120

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de la siguiente manera:

Host - Nombre	IP	MAC -Address
profdanteZ	192.168.0.120	6C71D901BDAF

Como se estableció en el capitulado teórico, al producirse la desconexión de cualquier dispositivo a la red y con posterioridad provocar una nueva conexión, el Router encargado de la red puede otorgar una dirección IP distinta de la anterior; posibilitando la impunidad del acto ilícito realizado. De esta manera se realiza la desconexión del dispositivo "profdanteZ" y posteriormente una nueva conexión.

Al realizar otro relevamiento, se observa que el hosts "profdanteZ" se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora "VictimaPC" se obtiene la siguiente dirección IP: 192.168.0.133.

Como último paso metodológico se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes, luego de haberse producido la desconexión y reconexión del dispositivo; obteniendo el presente resultado:

Se observa, que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora

Caso N°2:

El día 17 de Noviembre del año 2016, a horas 21:11 p.m. se realizó la conexión a la red Tecinfo de la computadora de nombre "VictimaPC" (Anexo N° 2: Captura de pantalla N° 2.1 a 2.7).

A continuación, se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 32 dispositivos activos, 10 dispositivo inactivo y 212 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a "VictimaPC", de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.135	6C71D90B9D94

Posteriormente, se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.118

Sobre el relevamiento realizado, se localiza dicha dirección IP de la siguiente manera:

Host - Nombre	IP	MAC -Address
PC05-PC	192.168.0.118	90F652162D96

Seguidamente se produjo la desconexión del dispositivo “PC05-PC” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “PC05-PC” se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.120

A continuación, se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento, y las obtenidas luego de haberse producido la desconexión y reconexión del dispositivo, alcanzando el presente resultado:

Se observa, que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°3:

El día 21 de Noviembre del año 2016, a horas 19:21 p.m. se realizó la conexión a la red “Cockie” de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 3.1 a 3.6).

A continuación, se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban

conectados a la red, arrojando como resultado que en la presente red se encontraban 7 dispositivos activos, 30 dispositivo inactivo y 118 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.105	6C71D90B9D94

Posteriormente, se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.109

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
ManuGonza	192.168.0.109	B8030550D656

Seguidamente, se produjo la desconexión del dispositivo “ManuGonza” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “ManuGonza” se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.112

A continuación se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:

Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para este dispositivo.

Caso N°4:

El día 21 de Noviembre del año 2016, a horas 19:39 p.m. se realizó la conexión a la red “Cockie” de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 4.1 a 4.7).

A continuación, se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 5 dispositivos activos, 30 dispositivo inactivo y 120 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.105	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.103

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
danielaPC	192.168.0.103	34DE1A309657

Sin embargo, y debido a las inclemencias climáticas acaecían en la jornada, se produjo una baja en el suministro eléctrico; produciendo el cese de las funciones del Router, encargado de la red, y el consecuente reinicio a sus labores, luego de transcurrido un lapso temporal de aproximadamente una (1) hora.

Al realizar un nuevo relevamiento, al restablecerse el suministro eléctrico, se observa que tanto el hosts “danielaPC” como “VictimaPC”, se encuentran asociados a otras direcciones IP distintas de las atribuidas en un primer momento, siendo estas, las siguientes:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.116	6C71D90B9D94
danielaPC	192.168.0.117	34DE1A309657

Al entablar una nueva conexión directa con la computadora “VictimaPC”, por parte de la computadora “danielaPC”, se observa la siguiente dirección IP: 192.168.0. 117

A continuación, se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las obtenidas luego de haberse producido la desconexión y reconexión del dispositivo, brindando el presente resultado:

Se puede observar, que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°5:

El día 22 de Noviembre del año 2016, a horas 21:31 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts "VictimaPC" (Anexo N° 2: Captura de pantalla N° 5.1 a 5.6).

A continuación, se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 29 dispositivos activos, 21 dispositivo inactivo y 105 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a "VictimaPC", de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.180	6C71D90B9D94

Posteriormente, se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo

comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.183

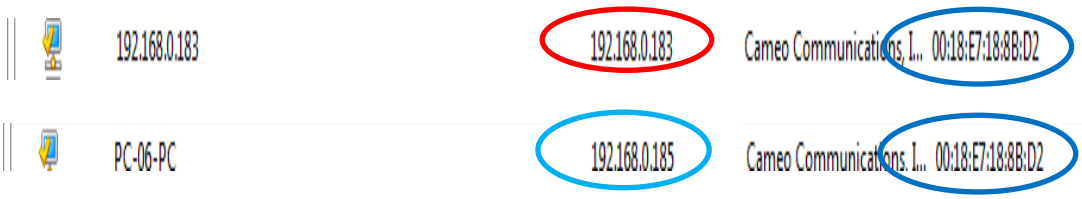
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de la siguiente manera:

Host - Nombre	IP	MAC -Address
192.168.0.183	192.168.0.183	0018E7188BD2

Seguidamente, se produjo la desconexión del dispositivo “192.168.0.183” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que ni el hosts ni la dirección IP “192.168.0.183” se localiza dentro del registro. A partir de un cotejo primario sobre la dirección MAC que presentaba con anterioridad, con respecto a las demás presentes en el relevamiento; se localiza que la dirección MAC 0018E7188BD2 se encuentra asociada al hosts “PC-06-PC” con dirección IP distinta a la anterior y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.185

A continuación, se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°6:

El día 22 de Noviembre del año 2016, a horas 21:47 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 6.1 a 6.6).

A continuación, se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 27 dispositivos activos, 23 dispositivo inactivo y 105 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.180	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.147

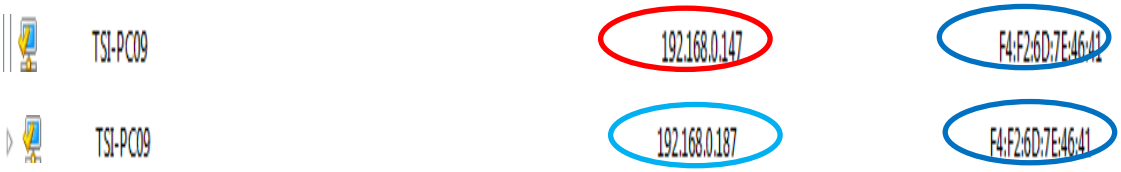
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
TSI-PC09	192.168.0.147	F4F26D7E4641

Seguidamente se produjo la desconexión del dispositivo “TSI-PC09” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “TSI-PC09” se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.187

A continuación se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°7:

El día 23 de Noviembre del año 2016, a horas 18:14 p.m. se realizó la conexión a la red ALVAREZ WIFI de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 7.1 a 7.7).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 3 dispositivos activos, 47 dispositivo inactivo y 105 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.100	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.101

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
HpMini-PC	192.168.0.101	54271EEACAEB

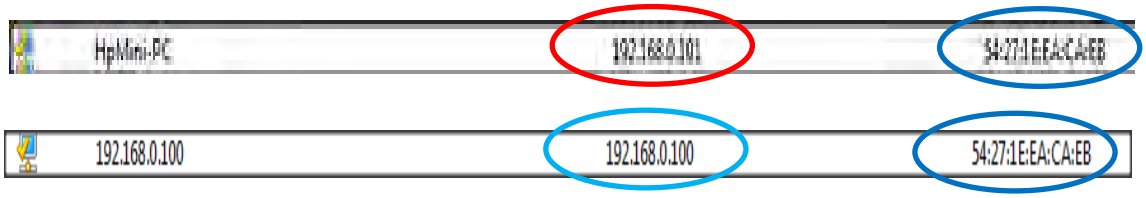
Debido a las inclemencias climáticas que acaecían el día que se realizó el presente caso, se produjo una baja en el suministro eléctrico; produciendo el cese de las funciones del Router encargado de la red y el consecuente reinicio a sus labores transcurrido un lapso temporal de aproximadamente 10 minutos.

Al realizar un nuevo relevamiento, luego de restablecido el suministro eléctrico se observa que tanto el hosts “HpMini-PC” como “VictimaPC” se encuentran asociados a otras dirección IP distintas de las atribuidas en un primer momento, y en el caso de “HpMini-PC” ha habido cambio de hosts; siendo:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.104	6C71D90B9D94
192.168.0.100	192.168.0.100	54271EEACAEB

Al entablar una nueva conexión directa con la computadora “VictimaPC” por parte de la computadora “192.168.0.100” se observa la siguiente dirección IP: 192.168.0.100

A continuación se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°8:

El día 23 de Noviembre del año 2016, a horas 19:45 p.m. se realizó la conexión a la red ALVAREZ WIFI de la computadora de hosts "VictimaPC" (Anexo N° 2: Captura de pantalla N° 8.1 a 8.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 3 dispositivos activos, 46 dispositivo inactivo y 106 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a "VictimaPC", de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.105	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.103

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
TECINF-PC	192.168.0.103	00IF3C5144F7

Seguidamente se produjo la desconexión del dispositivo “TECINF-PC” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “TECINF-PC” se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.103

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:

No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°9:

El día 24 de Noviembre del año 2016, a horas 19:34 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 9.1 a 9.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban

conectados a la red, arrojando como resultado que en la presente red se encontraban 34 dispositivos activos, 20 dispositivo inactivo y 101 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.137	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.116

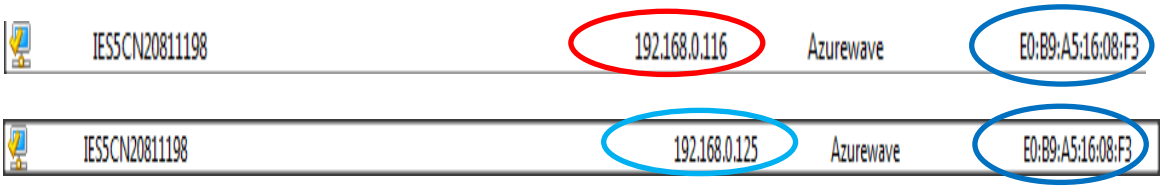
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
IESSN20811198	192.168.0.118	E0B9A51608F3

Seguidamente se produjo la desconexión del dispositivo “IESSN20811198” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “IESSN20811198” se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.125

A continuación se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

Caso N°10:

El día 24 de Noviembre del año 2016, a horas 20:24 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 10.1 a 10.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 32 dispositivos activos, 17 dispositivo inactivo y 106 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.137	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.109

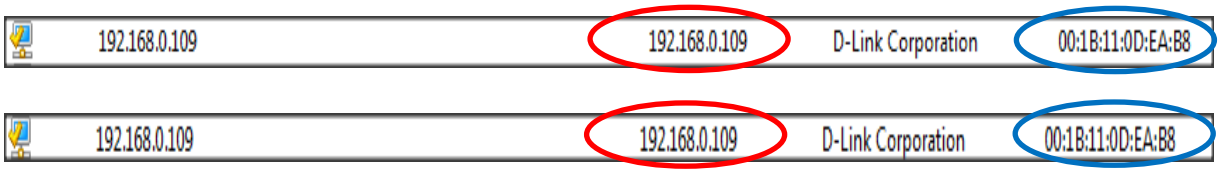
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
192.168.0.109	192.168.0.109	001B110DEAB8

Seguidamente se produjo la desconexión del dispositivo “192.168.0.109” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “192.168.0.109” se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.109

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°11:

El día 25 de Noviembre del año 2016, a horas 20:15 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 11.1 a 11.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 18 dispositivos activos, 32 dispositivo inactivo y 105 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.135	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.134

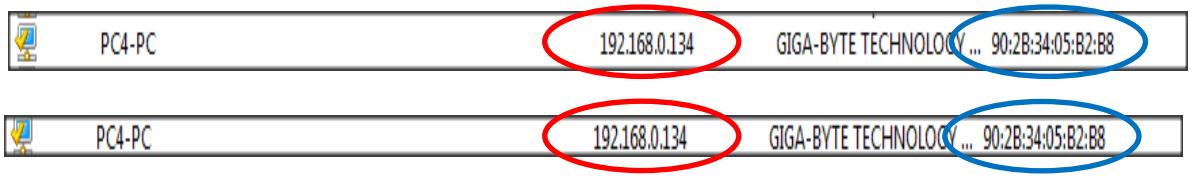
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
PC4-PC	192.168.0.134	902B3405B2B8

Seguidamente se produjo la desconexión del dispositivo “PC4-PC” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “PC4-PC” se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.134

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°12:

El día 25 de Noviembre del año 2016, a horas 20:48 p.m. se realizó la conexión a la red Tecinfo de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 12.1 a 12.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 18 dispositivos activos, 27 dispositivo inactivo y 110 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a "VictimaPC", de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.101	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.132

Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
PC-03-PC	192.168.0.132	002522C00235

Seguidamente se produjo la desconexión del dispositivo "PC-03-PC" y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts "PC-03-PC" se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora "VictimaPC" se obtiene la siguiente dirección IP: 192.168.0.132

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:

No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°13:

El día 3 de Diciembre del año 2016, a horas 21:57 p.m. se realizó la conexión a la red ZyXEL de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 13.1 a 13.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 12 dispositivos activos, 34 dispositivo inactivo y 109 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.110	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.109

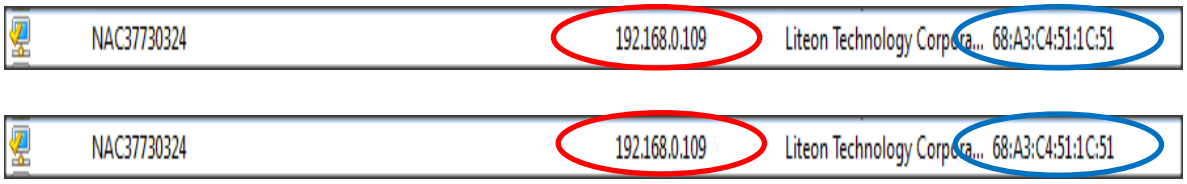
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
NAC37730324	192.168.0.109	68A3C4511C51

Seguidamente se produjo la desconexión del dispositivo “NAC37730324” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “NAC37730324” se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.109

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°14:

El día 3 de Diciembre del año 2016, a horas 10:57 a.m. se realizó la conexión a la red ZyXEL de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 14.1 a 14.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban conectados a la red, arrojando como resultado que en la presente red se encontraban 11 dispositivos activos, 33 dispositivo inactivo y 111 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.115	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.114

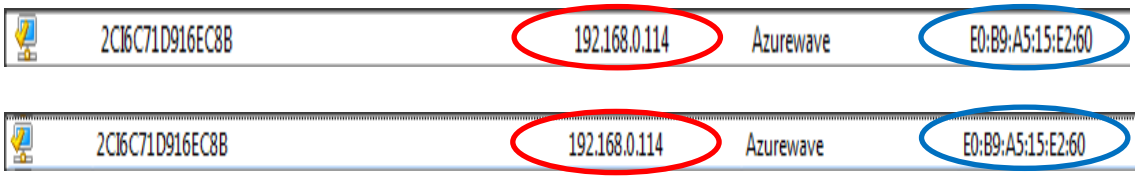
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
2CI6C71D916EC8B	192.168.0.114	E0B9A515E260

Seguidamente se produjo la desconexión del dispositivo “2CI6C71D916EC8B” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “2CI6C71D916EC8B” se encuentra asociado a la misma dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.114

Esto se hace visible, al realizar el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y luego de la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



No se ha producido cambio alguno en la dirección IP ni en la dirección MAC, pudiendo aplicar la identificación por dirección IP con la cual se procede en este tipo de ilícitos.

Caso N°15:

El día 3 de Diciembre del año 2016, a horas 11:39 a.m. se realizó la conexión a la red ZyXEL de la computadora de hosts “VictimaPC” (Anexo N° 2: Captura de pantalla N° 15.1 a 15.6).

A continuación se ejecutó el programa Advanced IP Scanner, realizando el relevamiento de los dispositivos que se encontraban

conectados a la red, arrojando como resultado que en la presente red se encontraban 4 dispositivos activos, 39 dispositivo inactivo y 112 dispositivos desconocidos. Donde se obtuvo la dirección IP y la dirección MAC correspondiente a “VictimaPC”, de la siguiente manera:

Host - Nombre	IP	MAC -Address
VictimaPC	192.168.0.115	6C71D90B9D94

Posteriormente se ejecutó el programa Wireshark en busca de determinar la dirección IP de la computadora emisora del material extorsivo. Este procedimiento arrojo como resultado que la dirección IP que entablo comunicación directa con la computadora VictimaPC es la siguiente:

192.168.0.117

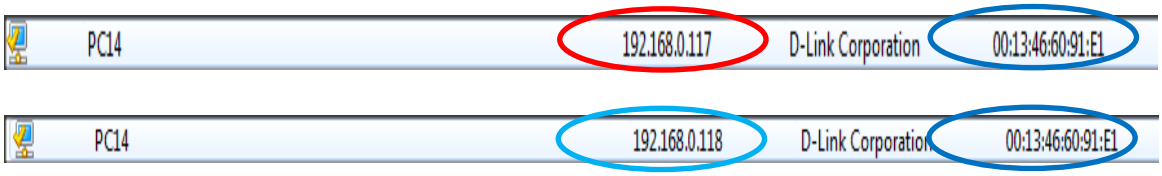
Sobre el relevamiento realizado anteriormente se localiza dicha dirección IP de manera consiguiente:

Host - Nombre	IP	MAC -Address
PC14	192.168.0.117	0013466091E1

Seguidamente se produjo la desconexión del dispositivo “PC14” y la conexión nuevamente.

Al realizar un nuevo relevamiento, se observa que el hosts “PC14” se encuentra asociado a otra dirección IP y al entablar una nueva conexión directa con la computadora “VictimaPC” se obtiene la siguiente dirección IP: 192.168.0.118

A continuación se realiza el análisis comparativo de la dirección IP y MAC arrojadas en un primer momento y las correspondientes luego de haberse producido la desconexión y reconexión del dispositivo, obteniendo el presente resultado:



Se puede observar que se produjo un cambio en la dirección IP otorgada en distintos momentos para el mismo dispositivo, pero la correspondiente dirección MAC sigue siendo la misma para la misma computadora.

CAPITULO V:

ANALISIS DE RESULTADOS

6. CAPITULO V: ANALISIS DE RESULTADOS

Habiendo realizado el trabajo de campo y la descripción de los quince (15) casos desarrollados, se procederá al análisis correspondiente de los resultados obtenidos.

6.1 Análisis Primario o de casos aislados

En base a los objetivos planteados, tanto general como específicos, el fin último de la investigación es determinar la efectividad de la identificación por MAC- Address en redes de área local, complementando el método de identificación por dirección IP, luego de haberse producido una desconexión y nueva conexión a la red empleada.

Al realizar el análisis de los datos obtenidos, se pueden considerar dos tipos de análisis: análisis de casos aislados y análisis de casos en conjunto

El análisis de casos aislados, y quizás el más significativo en lo que respecta a la presente investigación, describe el comportamiento que muestra tanto la dirección IP como la dirección MAC de cada computadora de forma separada, en cada uno de los casos de estudio. Es decir, si se registró o no cambio en las direcciones antes nombradas, luego de haberse producido la desconexión y nueva conexión a la red de estudio.

Con los datos relevados se pudo desarrollar la siguiente tabla:

N° CASOS	Dirección IP	Dirección MAC-Address
1	CAMBIA	NO CAMBIA
2	CAMBIA	NO CAMBIA
3	CAMBIA	NO CAMBIA
4	CAMBIA	NO CAMBIA
5	CAMBIA	NO CAMBIA
6	CAMBIA	NO CAMBIA
7	CAMBIA	NO CAMBIA
8	NO CAMBIO	NO CAMBIA
9	CAMBIA	NO CAMBIA
10	NO CAMBIA	NO CAMBIA
11	NO CAMBIA	NO CAMBIA
12	NO CAMBIA	NO CAMBIA
13	NO CAMBIA	NO CAMBIA
14	NO CAMBIA	NO CAMBIA
15	CAMBIA	NO CAMBIA

Como se puede observar, para cada caso, se puede analizar si se registró cambio en la dirección IP y MAC asignada a una misma computadora; dando como resultado que, en términos de efectividad la dirección MAC- Address no registro cambios en el total de los quince (15) casos analizados. Sin embargo, no se obtuvo el mismo resultado en el análisis realizado sobre las direcciones IP, ya que existen nueve (9) casos en los cuales se produjo cambio y seis (6) en los que la dirección IP permaneció inmutable.

Atento a lo expuesto, se puede establecer en términos de porcentaje que:

Efectividad	
Dirección IP	Dirección MAC
6 / 15 = 0,4 **40%**	15 / 15 = 1 **100 %**

Debido a que el estudio de la identificación por MAC- Address no registró ningún cambio, se puede considerar efectiva en el 100 % de los casos analizados en comparación a la identificación por IP donde se obtiene un 40 % de efectividad.

Con base en la inexistencia de modificación en las direcciones MAC, en los casos estudiados, no es posible realizar otro tipo de análisis estadístico; ya que con este punto de vista la identificación por dirección MAC de forma aislada, resulta efectiva sin margen de error alguno. No obstante, se puede desarrollar un análisis secundario relacionando la variación registrada de la dirección IP con la dirección MAC correspondiente obtenida en cada uno de los casos simulados.

6.2 Análisis Secundario o de casos en conjunto

En este punto se analizara en forma conjunta la variación tanto en dirección IP como la dirección MAC de cada caso simulado, pudiendo realizar un análisis estadístico descriptivo de los casos y posteriormente el análisis estadístico inferencial.

Con el fin de hacer ameno el análisis y su comprensión, se van a considerar “casos positivos” o éxitos, los casos simulados donde se pudo visualizar un cambio en la dirección IP de la computadora investigada, luego

de producida la desconexión y nueva conexión de la misma a la red. En estos, se observa que la dirección física o MAC Address de la computadora permanece inmutable, posibilitando la individualización del ordenador a partir de dicho indicador.

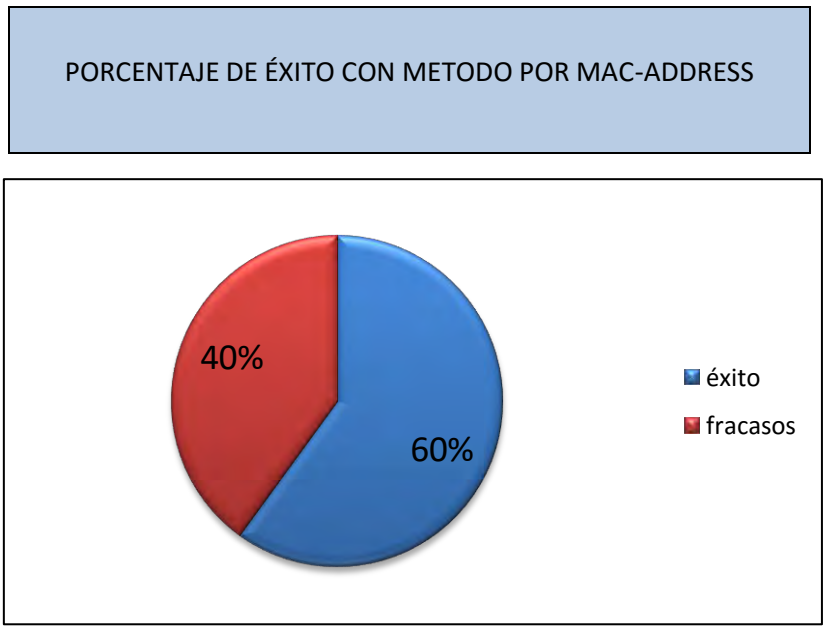
En contrapartida, se va a considerar "negativos" o fracasos, los casos simulados donde no existe cambio alguno tanto en la dirección IP como en la dirección MAC de la misma computadora investigada, luego de ocasionar la desconexión y reconexión nuevamente a la red; lo que justificaría la utilización del método vigente en la actualidad.

Habiendo hecho las debidas aclaraciones, se continúa con el análisis. Del total de quince (15) casos simulados objeto de análisis, y teniendo en cuenta las condiciones plateadas recientemente, se desarrolla la siguiente tabla:

N° de caso	**Resultado obtenido**
1	POSITIVO
2	POSITIVO
3	POSITIVO
4	POSITIVO
5	POSITIVO
6	POSITIVO
7	POSITIVO
8	NEGATIVO
9	POSITIVO
10	NEGATIVO
11	NEGATIVO
12	NEGATIVO
13	NEGATIVO
14	NEGATIVO
15	POSITIVO

Total EXITOS=	**9**
Total FRACASOS=	6
TOTAL=	**15**

Realizando el conteo, se observan nueve (9) casos positivos o efectivos y seis (6) casos negativos o no efectivos. A partir de estas cifras, se puede establecer que:



6.2.1 Análisis descriptivos de datos

En el campo de los estudios estadísticos, el trabajo desarrollado es compatible con una distribución de probabilidad de tipo *BINOMIAL;* ya que solo consideramos dos tipos de resultados (ÉXITO o FRACASO), mutuamente excluyente, para cada uno de los casos simulados; los que a fines del análisis serán considerados como *experimentos*.

La variable en estudio es una **variable aleatoria discreta,** ya que esta puede tomar valores finitos dentro del experimento: 1<x<15;

considerando a X como el número de “éxitos” que se obtienen para “n” experimentos.

En forma de ecuación:

$$P\,[X = x] = \binom{n}{x} p^{X} (q)^{n-x}$$

Siendo:

n: N° de experimentos

p: probabilidad de éxito

q: probabilidad de fracaso

Aplicando los datos obtenidos a la formula antes mencionada, se obtiene la siguiente tabla:

Datos:

Éxito ⟹ Cambio en IP y no cambio en MAC

Fracaso ⟹ No cambio en IP y no cambio en MAC

Muestra ⟹ n = 15

Probabilidad de Éxito ⟹ p = 0,5

Probabilidad de Fracaso ⟹ q = 0,5

Caso = x	Resultado	P(x)	Probabilidad de obtener éxitos (%)
1	ÉXITO	0,000457764	0,046%
2	ÉXITO	0,003204346	0,320%
3	ÉXITO	0,013885498	1,389%
4	ÉXITO	0,041656494	4,166%
5	ÉXITO	0,091644287	9,164%
6	ÉXITO	0,152740479	15,274%
7	ÉXITO	0,196380615	19,638%
8	FRACASO	0,196380615	19,638%
9	ÉXITO	0,152740479	15,274%
10	FRACASO	0,091644287	9,164%
11	FRACASO	0,041656494	4,166%
12	FRACASO	0,013885498	1,389%
13	FRACASO	0,003204346	0,320%
14	FRACASO	0,000457764	0,046%
15	ÉXITO	3,05176E-05	0,003%

- Media:

$$\mu = n \,.\, p \quad \Longrightarrow \quad 7{,}5$$

La media es el promedio del conjunto de datos que se están analizando, en este caso es de 7,5.

- Desviación Típica o estándar:

$$S = \sqrt{n \,.\, p.\, q} \quad \Longrightarrow \quad 1,9365$$

La desviación, muestra que los datos están distribuidos alrededor de la media; cuanto menor es el valor numérico, los datos se encuentran próximos a la media. Para el presente análisis se puede observar que la distribución tiende a concentrar valores positivos hacia el valor de la media (7,5).

6.2.2 Análisis inferencial de los datos

Para realizar los cálculos inferenciales, sobre los casos de estudio, se empleará el método "prueba de hipótesis"; utilizada para determinar si existe suficiente evidencia, en una muestra de datos, que posibilite inferir que cierta condición es válida para toda la población. Para hacerlo, se examinan dos hipótesis opuestas sobre los datos obtenidos: por un lado la *Hipótesis Nula* (H_o), que representa el postulado que se desea concluir como verdadero, y por otro la *Hipótesis Alternativa* (H_1).

Con base en los datos recolectados, y según el nivel de significación definido, se puede aceptar la hipótesis nula cuando el valor numérico de prueba calculado, a partir de la formula correspondiente (Zp) es menor al valor crítico (Zc) del análisis.

En primera medida se definirán los postulados de cada hipótesis, de la siguiente manera:

$H_o \leq 7$ → La cantidad de éxitos obtenidos son **menores o iguales** que 7 de 15 casos

$H_1 > 7$ → La cantidad de éxitos obtenidos son **mayores** que 7 de 15 casos analizados

En cuanto al nivel de significancia (α) de la prueba, se lo especificará como 0,05, lo que establece que el nivel de confianza será del 95 %. La elección del nivel de significancia se realizó atento a la reducida muestra con la que se está trabajando (15 casos simulados).

Seguidamente, se debe establecer el valor crítico (Zc) apropiado para este análisis; ya que el mismo define la zona de aceptación y zona de rechazo de la hipótesis nula. Según la Tabla de Distribución Binomial, para el valor de significancia tomado (0,05), el valor de Zc es 1,0000.

De esta manera, la región de aceptación estará comprendida entre – infinito y 1 (-∞; 1), y la región de rechazo entre 1 y + infinito (1; +∞).

Prosiguiendo, se debe calcular el valor de prueba (Zp) a partir del siguiente análisis:

Datos:

n = 15	μ = 7,5
p = 0,5	S = 1,9365
α = 0,05	Zc = 1,000

Ecuación para distribución binomial:

$$Zp = \frac{\mu - Ho}{\frac{S}{n^p}}$$

$$Zp = \frac{7{,}5 - 7}{\frac{1{,}9365}{15^{0{,}5}}}$$

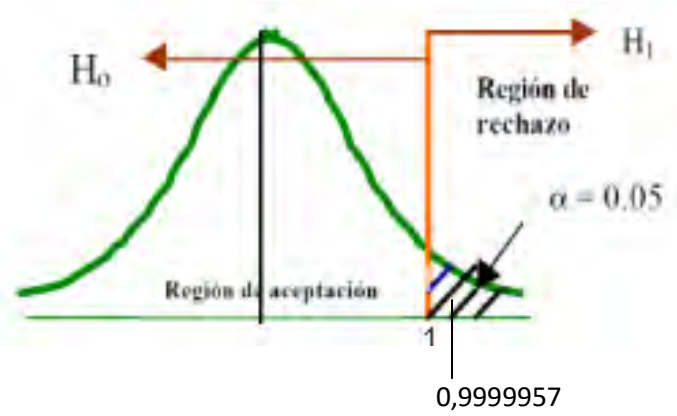
$$Zp = 0{,}9999957$$

Por último, se realiza la comparación entre el valor crítico Zc y el valor que se obtuvo de la prueba Zp, para determinar si la hipótesis nula se encuentra dentro de la zona de aceptación o rechazo.

$$Zc > Zp$$

$$1{,}000 > 0{,}9999957$$

En forma gráfica:



Concluyendo el análisis, dado que Zp se encuentra dentro de la región de aceptación:

Se establece que de 15 casos analizados se obtendrán al menos 7 resultados exitosos con un nivel de confianza del 95 %.

CAPITULO VI:

CONCLUSIONES

7. CAPITULO VI: CONCLUSIONES

El continuo desarrollo de la tecnología y el alto impacto que representa en la vida cotidiana de las personas hace que en menor o mayor medida, todo individuo deba relacionarse con redes de computadoras. Esta relación establece ciertas ventajas, pero también implica muchos riesgos; pues permite abrir ventanas que viabilizan la comisión de delitos con un alto grado de anonimidad.

Es por ello, que luego del trabajo de campo realizado y análisis exhaustivo de sus resultados, se llegó a la siguiente conclusión:

La efectividad de los mecanismos que permiten identificar la dirección física (MAC- Address), de las computadoras empleadas para efectuar acciones ilícitas, resulto efectiva en la totalidad de los casos estudiados (Ítem 6.1); complementando de forma positiva la identificación de computadoras vigente en la actualidad, que emplea como indicador la dirección IP.

Del mismo modo, y a partir del análisis estadístico inferencial sobre los datos relevados bajo las condiciones establecidas, se concluye que:

Si se analizan (15) quince casos de delitos cometidos en redes de área local, se obtendrán al menos (7) siete casos donde resulta 95 % efectiva la identificación por dirección física (Ítem 6.2.2) complementando exitosamente la identificación por dirección IP.

Por todo lo expresado a lo largo del trabajo, y debido a las conclusiones arribadas, se considera que el empleo de la dirección MAC se traduciría en un mayor grado de exactitud al momento de identificar computadoras implicadas en delitos; facilitando, de esta manera, la labor diaria de los investigadores, cuyo objetivo es encontrar al individuo responsable del acto delictivo.

CAPITULO VII:

ALCANCES Y NUEVOS INTERROGANTES

8. CAPITULO VII: ALCANCES Y NUEVOS INTERROGANTES

Se podría decir que el concepto de dirección física o MAC –Address no se encuentra dentro de la lenguaje empleado en investigaciones criminales en la actualidad; esto motivó la presente investigación ya que se considera un indicador que puede resultar beneficioso a la hora de obtener resultados lo más acertado posible.

Nótese que el término empleado es “lo más acertado posible”, porque se debe tener presente que en el ámbito Informático, y sobre todo en el ámbito Informático Forense, no existe indicador que sea 100 % seguro y eficaz. Esto se debe, entre otros factores, al constante avance de la tecnología.

El desarrollo de un nuevo hardware o software implica, a veces, repetir el proceso de adaptación de los usuarios al funcionamiento y manejo del mismo. Esta “adaptación” también las realizan personas que desean cometer ilícitos en las macro o micro redes de computadoras, con el fin de sofisticar su accionar para no ser identificados.

En el área de Seguridad Informática se habla de “niveles de seguridad”; haciendo referencia a una escala jerárquica donde existen medidas o indicadores de seguridad baja, media y alta; de la misma manera se puede considerar en el ámbito de la Informático-forense, situando como indicador de baja confiabilidad la identificación dada por “Hosts” o nombre de la computadora. Un indicador intermedio a la identificación por “dirección IP” y como un indicador superior a la identificación por “dirección MAC –Adrdress”

Sin embargo, así como existen algunos programas y maniobras para cambiar la dirección IP de una computadora, existen también algunos métodos por medio de los cuales se puede cambiar, enmascarar o hasta incluso clonar la dirección MAC –Address de una tarjeta de red. Estas maniobras, no son tan comunes en la actualidad, porque son procedimientos

complejos que requieren un conocimiento mucho más profundo en lo que respecta a redes de computadoras y a su funcionamiento interno.

Como se mencionara en párrafos anteriores, la identificación por MAC –Address puede ser considerada como un escalón más arriba que la identificación por IP, en lo que a efectividad se refiere, pero en el amplio mundo de la Informática nada es seguro.

Por ello, el presente trabajo académico pretende mostrar que el análisis conjunto de la dirección IP como MAC-Address en las investigaciones de delitos informáticos colabora mejorando la probabilidad de una identificación exitosa de la computadora involucrada en un accionar delictivo.

En lo que respecta al análisis sobre direcciones IP, ya se destacó en capítulos anteriores que existen dos versiones de este protocolo: IPv4 y IPv6. El primero corresponde al que se encuentra en uso actualmente y con el cual se trabajo durante todos los experimentos realizados. El protocolo IPv6 se encuentra en fase experimental y promete ser el futuro en el mundo de las redes, coexistiendo hoy con IPv4 hasta poder llegar a reemplazarlo.

El protocolo IPv6 surgió a partir del acelerado crecimiento de Internet, donde las direcciones IPv4 ya no son suficientes para identificar todos los dispositivos que se conectan a las redes. El protocolo IPv4 sólo posibilita 4.294.967.296 direcciones IP que puede asignar. Sin embargo, en la actualidad, este número no satisface a la cantidad de dispositivos que se pueden conectar a redes informáticas; tal es el caso de: computadoras, teléfonos, autos, heladeras, lavarropas, etc.

La nueva versión del protocolo IP implemente algunas ventajas por encima de la versión vigente; dentro de las cuales se puede mencionar: envió de paquetes de datos seguros (cifrados/encriptados) haciendo difícil la interpretación de su contenido, varias direcciones de red asignadas al mismo

dispositivo posibilitando la conexión con distintas redes de forma simultánea, entre otras.

Como se dijo, la versión IPv6 se encuentra recorriendo su camino en las redes, esto amerita el desarrollo de futuras investigaciones acerca del tema, con el fin de poder establecer si es más o menos efectiva a la hora de identificar a posibles delincuentes cibernéticos.

De la misma manera, otra línea investigativa que se puede considerar para futuras investigaciones, es la aplicación de “Servidores Logs” en redes informáticas. El mismo hace referencia a computadoras independientes o, a programas dentro de la misma computadora, que almacena cronológicamente toda la actividad que tuvo lugar en una red. De esta forma, se puede obtener los accesos que se produjeron registrando dirección IP, dirección MAC, fecha y hora de cada ingreso a la red. Sin embargo, su aplicación se encuentra aun muy limitada a pesar de que esta facilitaría, en gran medida, las investigaciones de delitos informáticos en redes; porque funciona como base de datos de cada proceso que se produjo dentro de la misma.

9. Referencias

Acordada del Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires, aprobada por acuerdo de la Suprema Corte de Justicia Provincial el 15/08/2007.

Allan, A. V. *"Manual de Criminalística".* Recuperado de: http://criminalistica.com.mx/descargas/documentos/pdf/CRIMINALISTICA-AAV.pdf

Álvarez N. y Monzalvez J. (2008) - "*Introducción a las Redes de Computadoras"*- UTFSM

Arocena, G. A. (2012) - *"Introducción a la Ley Nacional N°26.388"*- Recuperado de: http://www.carc.org.ar/wp-content/themes/vox/revista/4-Sobre-regulacion-delitos-informaticos.pdf

Aparici, R. y Osuna Acedo, S. (2013*). "La Cultura de la Participación".* Revista Mediterránea de Comunicación, vol. 4.

Barbini, A. (2015). *"Correo electrónico, redes sociales y proveedores de Internet en el Proceso Penal"*. Ed. La Roca.

Cano Martínez, J. J. (2005). *"Evidencia Digital: Contexto, Situación e implicaciones nacionales."*

Casey, E. (2004). *"Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet".*

Diccionario Judicial del NOA. Recuperado de: http://judicialdelnoa.com.ar/diccionario_juridico/DICCIONARIO%20JURIDICO.pdf

Giovanni Zucardi, Juan D. Gutiérrez (2006) – *"Informática Forense"*. Recuperado de: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Gómez Vietes, A. (2007). *Enciclopedia de la Seguridad Informática*. México. Ed. Alfa omega Ra-Ma:

Hernandez Sampieri, R**.** "*Metodologia de la Investigacion".* Mexico. Ed. Digital.

Juan, H. R.(2001). *"Introducción a la Ciencia Criminalística"*. Ed. Jurídicas Cuyo.

Katz, M. (2013*). "Redes y Seguridad".* Buenos Aires . Ed. Alfa omega.

López; Amaya; León; Acosta (2002)- *"Informática Forense: Generalidades, aspectos técnicos y herramientas"*-Univ. los Andes.

Luzuriaga Quichimbo, J. E. (2008) - *Tesis "Aplicación Web para encender y apagar computadoras (con tarjeta de red con opción Wake on Lane)*". Recuperado de: http://repositorio.ute.edu.ec/bitstream/123456789/5667/1/33533_1.pdf

Machado Schiaffino (1992). *Diccionario Pericial.* Ed. La Roca

Montiel Sosa, J. (2003). *Criminalística Tomo I*. Ed. Noriega

ONU (1994). *"Manual de las Naciones Unidas para la prevención y control de delitos informáticos".*

ONU (2001). *"Convenio sobre la Ciberdelincuencia"*- Budapest. Recuperado de: http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

Ordinas; Griega; Escale; Olive; Tornil (2004)- *"Redes de Computadoras"*- Formación de Posgrado UOC

Poder Judicial de la Provincia de Neuquen (2015)- *"Protocolo de Actuacion para Pericias Informaticas".* Recuperado de: http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloActuacionPericiasInformaticas.pdf

Portantier, F. (2012)- "*Seguridad Informática".* Buenos Aires- Argentina. Ed. RedUsers.

Riffo Gutiérrez, M. A.(2009). *Tesis "Vulnerabilidad de las redes tcp/ip y principales mecanismos de seguridad".* Recuperado de:http://cybertesis.uach.cl/tesis/uach/2009/bmfcir564v/doc/bmfcir564v.pdf.

Toranzo F. R. y Ruiz Rivas, J. A. (2004)- "*Redes de área local".* Recuperado de: http://www.forpas.us.es/aula/hardware/dia4_redes.pdf

Piscitelli, E. (2015). "*El fin de la privacidad". USERS* edición N° 295, 8-9. Recuperado de: http://issuu.com/redusers/docs/issue_users_245/9?e=1678534/31002152

ANEXO N° 1:

"PROTOCOLO DE ACTUACION PARA PERICIAS INFORMATICAS"

10. ANEXO Nº1: "PROTOCOLO DE ACTUACION PARA PERICIAS INFORMATICAS"

a) Descripción general de servicios de informática forense

A los fines de brindar mayores detalles del quehacer pericial, dando a conocer las áreas de competencia de la pericia informática, es oportuno detallar un catálogo de servicios de informática forense. Este conjunto de categorías no es taxativo sino descriptivo e informativo. No se trata de un número cerrado de servicios forenses sino que dicha enumeración pretende orientar al operador judicial sobre temáticas en las que es posible plantear requerimientos judiciales. Finalmente serán los puntos de pericia los que deberán contener elementos particulares de información objetiva sobre los hechos investigados, para que el especialista pueda aplicar teorías, técnicas y métodos de análisis forense a través de herramientas especializadas. Sin perjuicio de ello, los requerimientos periciales han de procurar la necesidad real de conocimientos especiales en informática forense, siendo esta disciplina una especialidad de las ciencias informáticas como lo es la medicina legal respecto de la medicina.

Catálogo de servicios[1]
1. Pericia sobre infracción a la ley de propiedad intelectual del software.
2. Pericia sobre control, actualización y adquisición de licencias de software.
3. Pericia sobre robo, hurto, borrado intencional o accesos no

[1] Concordante con los servicios ofrecidos por Peritos: Especialidad en Sistemas Informáticos, definida por el Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires, aprobada por acuerdo de la Suprema Corte de Justicia Provincial el 15/08/2007.
http://www.cpciba.org.ar/

autorizados a la información de una determinada empresa o institución, procesada y/o generada por los sistemas de informáticos.
4. Pericia sobre duplicación no autorizada de datos procesados y/o generados por los sistemas informáticos.
5. Pericia sobre métodos y normas a seguir en cuestión de seguridad y privacidad de la información procesada y/o generada por los sistemas informáticos.
6. Pericia sobre la realización de auditorías de áreas de sistemas y centros de cómputos así como de los sistemas informáticos utilizados.
7. Pericia sobre recupero de datos borrados y rastreo de información en los distintos medios informáticos (magnéticos – ópticos).
8. Pericia sobre métodos y normas a seguir en cuestión de salvaguarda y control de los recursos físicos y lógicos de un sistema informático.
9. Pericia sobre desarrollo, manejo e implementación de proyectos informáticos.
10. Pericia sobre contratos en los que la informática se encuentre involucrada (contratación de servicios, adquisición de equipamiento informático y de sistemas, tercerización de servicios).
11. Pericia sobre aspectos laborales vinculados con la informática. Uso de Internet en el trabajo, uso indebido de las facilidades de la organización otorgadas a los empleados (servicio de correo electrónico, acceso a la navegación por Internet, uso de computadoras, entre otros elementos).
12. Pericia sobre robos o determinación de identidad a través de correos electrónicos.
13. Pericia sobre aspectos vinculados al comercio electrónico y operaciones realizadas a través de Internet.
14. Pericia sobre dispositivos de telefonía celular

b) Del procedimiento general de investigación judicial con tecnología informática

En el ámbito penal, el procedimiento general de investigación judicial utilizando servicios de informática forense consta de dos etapas principales:

a) Incautación confiable de la prueba y mantenimiento de la Cadena de Custodia.
b) Análisis de la información disponible con arreglo al incidente investigado y redacción del informe pericial.

La primera etapa debe ser llevada a cabo por personal policial junto al Fiscal responsable del control o de la ejecución de la medida, siguiendo la "Guía operativa para el secuestro de tecnología Informática". La segunda etapa debe ser efectuada en el laboratorio por un Perito, siguiendo los estándares de la ciencia forense para el manejo de evidencia digital, en función a los puntos de pericia que sean indicados por los operadores judiciales.

c) De la identificación y preservación de evidencia digital

El Fiscal deberá realizar una planificación minuciosa del procedimiento judicial para la incautación de material probatorio. La identificación de material tecnológico por parte del personal policial debe ser efectuada conforme las pautas de la "Guía operativa para el secuestro de tecnología informática" que integra el presente documento. Es de especial importancia la utilización de precintos de seguridad desde el momento del secuestro del material, y todos aquellos medios tendientes a garantizar la autenticidad e integridad de la evidencia digital. A tal fin se deben seguir los lineamientos indicados en el "Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos" que complementa el presente protocolo. Por regla deberá preferirse el secuestro del material tecnológico a cualquier otra alternativa para la preservación de información digital. Es

importante tener presente que existen características únicas de determinado material tecnológico que imposibilita la realización de la pericia informática si no se cuenta con los elementos originales. Las tareas operativas en el lugar del hecho resultan sumamente dificultosas por el tiempo que requieren las herramientas forenses para completar su ejecución, la carencia de personal policial capacitado para dichas tareas, la escasez de 6 recursos tecnológicos, y las complejidades técnicas y riesgos asociados al trabajo en un entorno bajo presión. Excepcionalmente, si existiese la posibilidad de preservar la información digital en el lugar del hecho, dichos menesteres deberán ser realizados por personal policial capacitado, con los elementos técnicos adecuados y siguiendo una guía de procedimiento. Ello quedará a criterio facultativo del responsable de la operatoria técnica, quien determinará la viabilidad de la tarea.

d) Del requerimiento judicial

Cuando sea requerido, el Perito evacuará las consultas previas de los operadores judiciales para eliminar ambigüedades y definir el alcance de los puntos de pericia en lo que respecta a los servicios de informática forense. Conforme lo prescripto por el Código Procesal Penal y Correccional, sólo se podrán requerir informes periciales cuando para descubrir o valorar alguna evidencia sea necesario poseer conocimientos especiales en informática forense. Se debe proveer toda la información necesaria para realizar la tarea pericial, de manera clara y precisa. El oficio con los puntos de pericia deberá enviarse desde el organismo requirente indefectiblemente junto con el material probatorio que será sometido a análisis forense. En dicho oficio deberán constar los números de serie de las etiquetas que resguardan el material probatorio, y que fueran detalladas en el acta de allanamiento. Una vez que se instrumente el Formulario para Requerimiento del Servicio de informática pericial para todas las dependencias judiciales, éste deberá ser completado por el organismo de origen y enviado al laboratorio pericial como condición excluyente para dar ingreso al pedido de pericia. Sólo se

realizarán pericias que involucren la utilización del hardware y software para informática forense y aquellas que requieran la experticia de un profesional. Quedan excluidas del servicio de pericias informáticas toda tarea administrativa o técnica que no sea propia de la disciplina (tareas de transcripción de texto o simplemente dactilografías, tareas de ordenamiento de información o cruzamiento de datos, tareas de impresión, tareas de escucha, tareas de filmación, elaboración de copias simples conocidas como backups o de resguardo de dispositivos de almacenamiento de información digital). En función a la metodología de trabajo establecida para la actividad pericial informática, no se realizan backups sino que se generan "imágenes forenses" de los 7 dispositivos que contienen información digital (copia bit-a-bit de la evidencia digital – en un formato propietario del software forense utilizado- únicamente a los efectos de realizar sobre ella el análisis forense). La imagen forense es el resultado de un procedimiento metodológico que sirve únicamente para prevenir una posible mala praxis del perito, evitando la contaminación de la prueba. Un backup –por si mismo es un procedimiento invasivo que altera la evidencia digital y no conserva información digital oculta o remanente que es de especial utilidad para la pericia informática. Los "backups" (copia simple de archivos) son medidas de seguridad informática utilizadas por los propietarios de los equipos informáticos para resguardar sus datos, y deben realizarlos con la frecuencia que estimen conveniente, quedando fuera del alcance de la actividad pericial en informática forense. En una empresa, la realización de backups es responsabilidad del área de sistemas o seguridad de la Información de la empresa. En el caso de un particular, es responsabilidad del propietario del equipo informático.

e) De la priorización de casos urgentes

Únicamente se establecerá prioridad en pericias nuevas sobre aquellas que estén en lista de espera cuando se trate de causas con personas detenidas, debiendo ello ser explícitamente ser indicado en el

oficio con el requerimiento judicial. Asimismo, tienen prioridad aquellas causas judiciales por delitos que prevean penas severas por tratarse de bienes jurídicos protegidos de suma relevancia, como la vida o la integridad sexual con autores ignorados, en los que el paso del tiempo ponga en riesgo el devenir de la investigación. En caso de tener dos pericias informáticas con el mismo nivel de urgencia, se dará trámite por orden de ingreso. El especialista podrá brindar una estimación del tiempo requerido para el inicio de la pericia en función de la capacidad operativa disponible, las pericias en trámite y aquellas que estén en lista de espera, conforme las estadísticas propias de la actividad.

f) Del traslado y recepción del material secuestrado

Es responsabilidad del personal policial el traslado de todo el material secuestrado hasta los organismos judiciales. Posteriormente el requirente arbitrará los medios necesarios para el envío de los elementos probatorios al laboratorio pericial. Todo el 8 personal policial o judicial que intervenga en el manejo de la Cadena de Custodia, deberá tener presente las sanciones previstas por el art. 254 y 255 del Código Penal Argentino. Se cotejará la existencia de los precintos sobre los secuestros y la correcta identificación de los elementos enviados a peritaje. En caso de detectarse la alteración o ausencia de precintos de seguridad, se dejará constancia. Cada una de las personas que haya trasladado los elementos probatorios deberá dejar registrada su intervención con los medios que se establezcan.

g) Del análisis forense

Todo el proceso forense está conducido por una metodología de trabajo para el manejo de evidencia digital. Durante el desarrollo de una pericia se utilizan procedimientos operativos estándares con un control de calidad previo realizado en el laboratorio pericial. El Perito trabaja con un equipo profesional, con funciones específicas asignadas y una organización interna, tanto administrativa como profesional. Las distintas actividades

están segmentadas y pueden separarse, permitiendo un análisis autónomo y específico, sin perjuicio de su unión respecto a un resultado. Existe una clara distinción de roles dentro del laboratorio, a saber: asistente técnico, perito informático auxiliar y perito informático oficial. Se considera la capacitación interna para llevar adelante la actividad forense, la idoneidad y la responsabilidad asignada, y el nivel jerárquico conforme experiencia y experticia. La definición del alcance y líneas de investigación forense, así como la elaboración de dictámenes queda a cargo de los peritos de mayor jerarquía y experiencia.

h) De la presentación del dictamen

El dictamen será presentado siguiendo los estándares utilizados para la presentación de reportes informáticos forenses. Se intentará minimizar el volumen de información en soporte papel, suministrando toda la información complementaria que sea necesaria para el objeto de la pericia en soporte digital.

i) De la remisión del material secuestrado

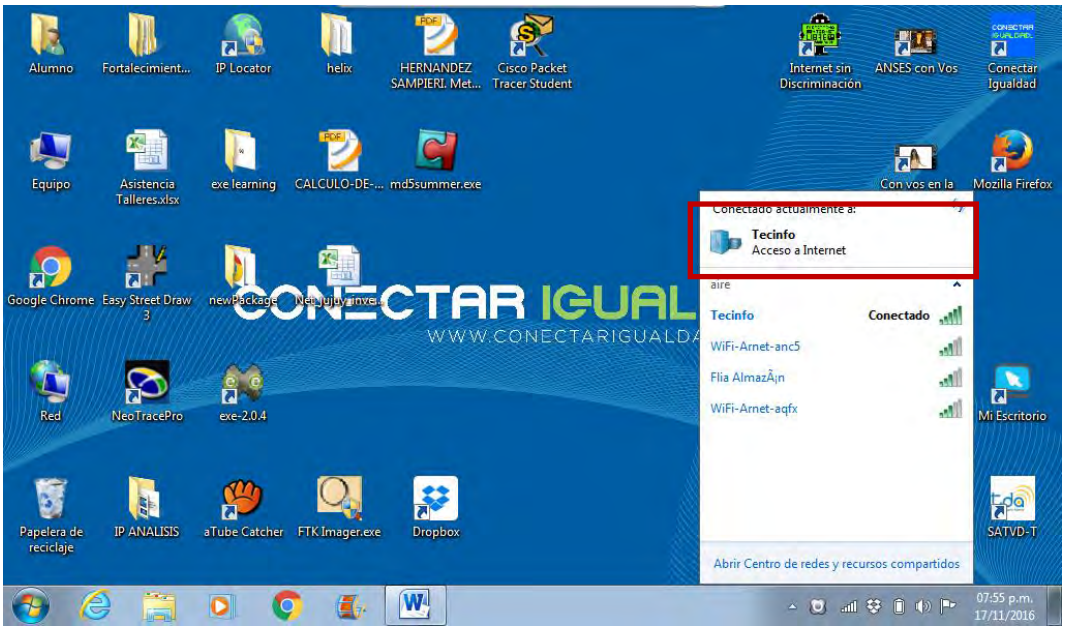
Una vez finalizada la pericia, se remitirá el dictamen y el material secuestrado al organismo de origen. Los elementos analizados deberán ser resguardados con los 9 medios adecuados para preservar la integridad y la autenticidad de la evidencia digital. Los elementos probatorios que contengan evidencia digital deberán resguardarse hasta finalizar el proceso judicial, siendo imprescindible su conservación ya que permite a futuro -y si fuera necesario- repetir o ampliar la pericia.

ANEXO N°2:

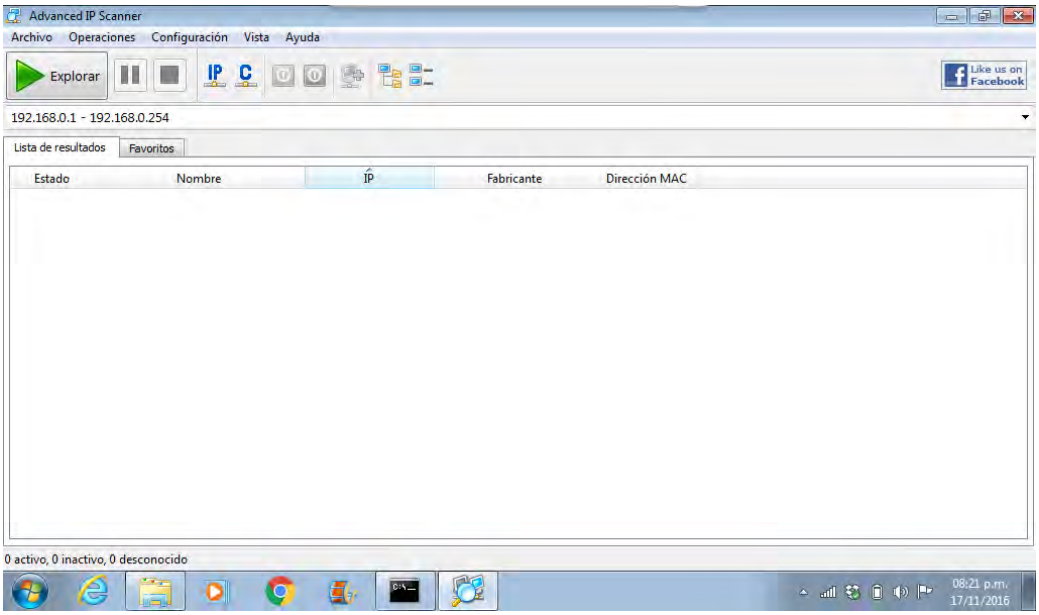
REGISTRO DE CASOS SIMULADOS

11. ANEXO N°2: REGISTRO DE CASOS SIMULADOS

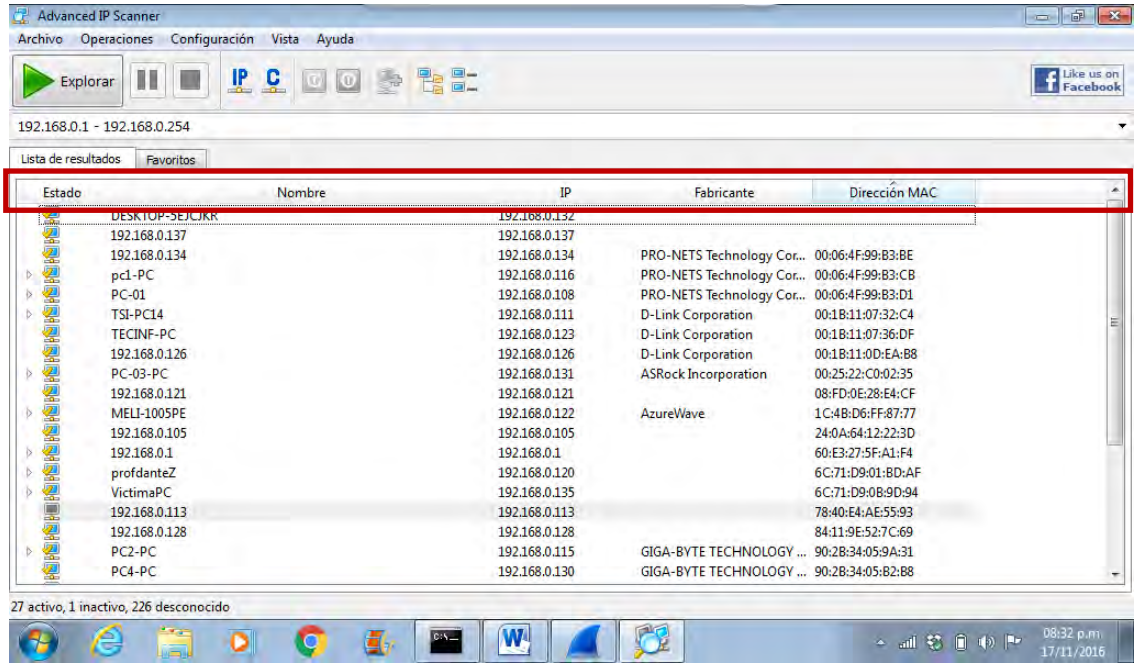
Caso N° 1: 17/11/2016



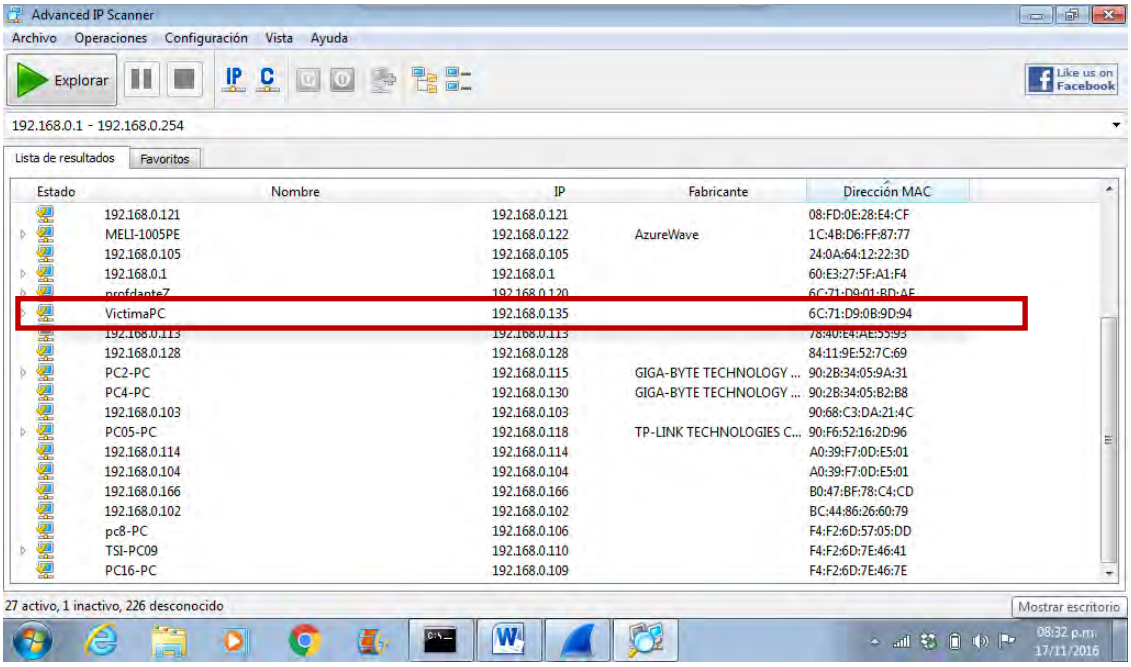
Captura de pantalla N° 1.1: Se establece conexión efectiva con la red "Tecinfo".



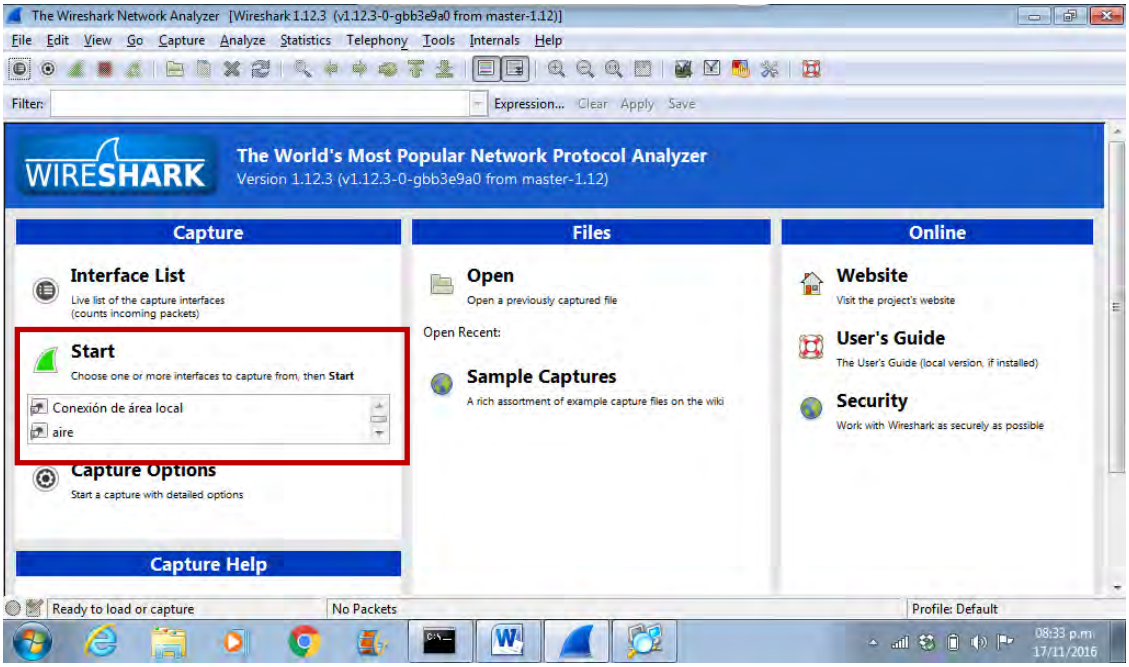
Captura de pantalla N° 1.2: Interfaz del programa "Advanced IP Scanner"



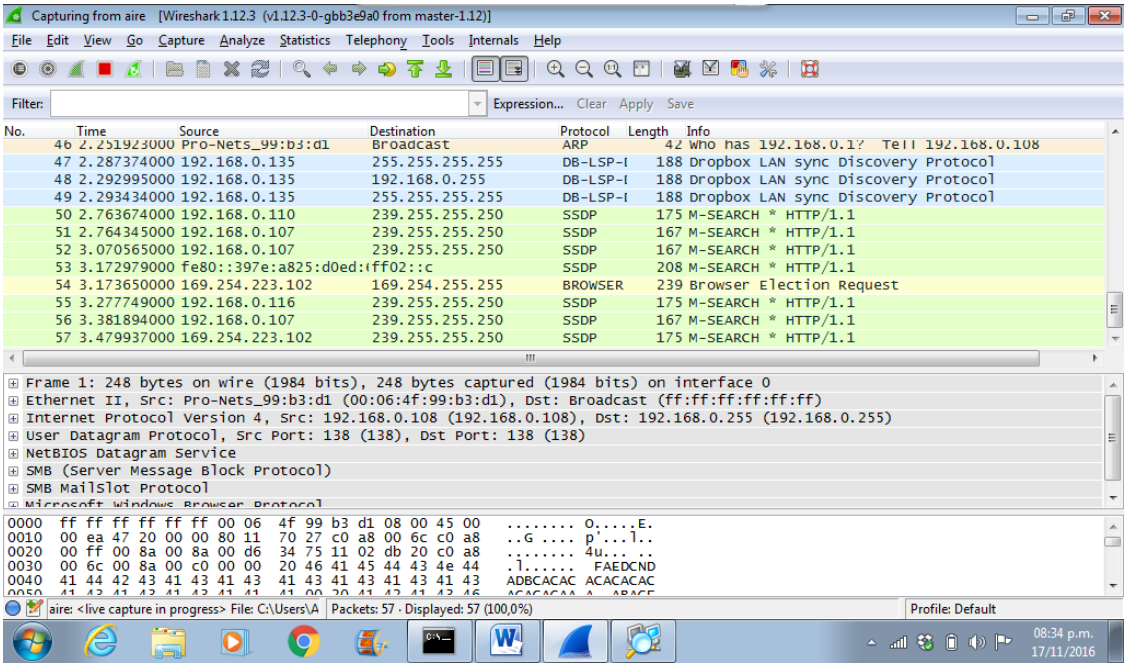
Captura de pantalla N° 1.3.1: Relevamiento de los dispositivos conectados a la red en tiempo real, puediendo obtener: Estado, Nombre, IP, Fabricante y Direccion MAC de cada compuadora.



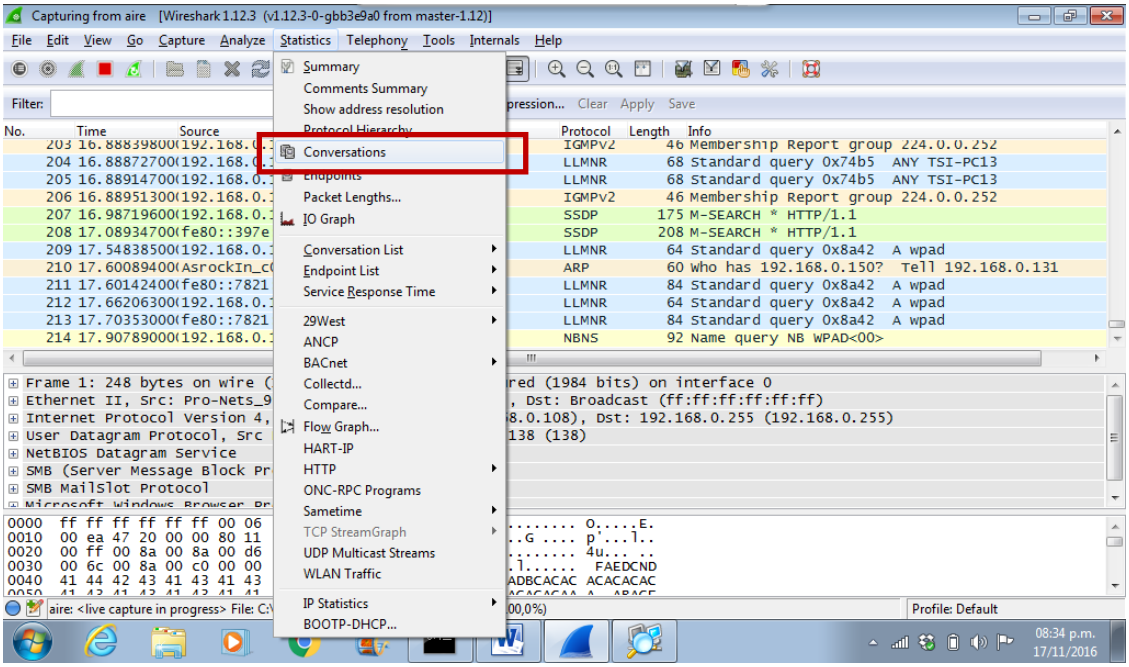
Captura de pantalla N°1.3.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora “VictimaPC” con direccion IP **192.168.0.135**, la cual va a ser la computadora receptora de las acciones ilicitas.



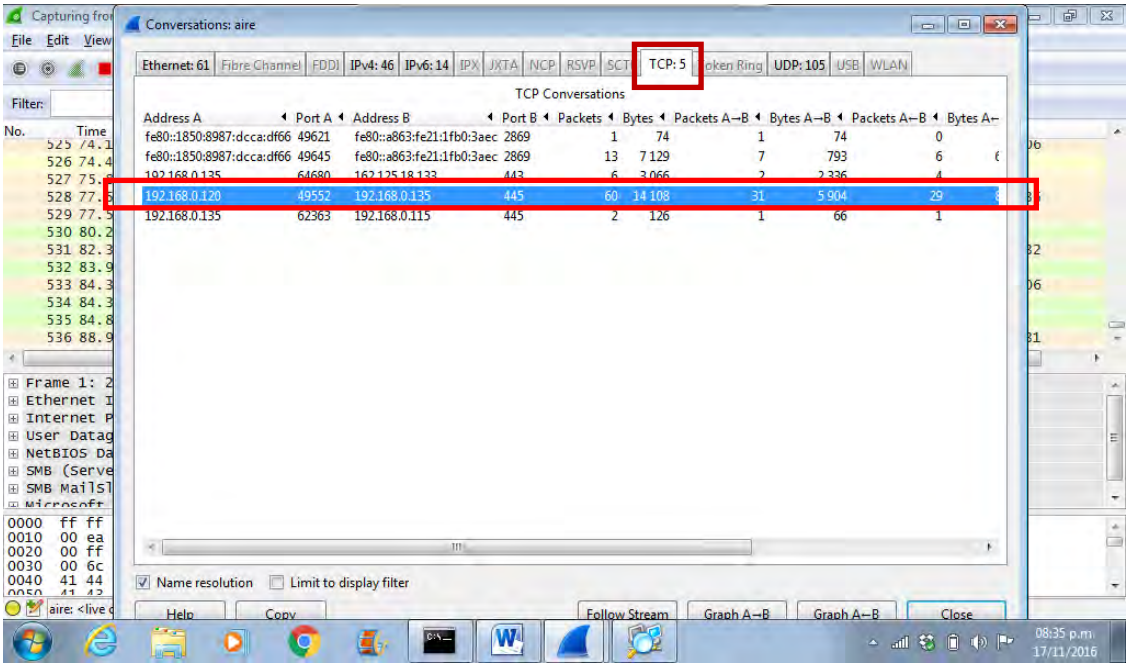
Captura de pantalla N° 1.4: Se procede a ejecutar el programa “Wireshark”. Se presiona “Start”



Captura de pantalla N°1.5: El programa muestra el trafico de los paquetes de datos que circulan por la red en tiempo real

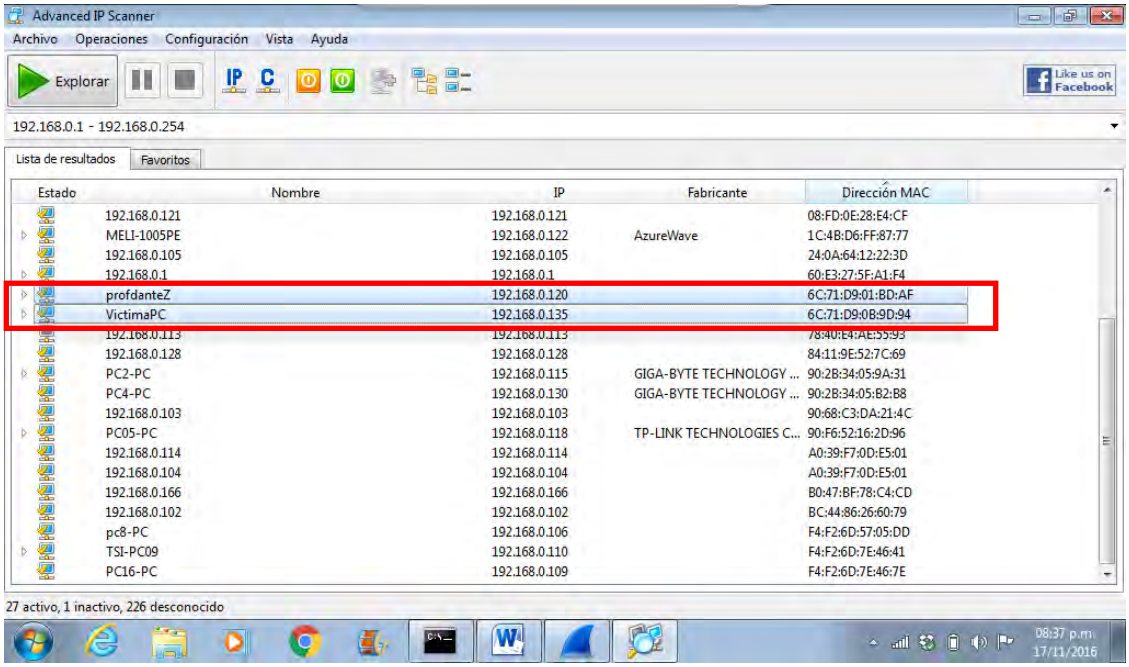


Captura de pantalla N° 1.6: En la pestaña “Statistics” se selecciona la opcion “Conversations”.



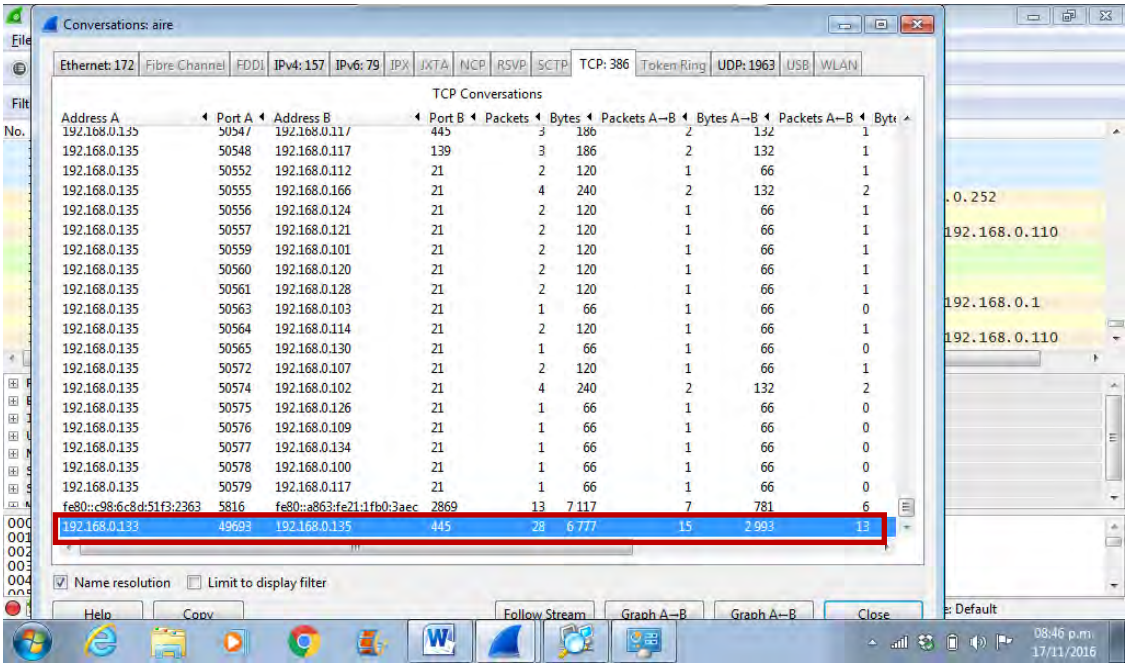
Captura de pantalla N° 1.7: A continuacion se abre una ventana “Conversations: aire”. Dentro de la pestaña “TCP” se pueden visualizar las conexiónes intrared que se estan produciendo, individualizando las direcciones IP que estuvieron en contacto.

Se registra que existio comunicación directa entre la direccion IP **192.168.0.120** con la direccion **192.168.0.135**.

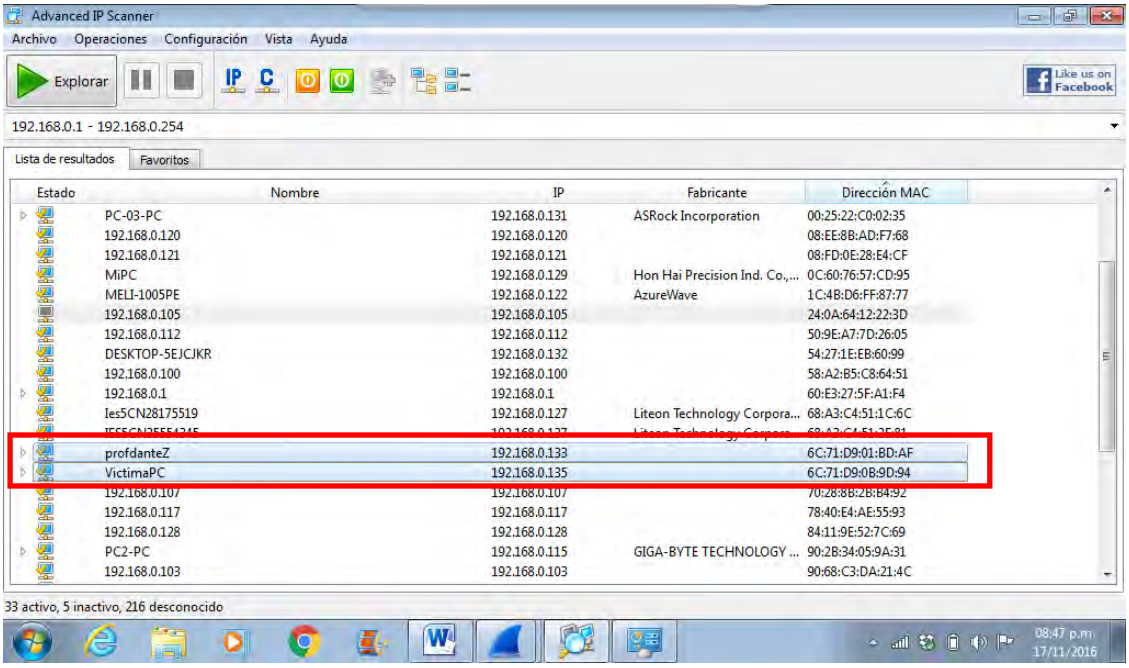


Captura de pantalla N° 1.8: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.120** la asignada al hosts **"profdanteZ"** con direccion MAC **6C:71:D9:01:BD:AF**.

Desconexión del host "profdanteZ": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte.

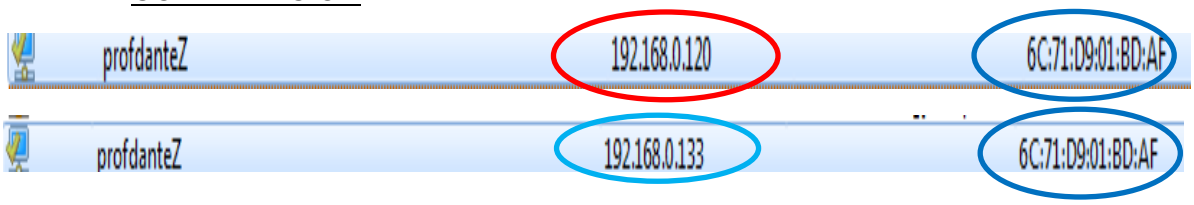


Captura de pantalla N° 1.9: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora "VictimaPC" y una IP hasta ahora desconocida: **192.168.0.133**



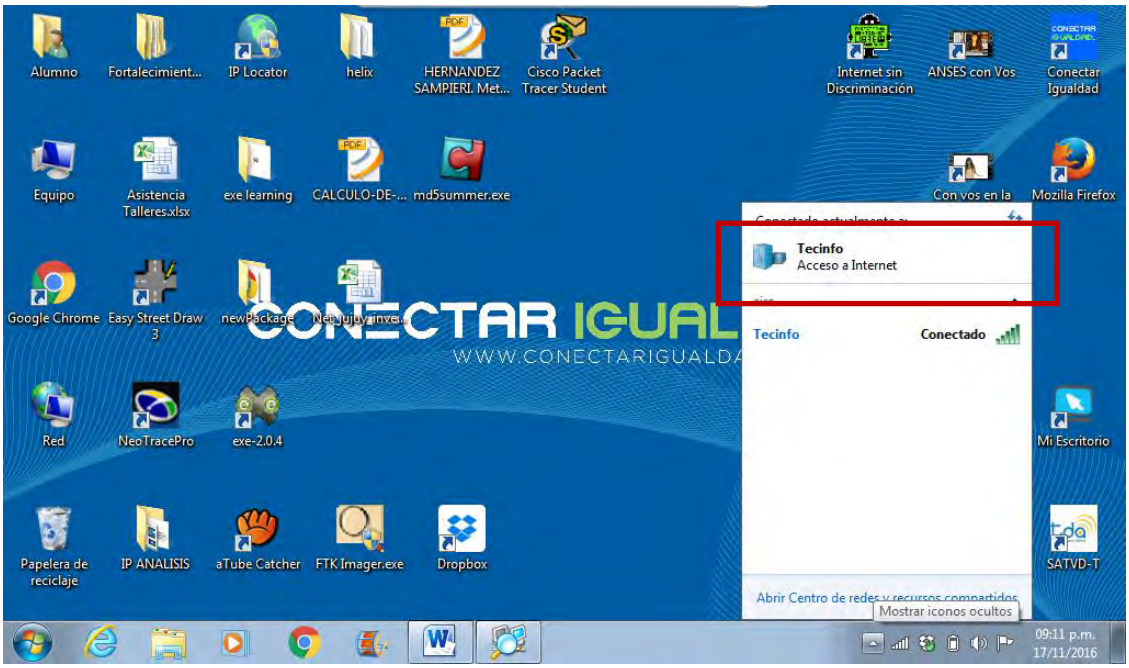
Captura de pantalla N° 1.10: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.133** corresponde al nombre **"profdanteZ"** identificado anteriormente.

CONFIRMACION

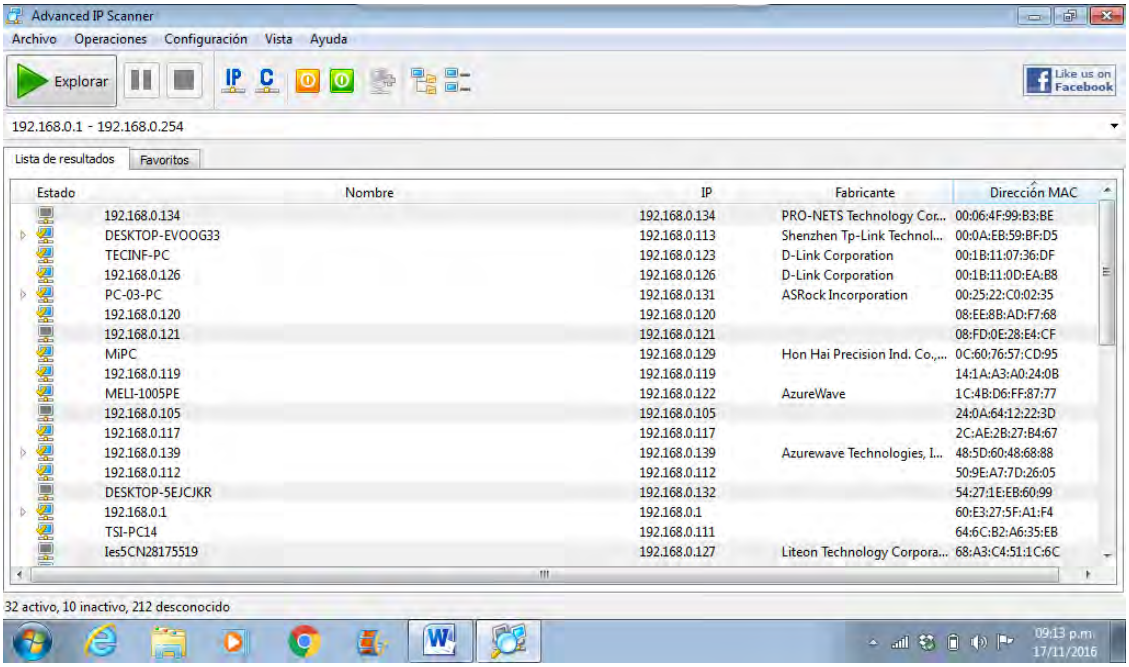


Se observa cambio de la dirección IP de 192.168.0.120 a 192.168.0.133; pero si se comparan las direcciónes MAC que entablaron comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento: **6C:71:D9:01:BD:AF**. Correspondiente a una misma computadora.

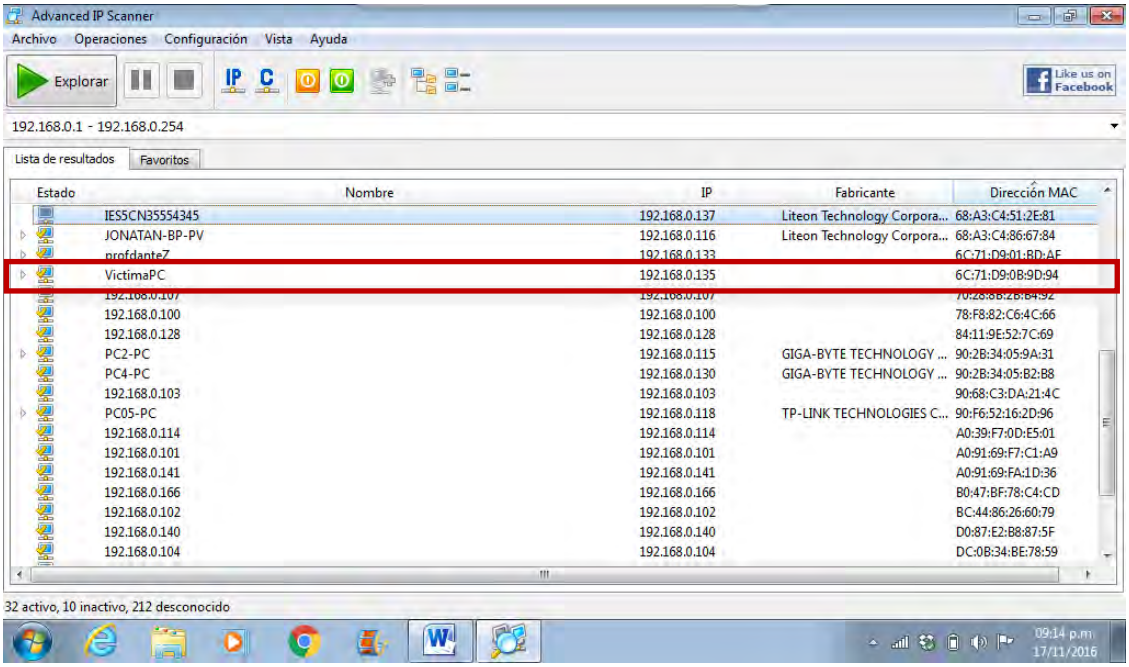
Caso N° 2: 17/11/16



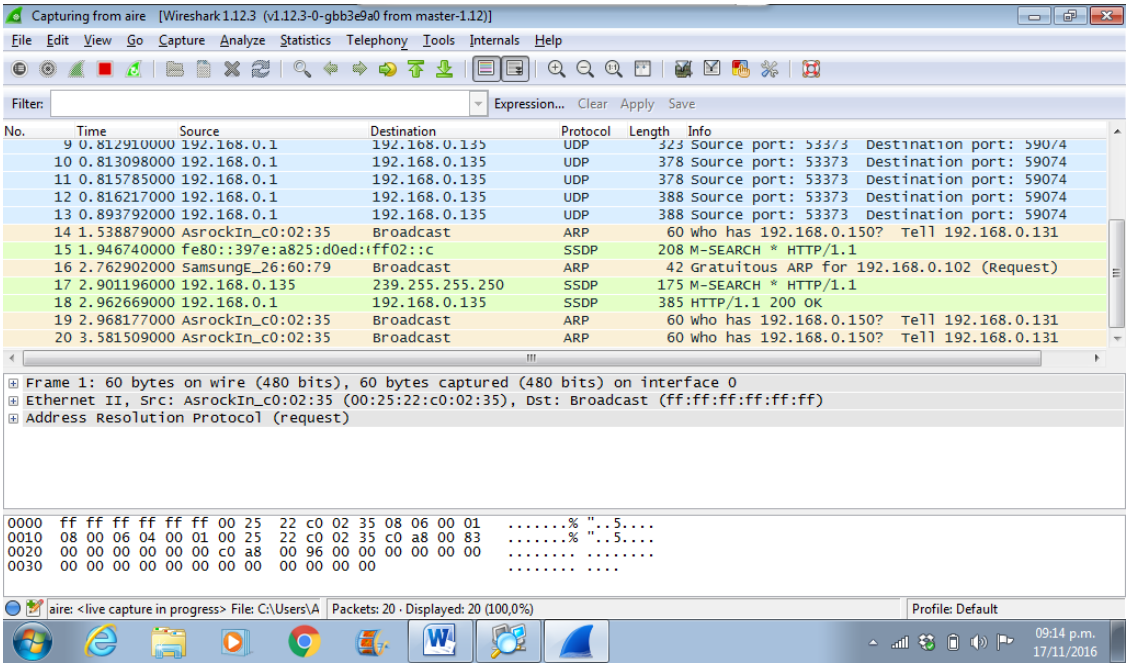
Captura de pantalla N° 2.1: Se establece conexión efectiva con la red "Tecinfo"



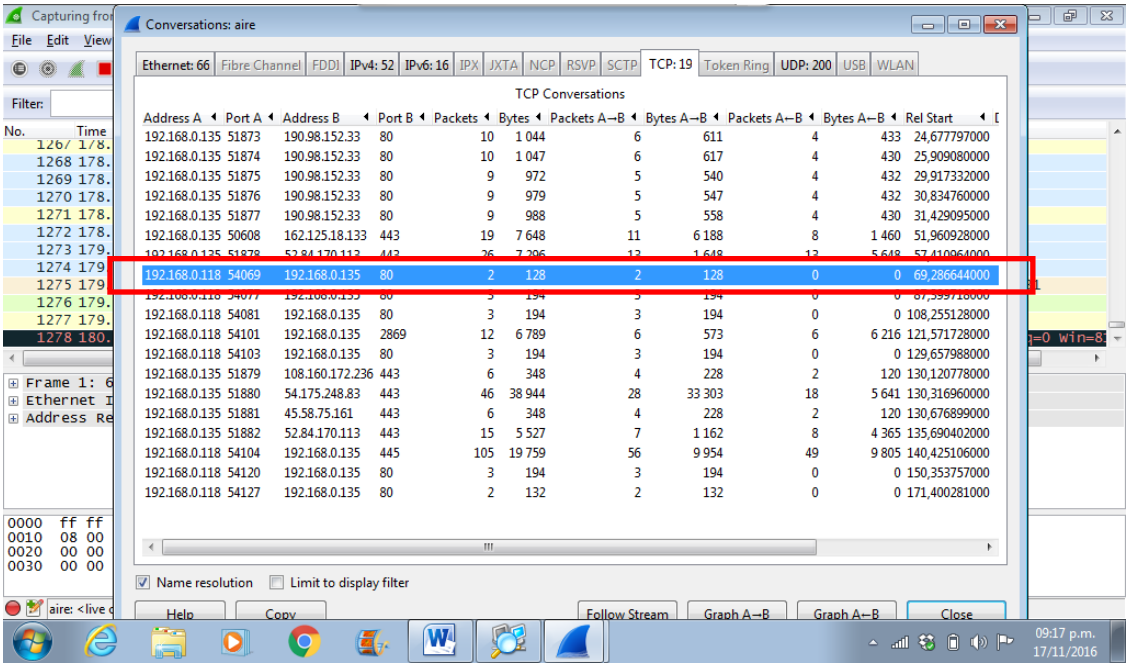
Captura de pantalla N° 2.2.1: Relevamiento de los dispositivos conectados a la red en tiempo real.



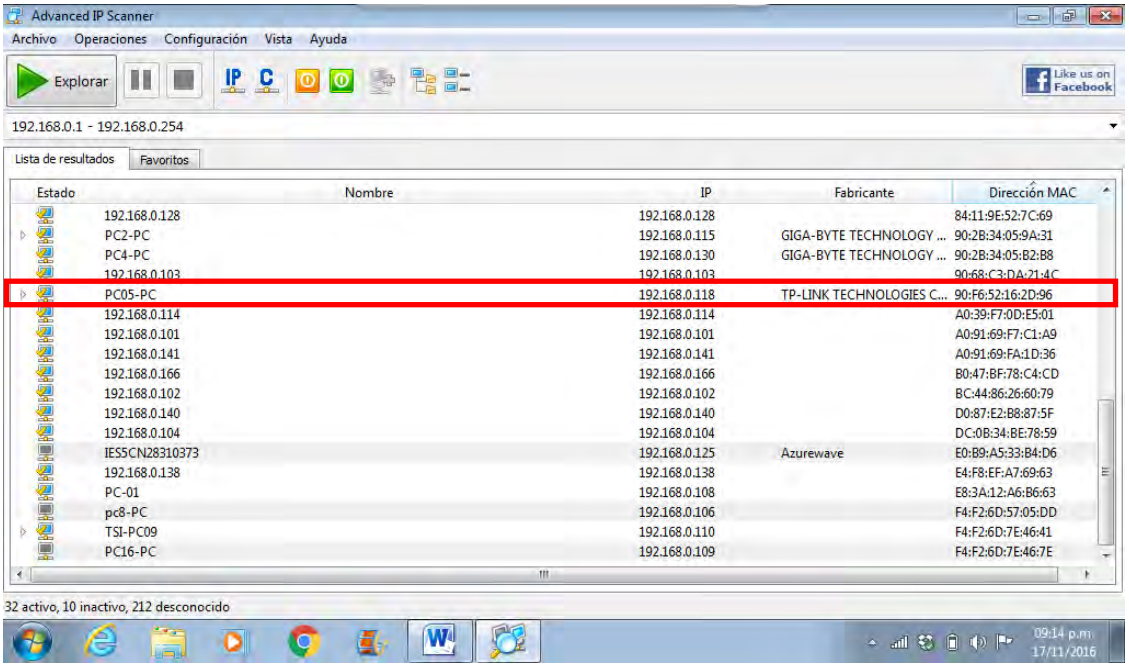
Captura de pantalla N° 2.2.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora **"VictimaPC"** con direccion IP **192.168.0.135**, la cual va a ser la computadora receptora de las acciones ilicitas.



Captura de pantalla N° 2.3: Al ejecutar el programa Wireshark se observa el trafico de los paquetes de datos que circulan por la red en tiempo real

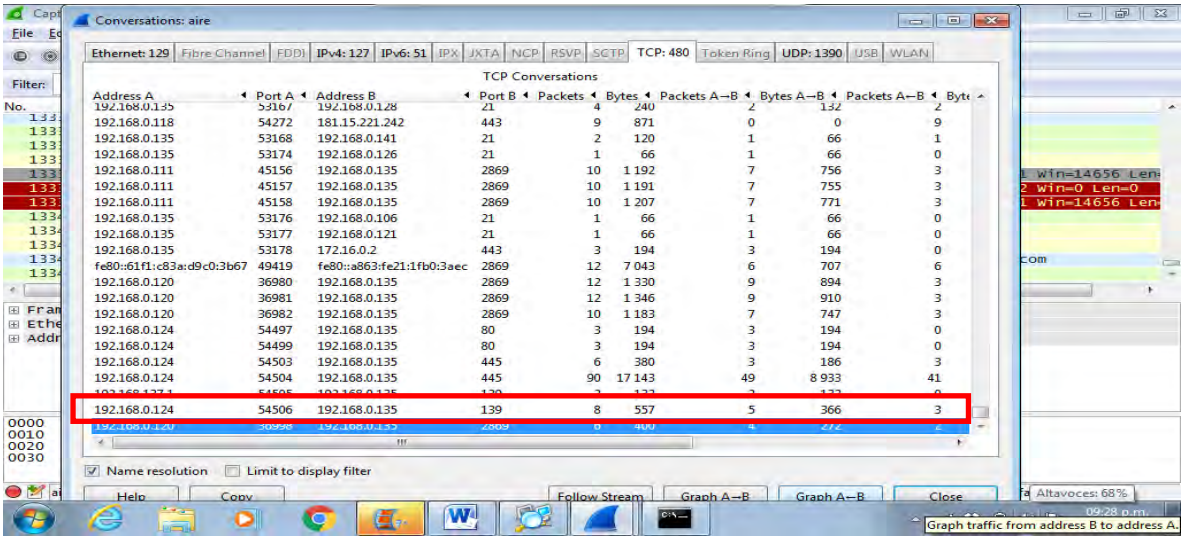


Captura de pantalla N° 2.4: En la ventana “Conversations: aire”, dentro de la pestaña “TCP” se registra comunicación entre la direccion IP **192.168.0.118** con la direccion IP **192.168.0.135.**

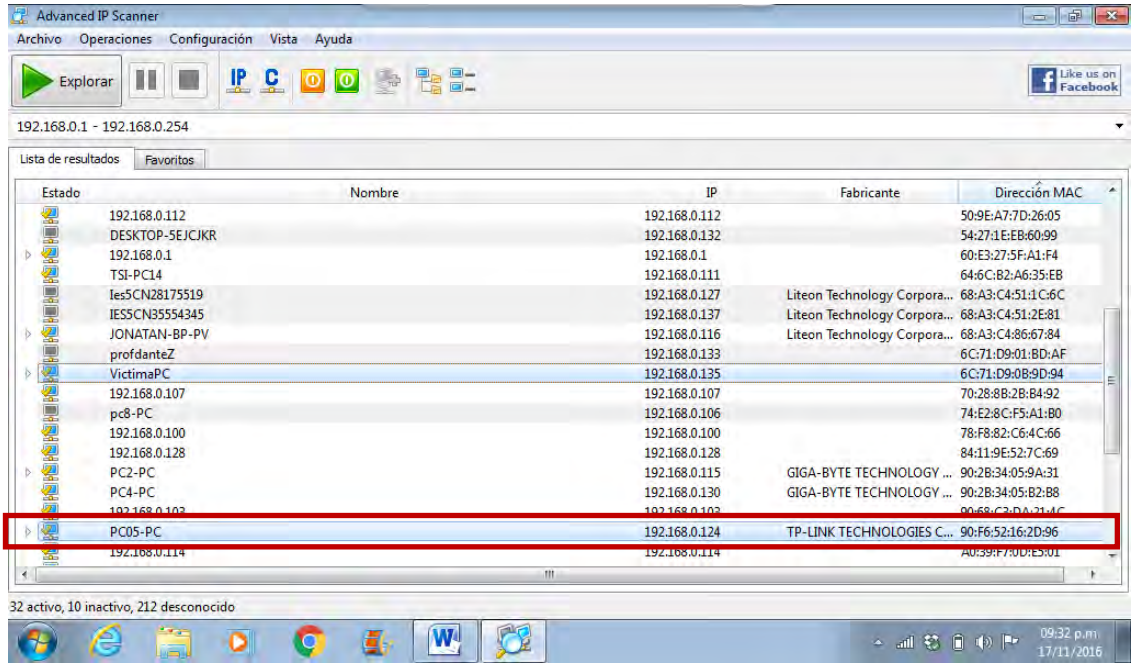


Captura de pantalla N° 2.5: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.118** la asignada al hosts **“PC05-PC”** con direccion MAC **90:F6:52:16:2D:96**.

Desconexión de "PC05- PC": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

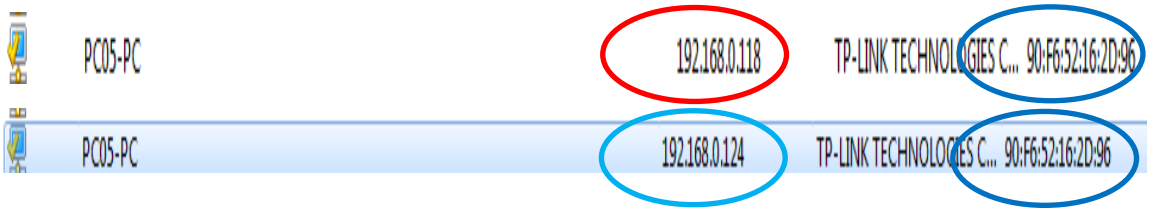


Captura de pantalla N° 2.6: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora "VictimaPC" y una IP hasta ahora desconocida: **192.168.0.124.**



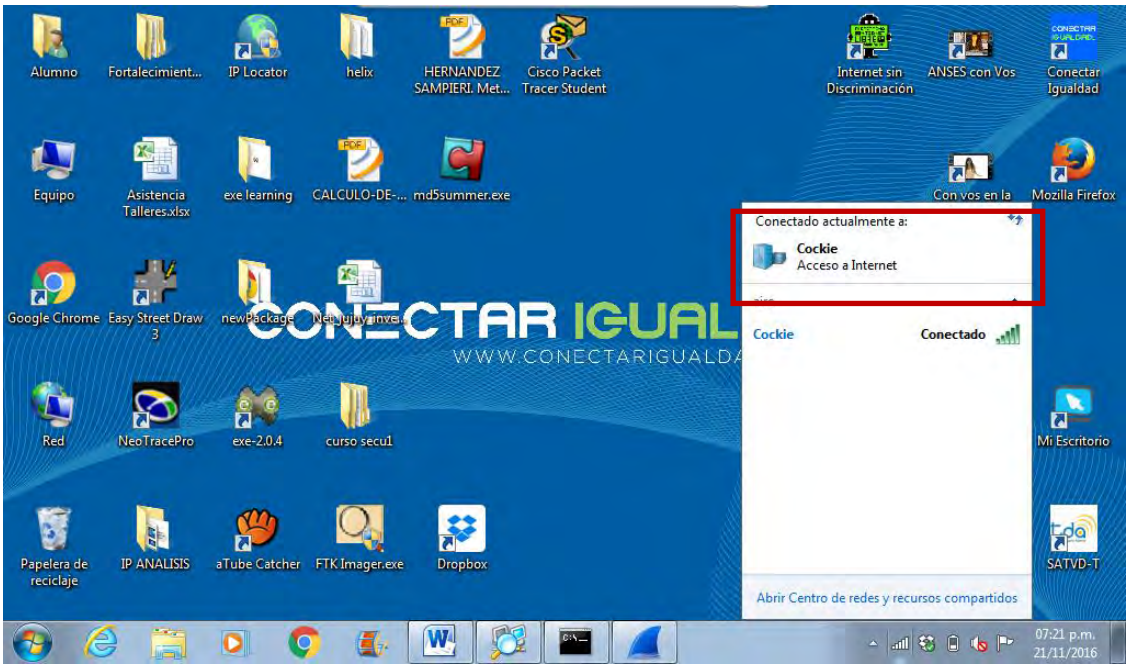
Captura de pantalla N° 2.7: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.124** corresponde al nombre **"PC05-PC"** identificado anteriormente.

CONFIRMACION

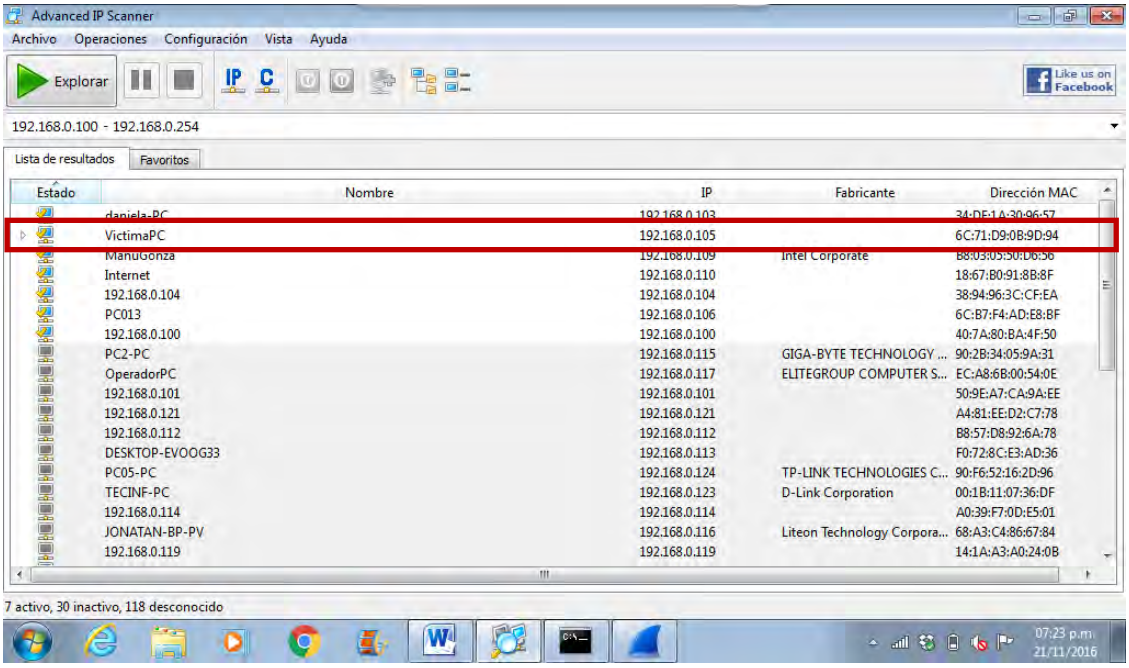


Se observa cambio de la dirección IP de 192.168.0.118 a 192.168.0.124; pero si se compara la dirección MAC que entablo comunicación con la dirección IP "VictimaPC" podemos confirmar que es la misma que en un primer momento: **90:F6:52:16:2D:96**. Correspondiente a una misma computadora.

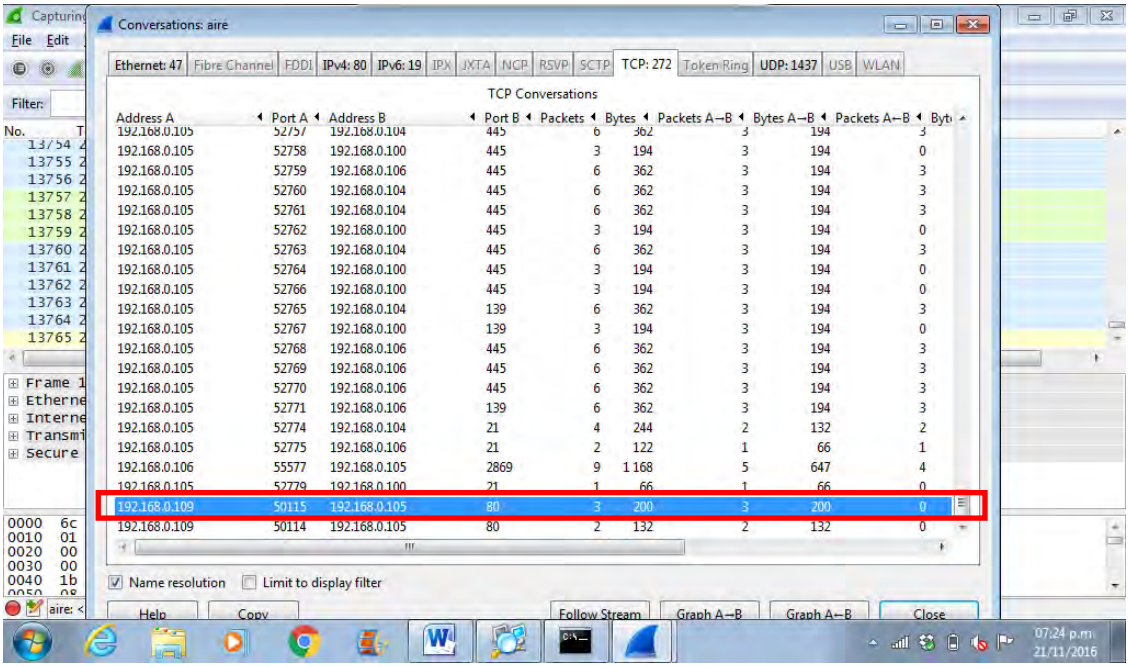
Caso N° 3: 21/11/2016



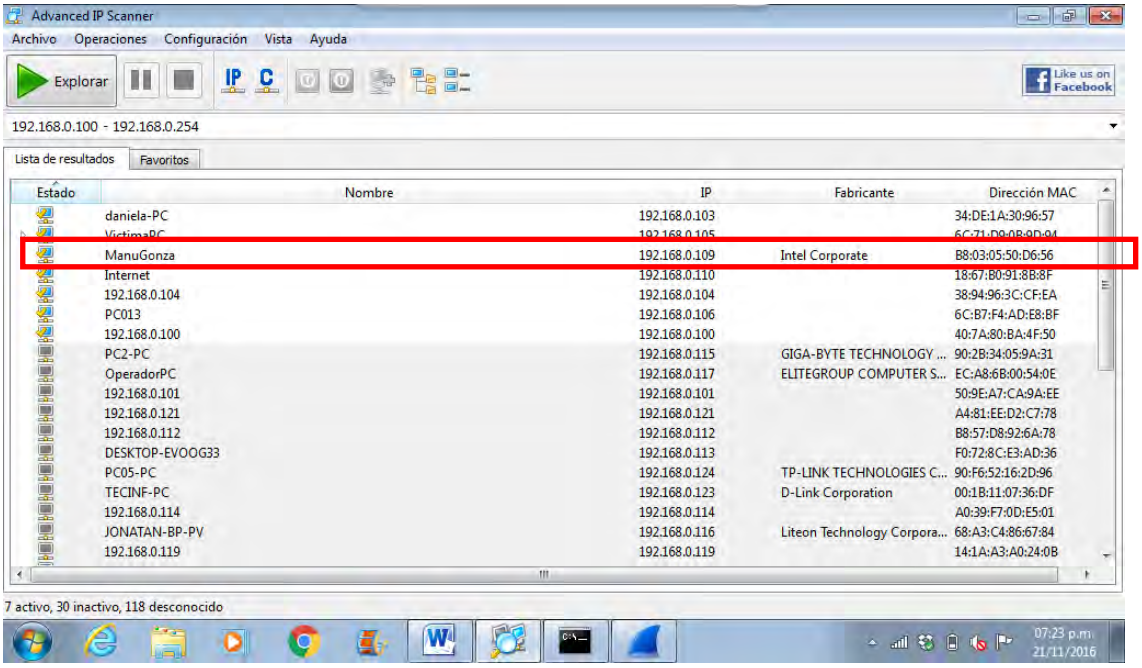
Captura de pantalla N° 3.1: Se establece conexión efectiva con la red "Cockie".



Captura de pantalla N°3.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.105**, la cual va a ser la computadora receptora de las acciones ilicitas.

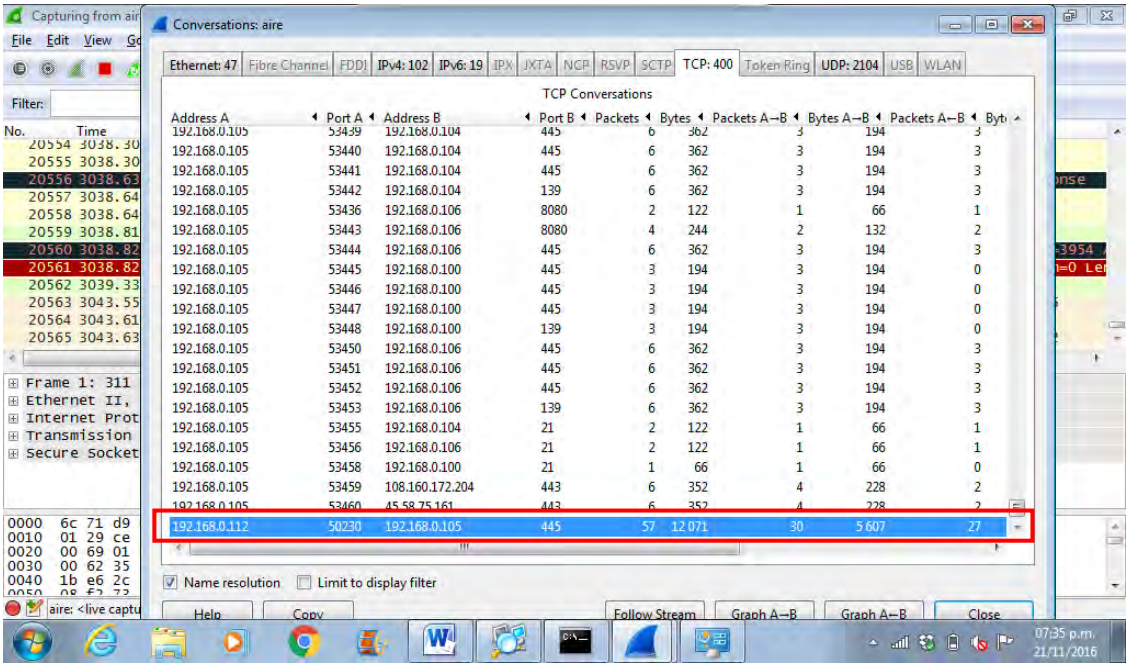


Captura de pantalla N° 3.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.109** con la direccion IP **192.168.0.105**.

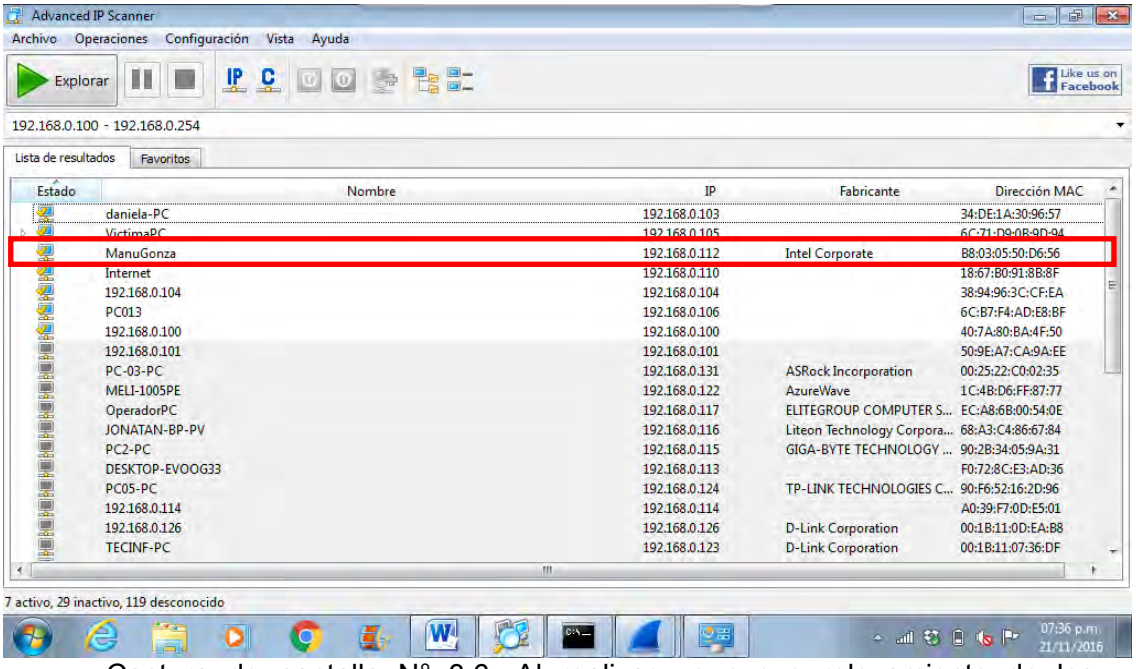


Captura de pantalla N° 3.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.109** la asignada al hosts **"ManuGonza"** con direccion MAC **B8:03:05:50:D6:56**.

Desconexión del hosts “ManuGonza”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

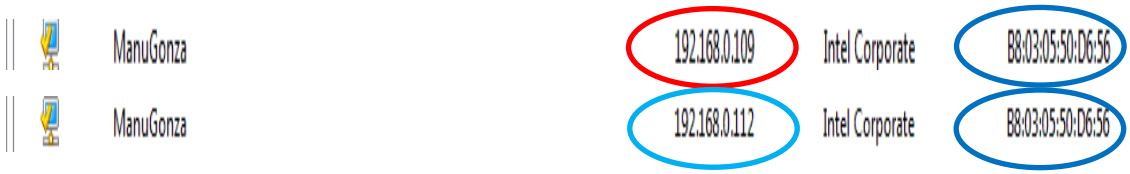


Captura de pantalla N° 3.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora “VictimaPC” y una IP hasta ahora desconocida: **192.168.0.112**.



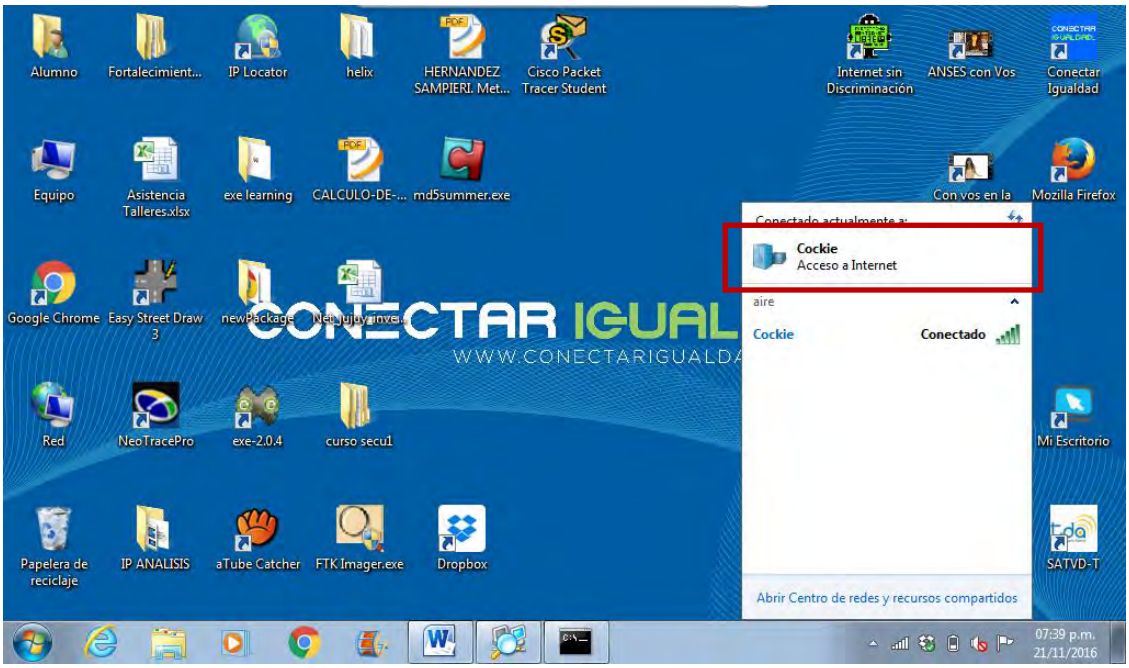
Captura de pantalla N° 3.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.112** corresponde al nombre **“ManuGonza”** identificado anteriormente.

CONFIRMACIÓN:

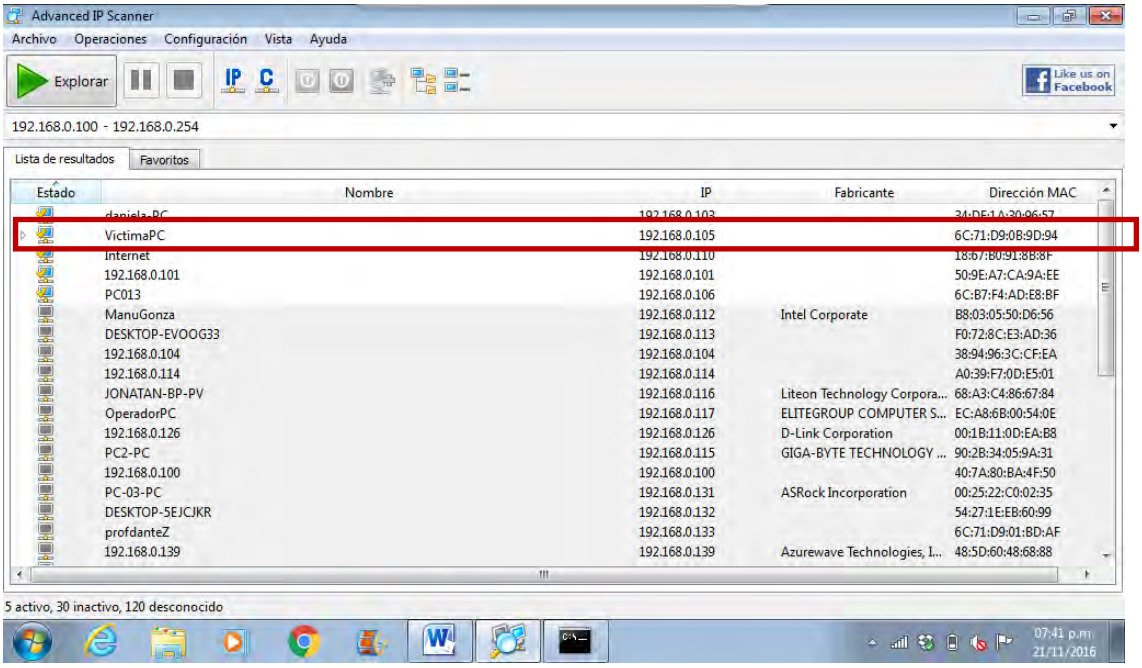


Se observa cambio de la dirección IP de 192.168.0.109 a 192.168.0.112; pero si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento**:** **B8:03:05:50:D6:56**. Correspondiente a una misma computadora.

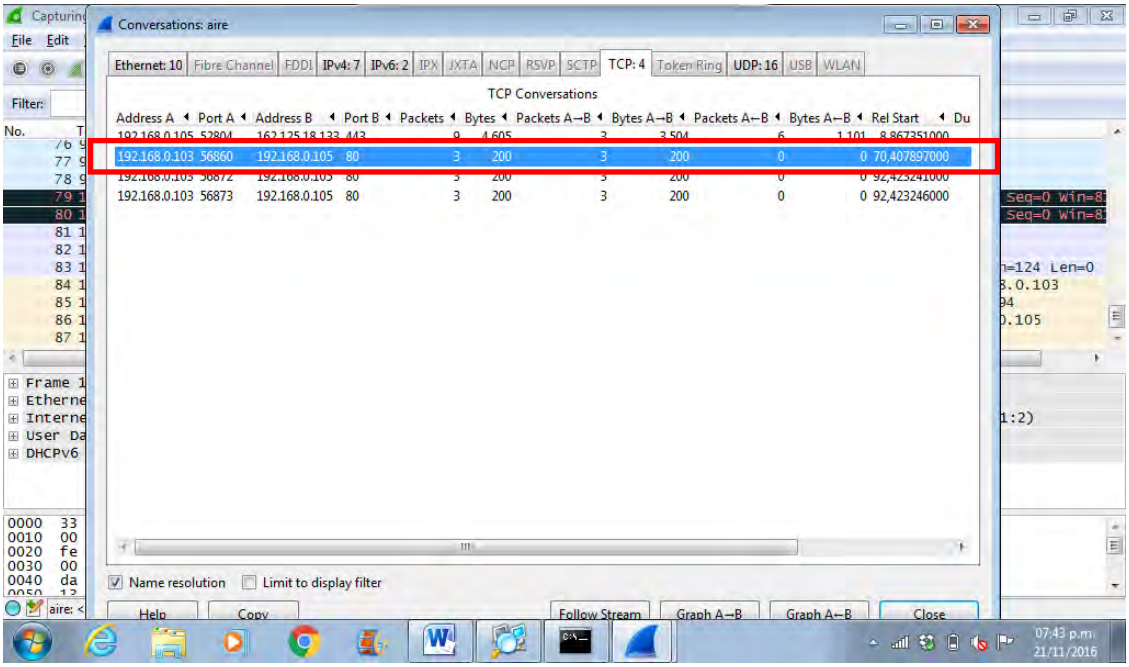
Caso N° 4 : 21/11/16



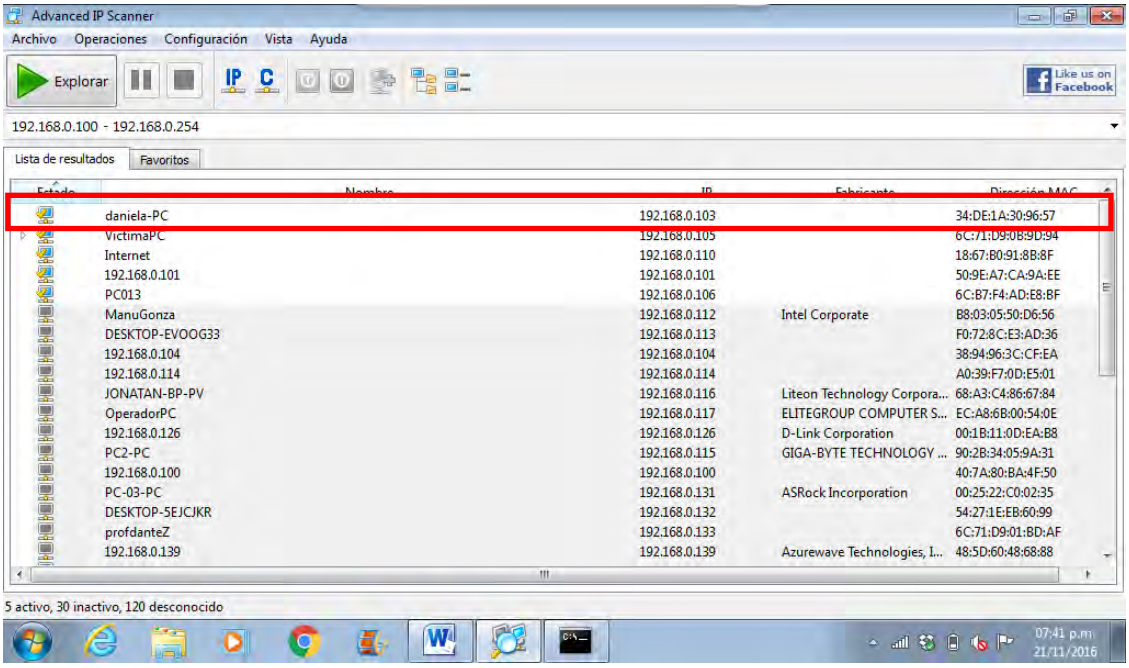
Captura de pantalla N° 4.1: Se establece conexión efectiva con la red "Cockie".



Captura de pantalla N° 4.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.105**, la cual va a ser la computadora receptora de las acciones ilicitas.

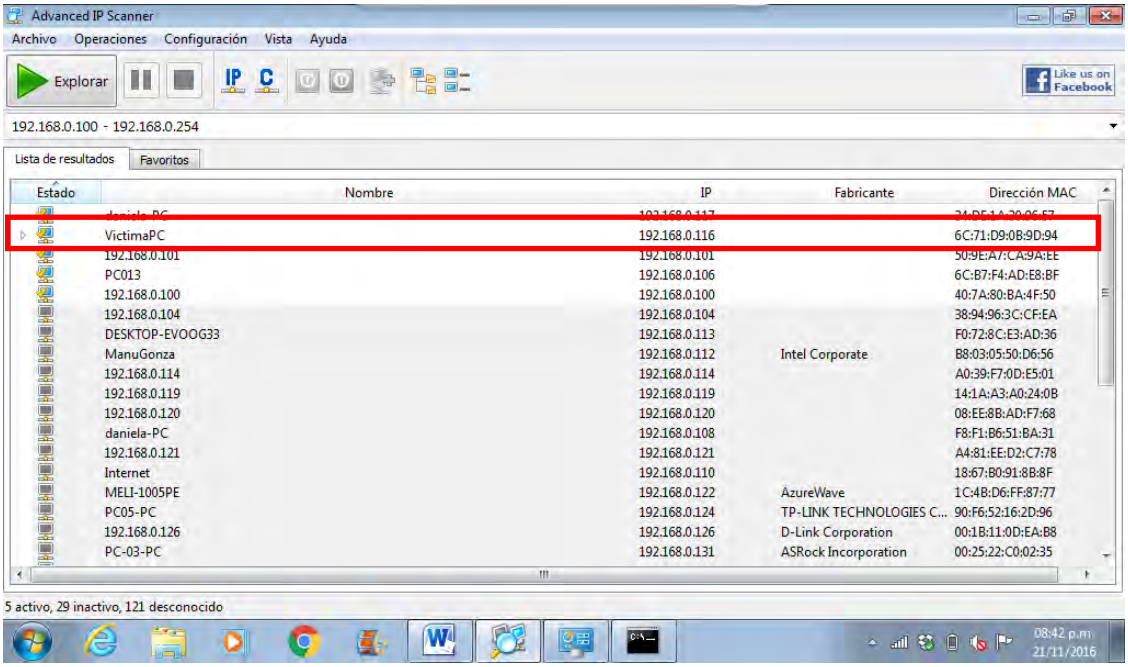


Captura de pantalla N° 4.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.103** con la direccion IP **192.168.0.105**.

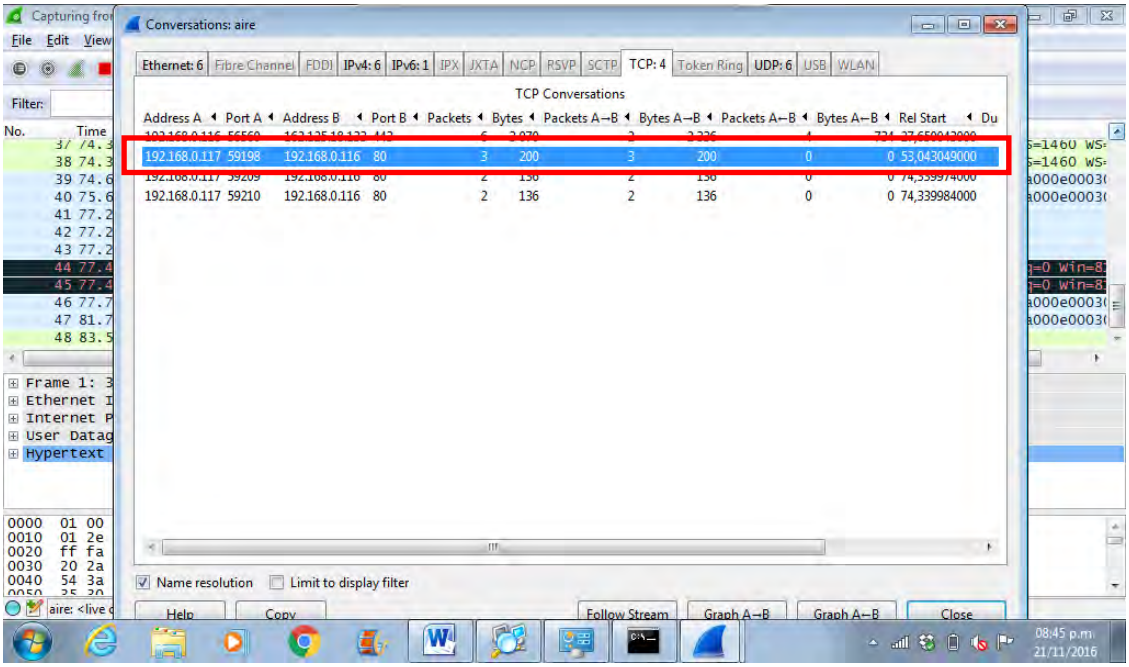


Captura de pantalla N° 4.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.103** la asignada al hosts **"daniela-PC"** con direccion MAC **34:DE:1A:30:96:57**.

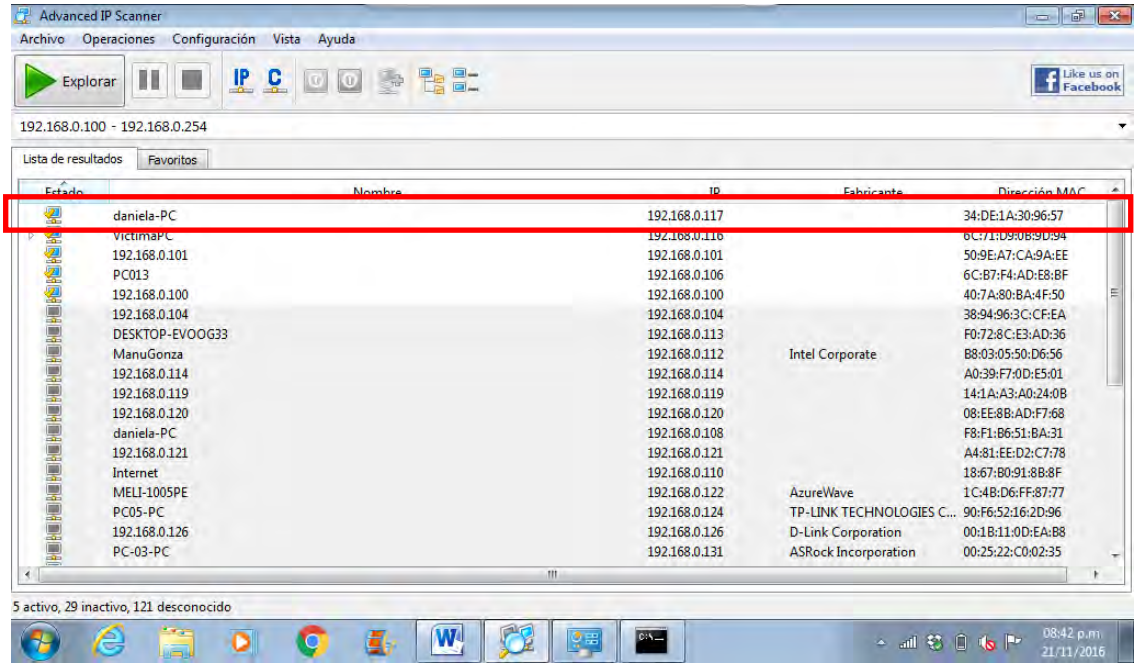
Desconexión del hosts “Daniela-PC”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte. En este punto debido a inclemencias climáticas que acaecían al momento de realizar el caso, se produjo una baja en el suministro eléctrico produciendo el reinicio del Router encargado de la red; reasignando las direcciones IP a cada dispositivo conectado.



Captura de pantalla N° 4.5: Se realizo un nuevo relevamiento de los dispositivos conectados a la red, posterior al reinicio del Router. Se identifica nuevamente que la computadora “VictimaPC” ahora posee como dirección IP **192.168.0.116.**



Captura de pantalla N° 4.6: Reiniciando el programa Wireshark se puede observar una nueva comunicación entre la dirección IP de la computadora victima (192.168.0.116) y una IP hasta ahora desconocida: **192.168.0.117.**

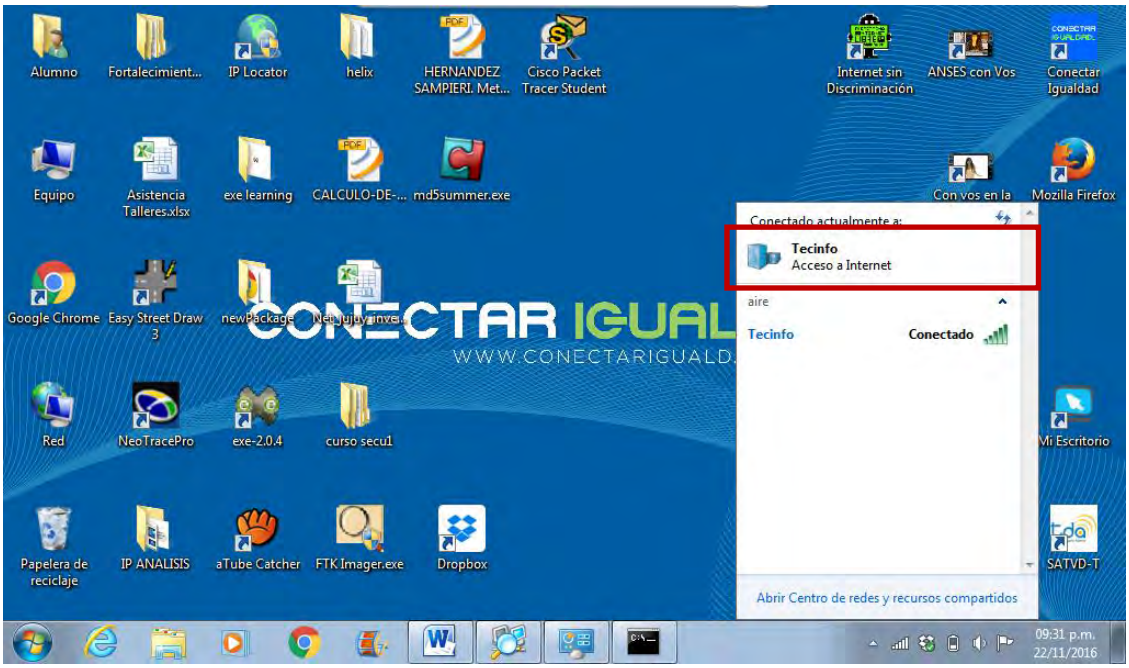


Captura de pantalla N° 4.7: Al realizar la búsqueda de la dirección IP desconocida en el relevamiento anterior, se logra determinar que la dirección IP **192.168.0.117** corresponde al nombre **"daniela-PC"** identificado anteriormente.

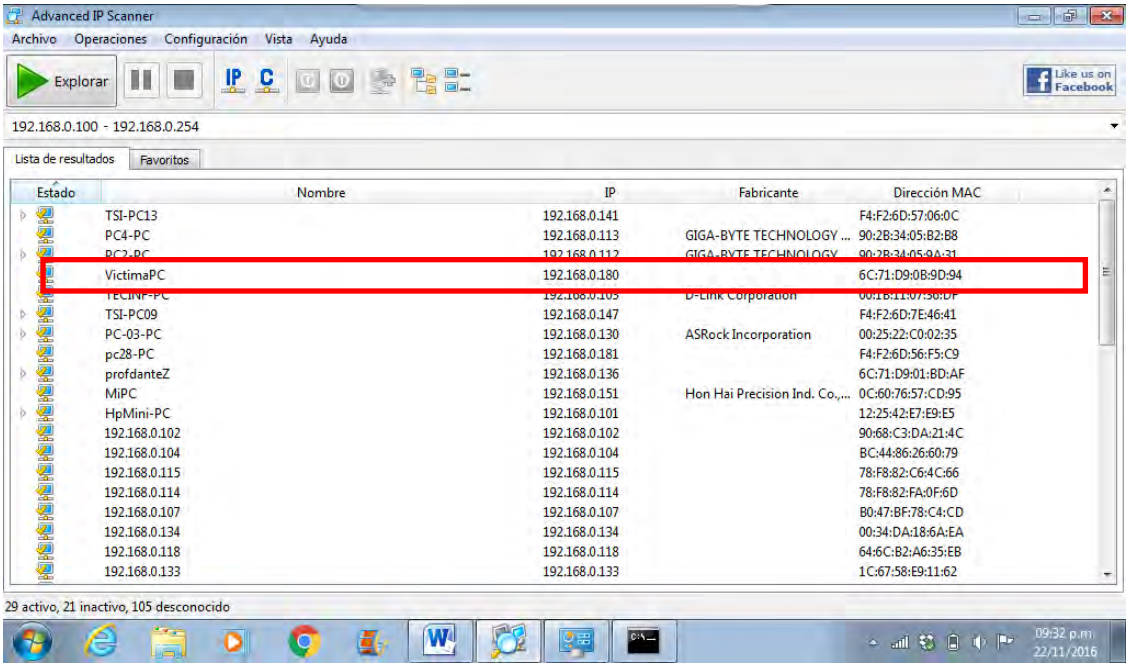
CONFIRMACIÓN:

Se observa cambio de la dirección IP de 192.168.0.103 a 192.168.0.117; pero si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento: **34:DE:1A:30:96:57** . Correspondiente a una misma computadora.

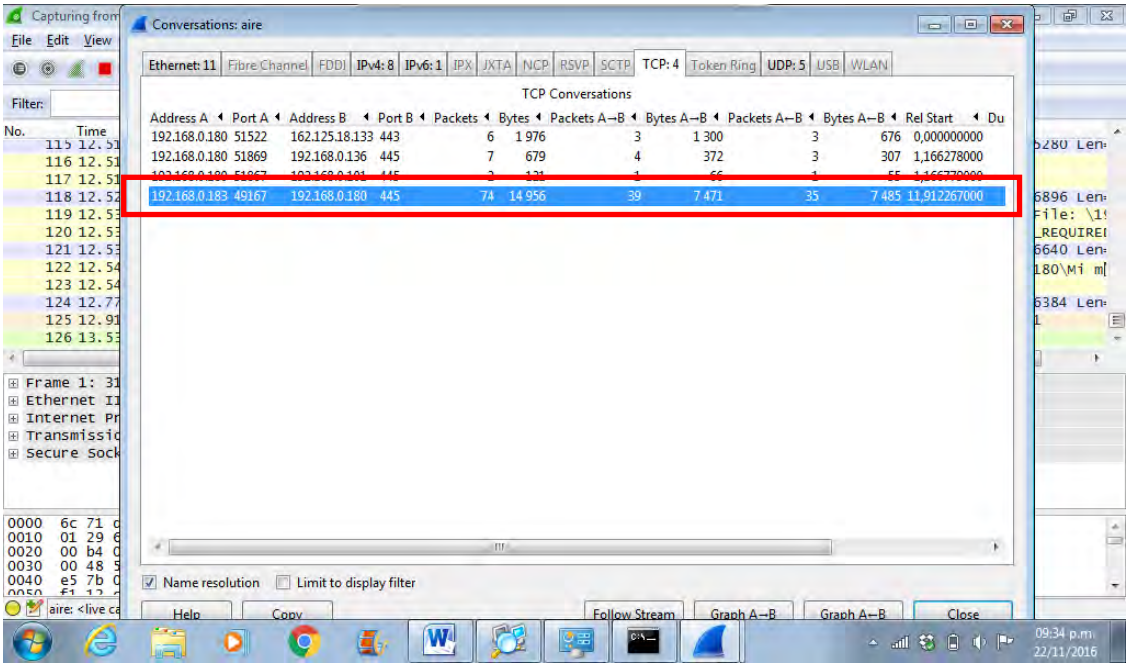
Caso N° 5: 22/11/16



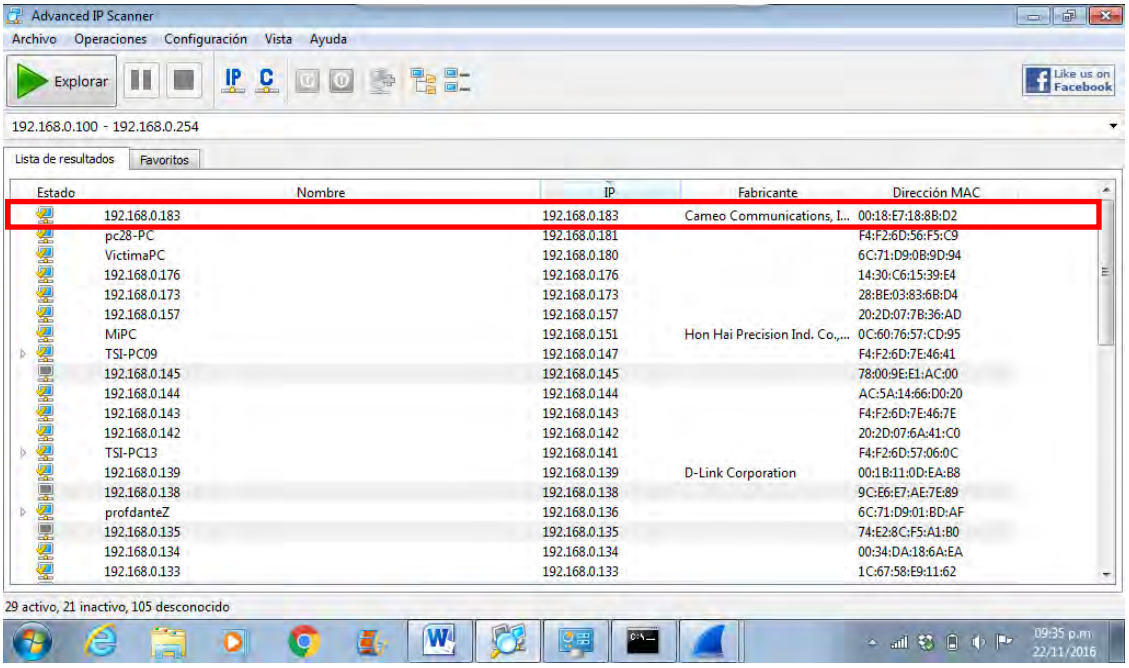
Captura de pantalla N° 5.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 5.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.180**, la cual va a ser la computadora receptora de las acciones ilicitas.

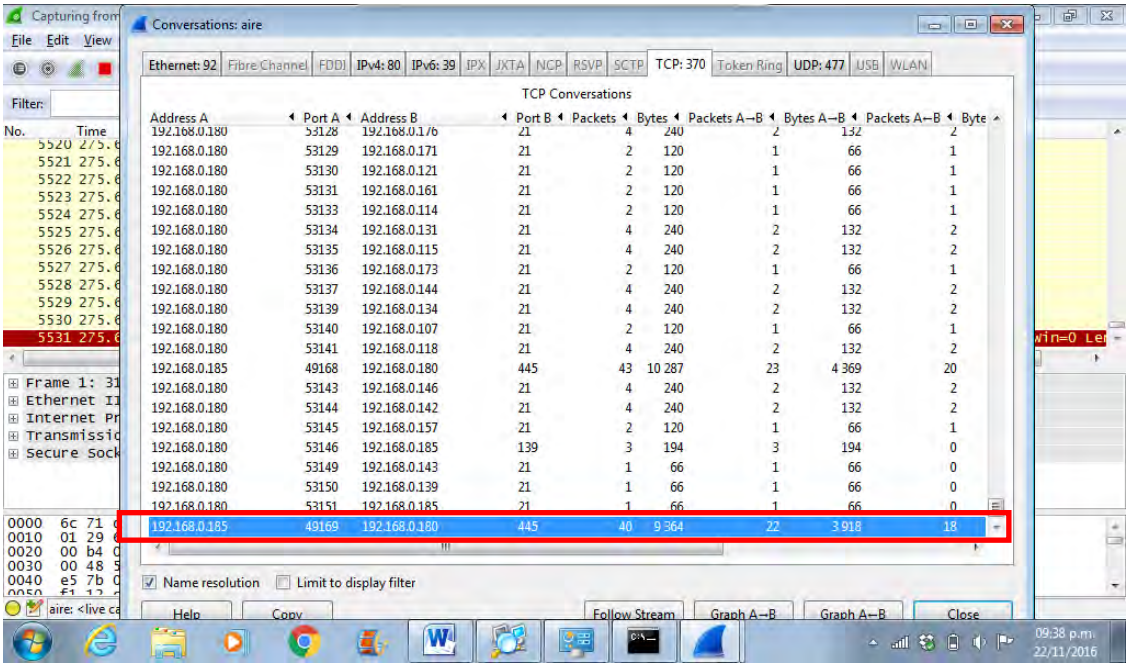


Captura de pantalla N° 5.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.183** con la direccion IP **192.168.0.180**.

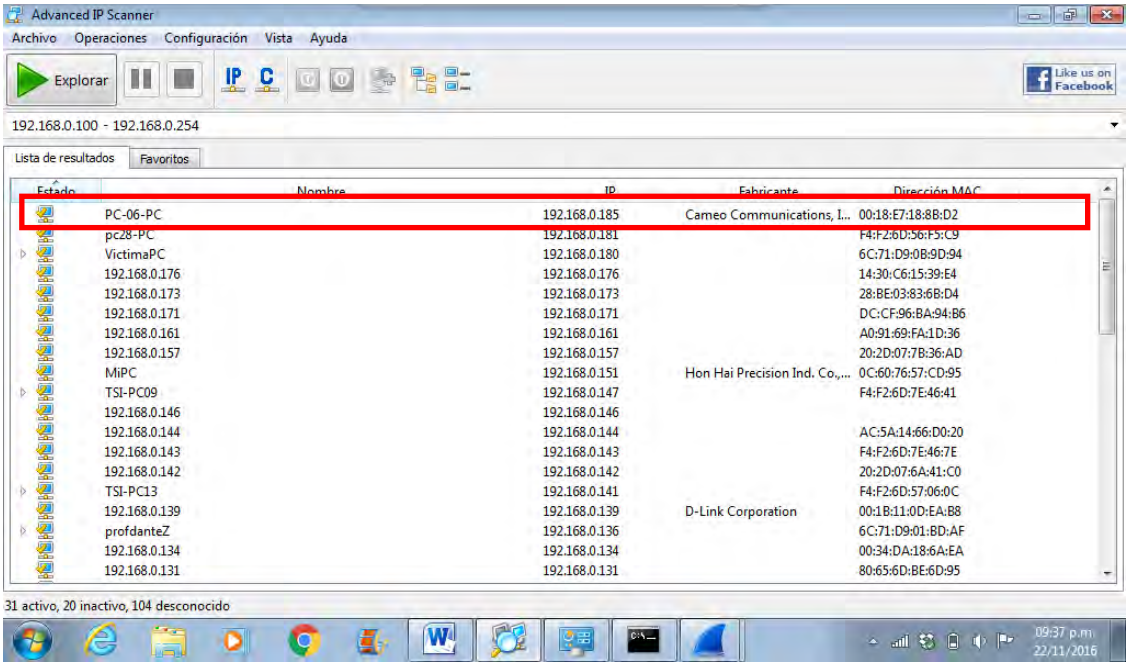


Captura de pantalla N° 5.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.183** la asignada al hosts "**192.168.0.183**" con direccion MAC **00:18:E7:18:8B:D2**.

Desconexion de “192.168.0.183”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

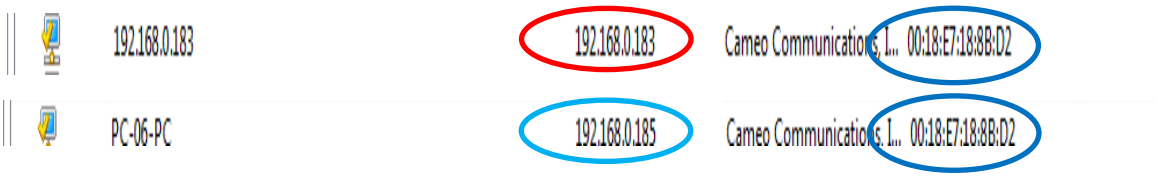


Captura de pantalla N° 5.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora “VictimaPC” y una IP hasta ahora desconocida: **192.168.0.185.**



Captura de pantalla N° 5.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.185** corresponde al nombre **“PC-06-PC”**

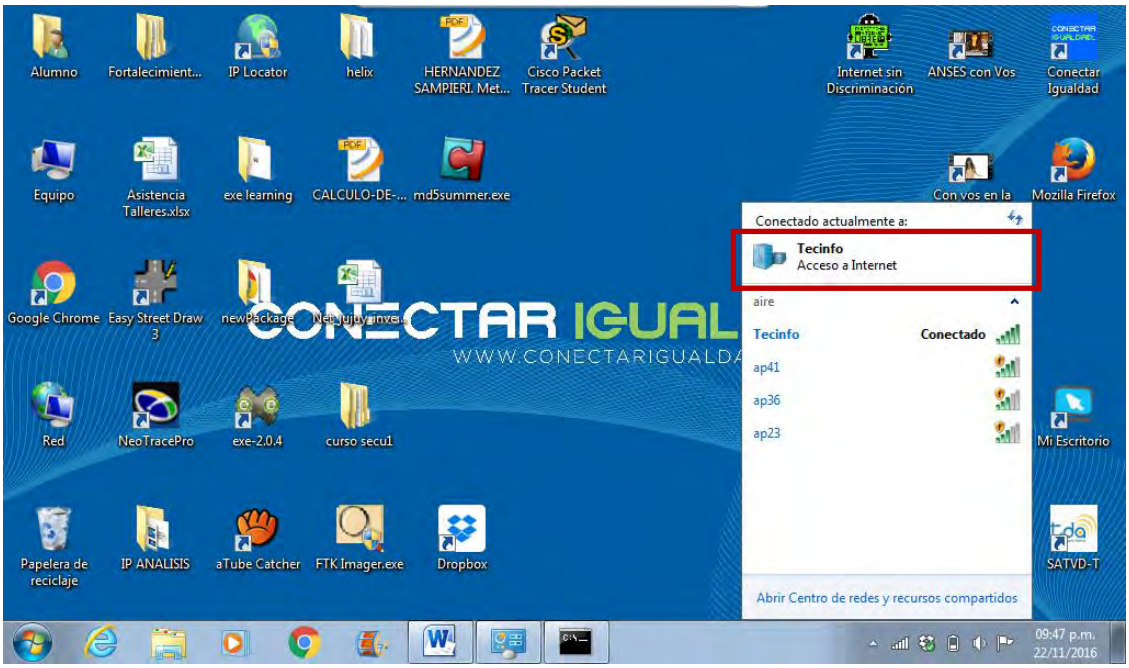
CONFIRMACION



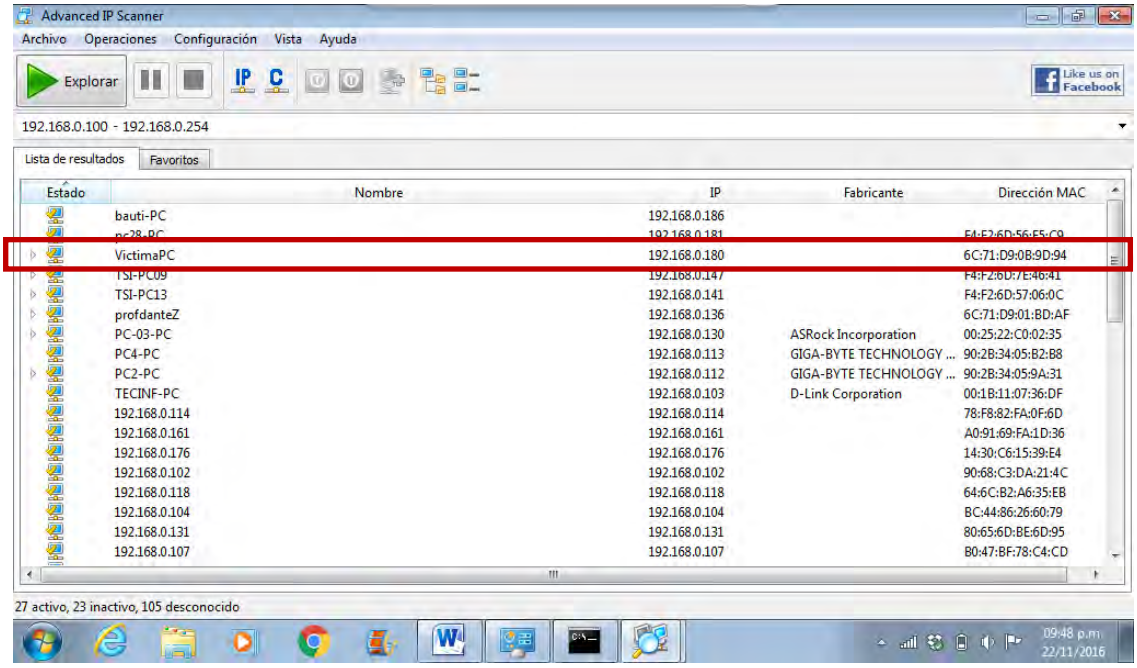
Se observa cambio de la dirección IP de 192.168.0.183 a 192.168.0.185; pero que si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC anteriormente podemos confirmar que es la misma que en un primer momento: **00:18:E7:18:8B:D2**

.

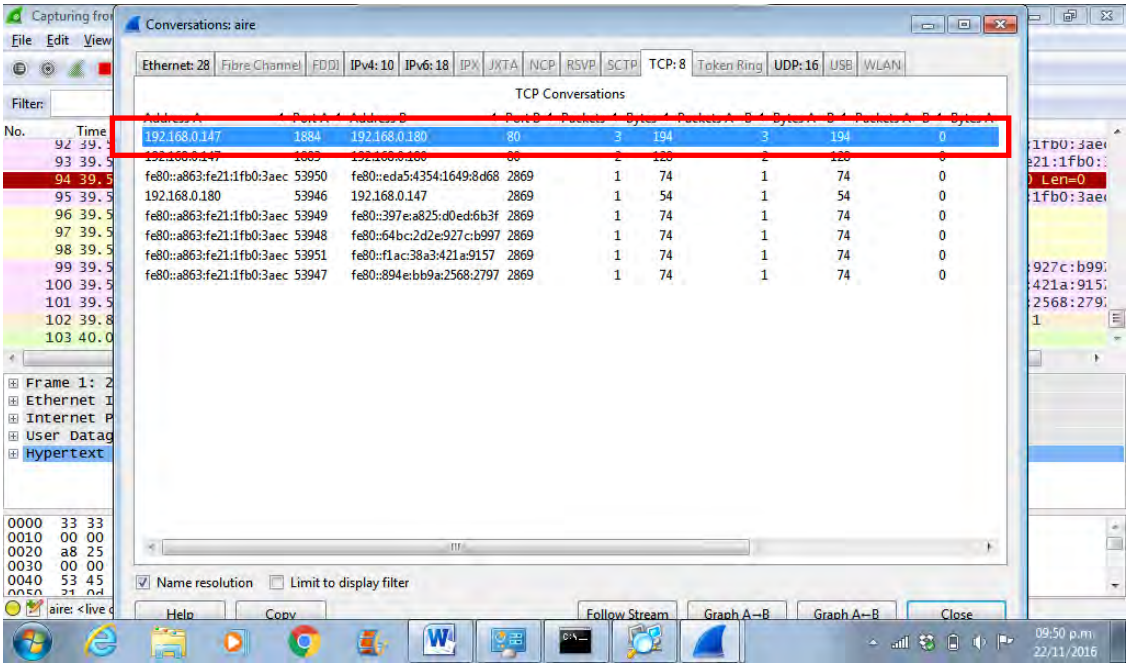
CASO N° 6: 22/11/16



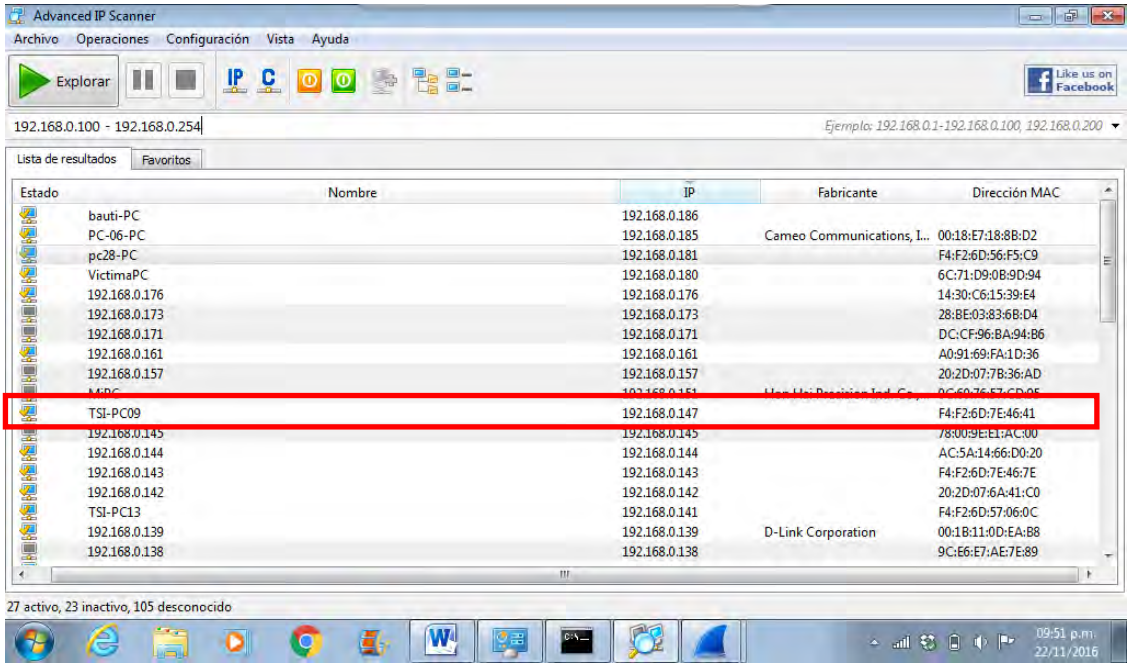
Captura de pantalla N° 6.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 6.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.180**, la cual va a ser la computadora receptora de las acciones ilicitas.

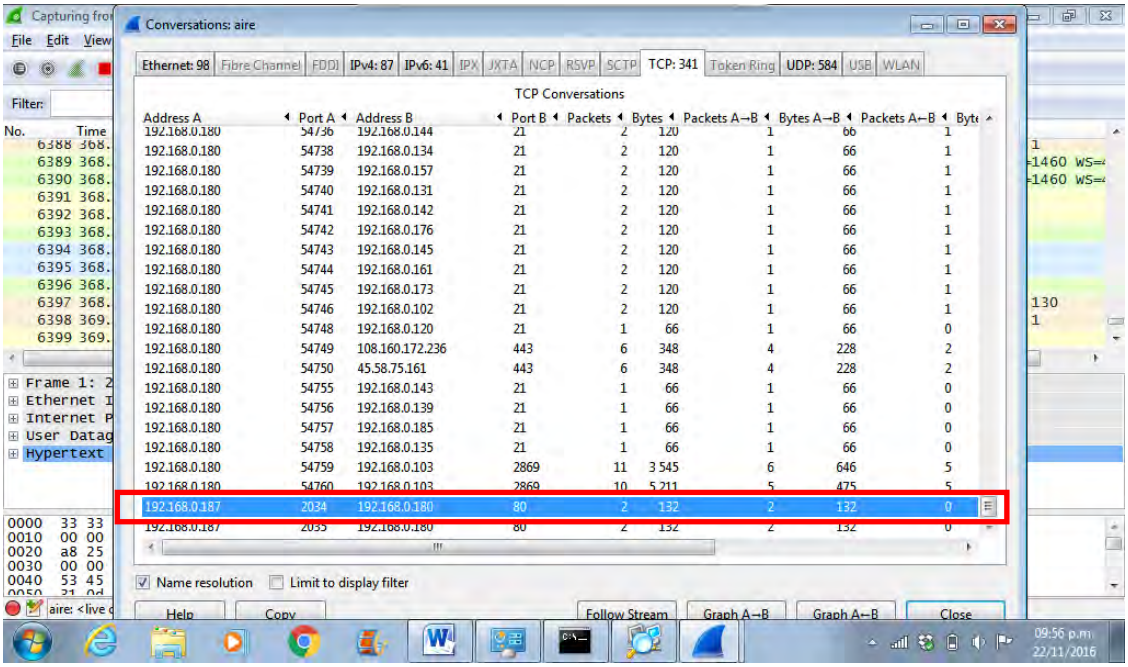


Captura de pantalla N° 6.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.147** con la direccion IP **192.168.0.180**

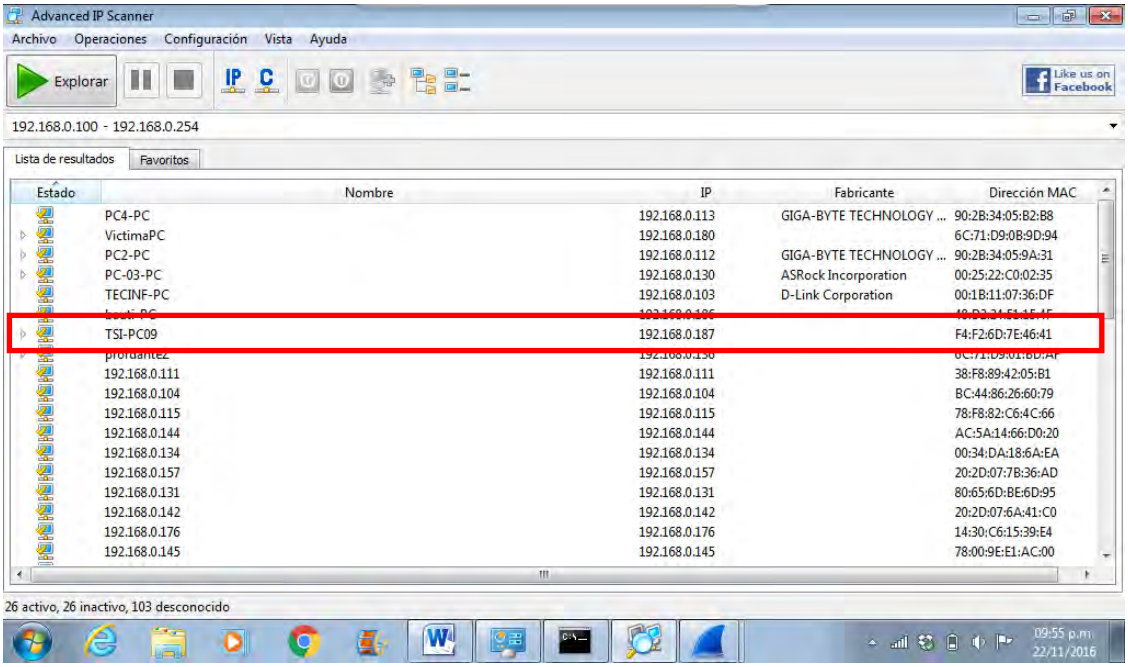


Captura de pantalla N° 6.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.147** la asignada al hosts "**TSI-PC09"** con direccion MAC **F4:F2:6D:7E:46:41.**

Desconexión de "TSI-PC09": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

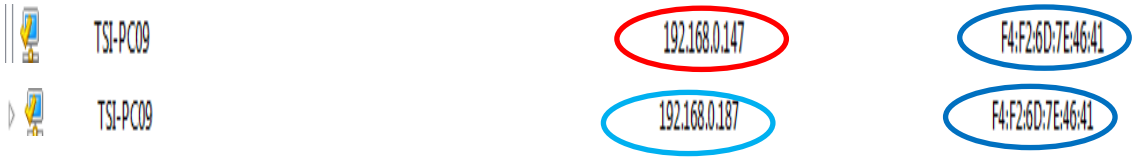


Captura de pantalla N° 6.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora "VictimaPC" y una IP hasta ahora desconocida: **192.168.0.187.**



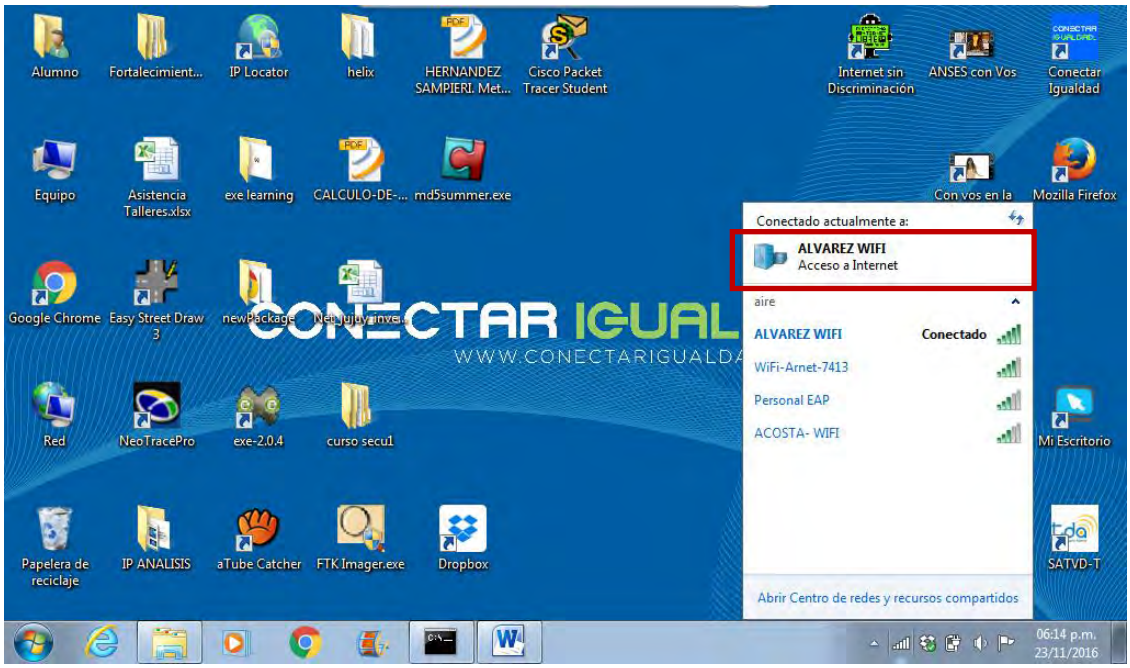
Captura de pantalla N° 6.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.187** corresponde al nombre "**TSI-PC09"** identificado anteriormente.

Confirmación

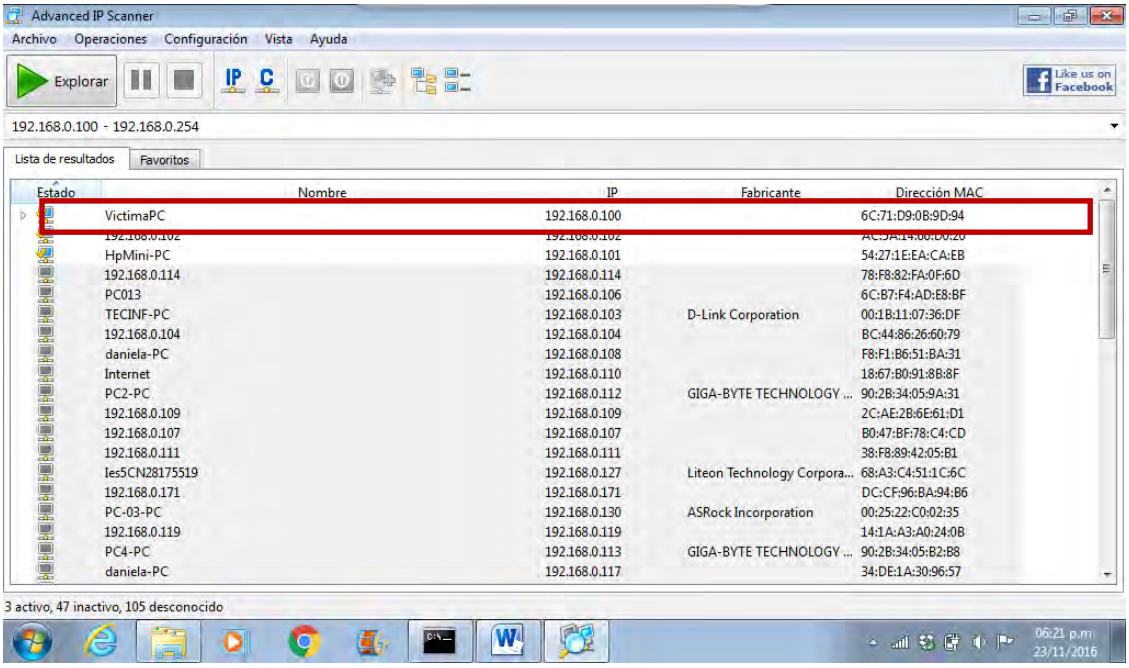


. Se observa cambio de la dirección IP de 192.168.0.147 a 192.168.0.187; pero si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento: **F4:F2:6D:7E:46:41.** Correspondiente a una misma computadora.

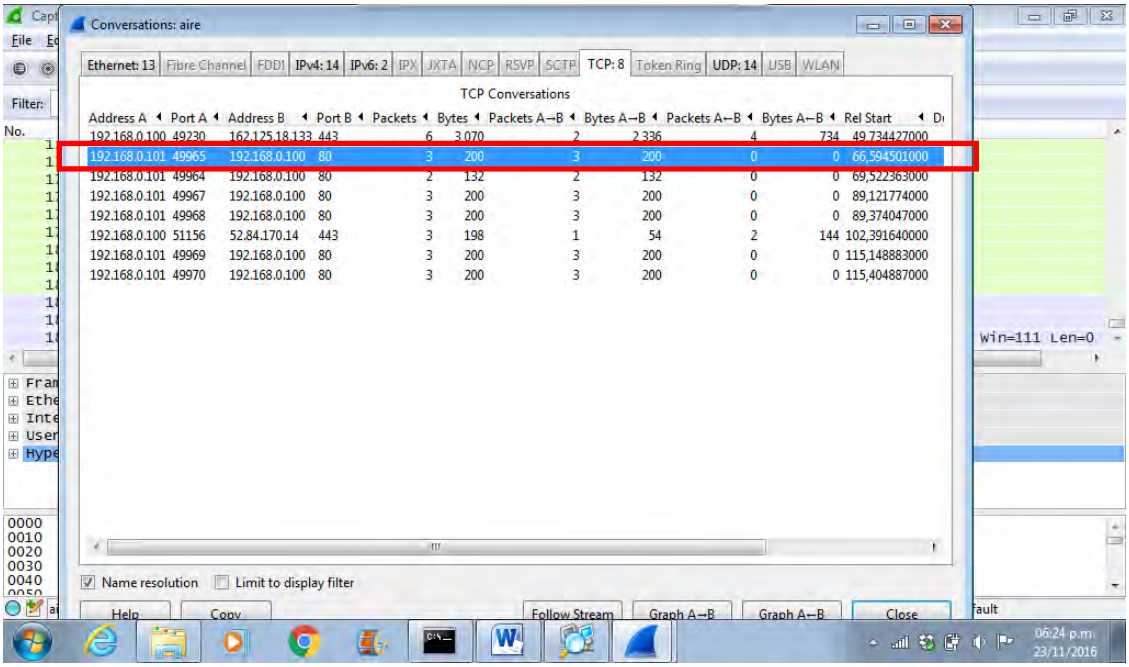
Caso N° 7: 23/11/16



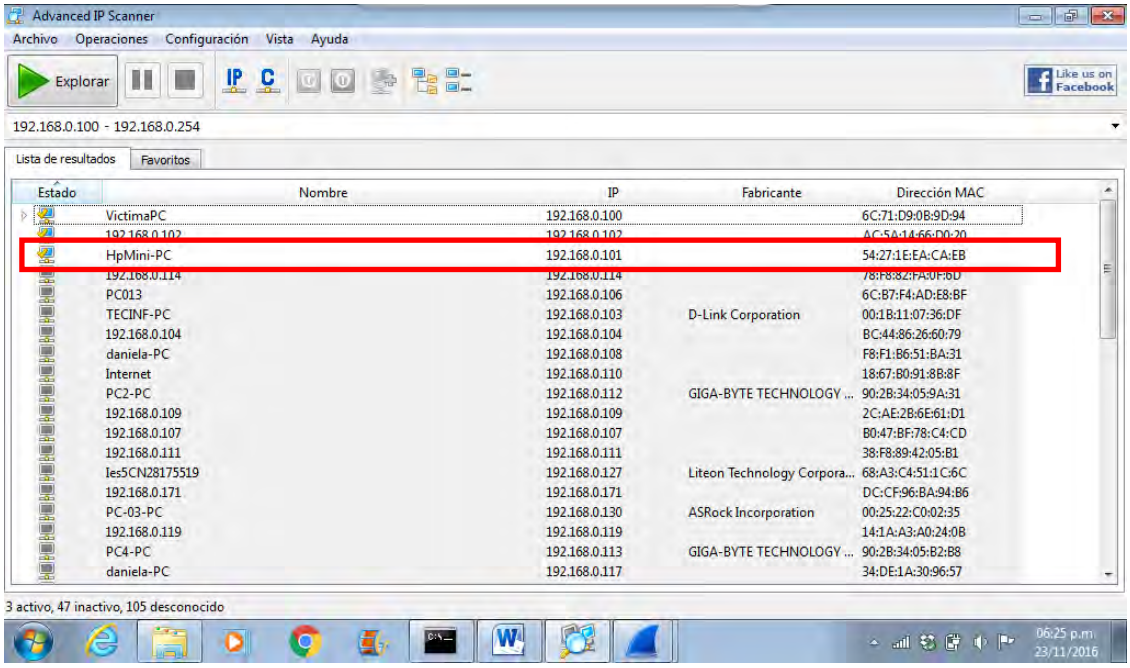
Captura de pantalla N° 7.1: Se establece conexión efectiva con la red "ALVAREZ WIFI".



Captura de pantalla N° 7.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.100**, la cual va a ser la computadora receptora de las acciones ilicitas.

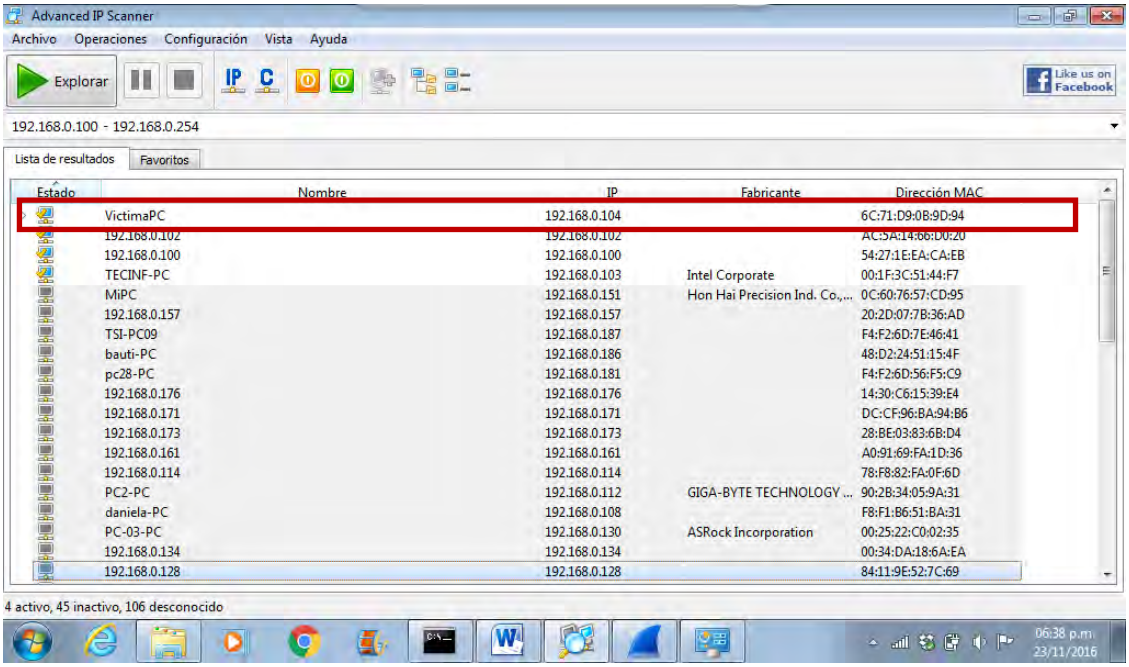


Captura de pantalla N° 7.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.101** con la direccion IP **192.168.0.100.**

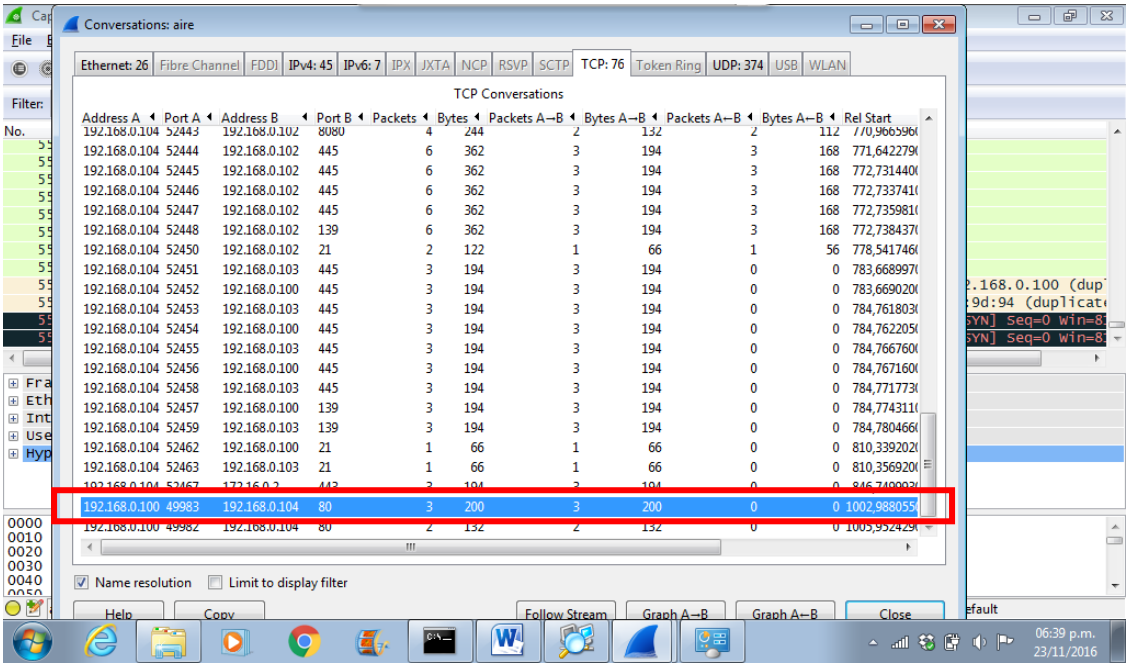


Captura de pantalla N° 7.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.101** la asignada al hosts **"HpMini-PC"** con direccion MAC **54:27:1E:EA:CA:EB**.

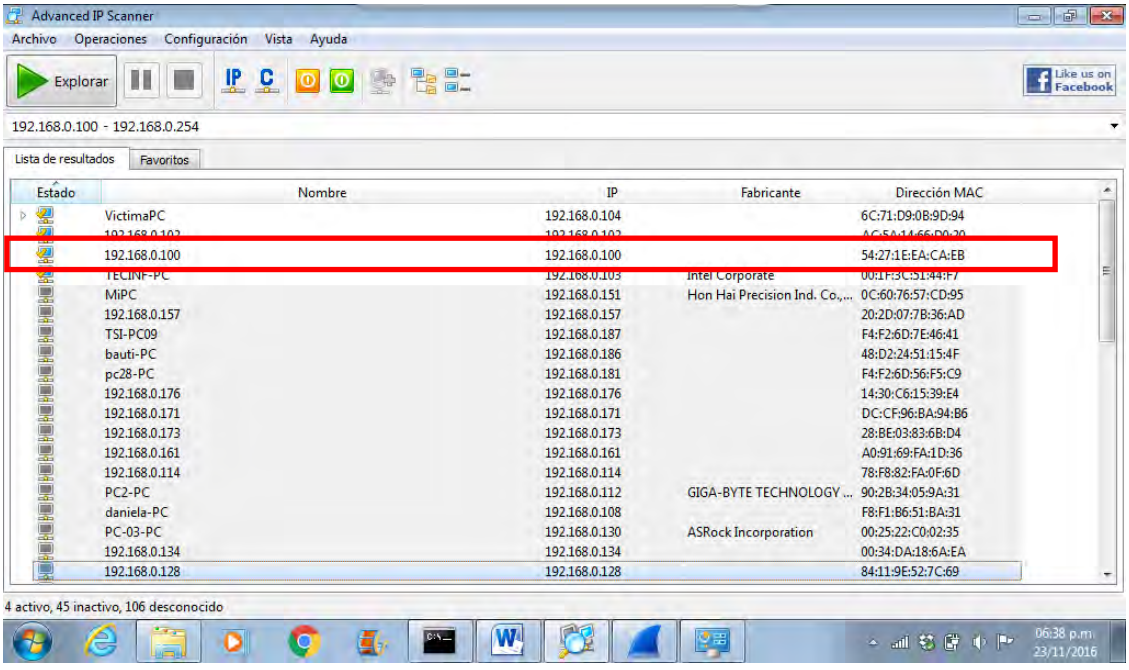
Desconexión del hosts “HpMini-PC”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte. En este punto debido a inclemencias climáticas que acaecían al momento de realizar el caso, se produjo una baja en el suministro eléctrico produciendo el reinicio del Router encargado de la red; reasignando las direcciones IP a cada dispositivo conectado.



Captura de pantalla N° 7.5: Se realizó un nuevo relevamiento de los dispositivos conectados a la red, posterior al reinicio del Router. Se identifica nuevamente que la computadora “VictimaPC” ahora posee como dirección IP **192.168.0.104.**

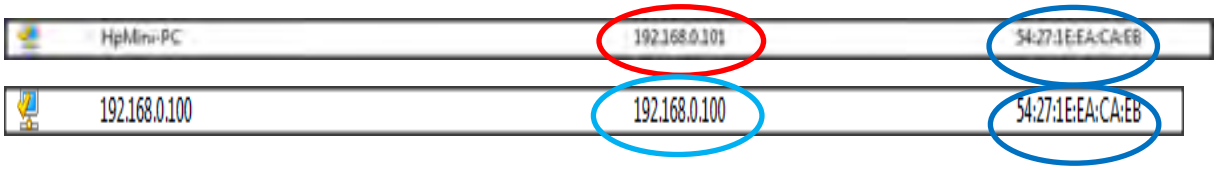


Captura de pantalla N° 7.6: Reiniciando el programa Wireshark se puede observar una nueva comunicación entre la dirección IP de la computadora victima (192.168.0.104) y la dirección IP que presentaba en un primer momento la computadora víctima: **192.168.0.100**



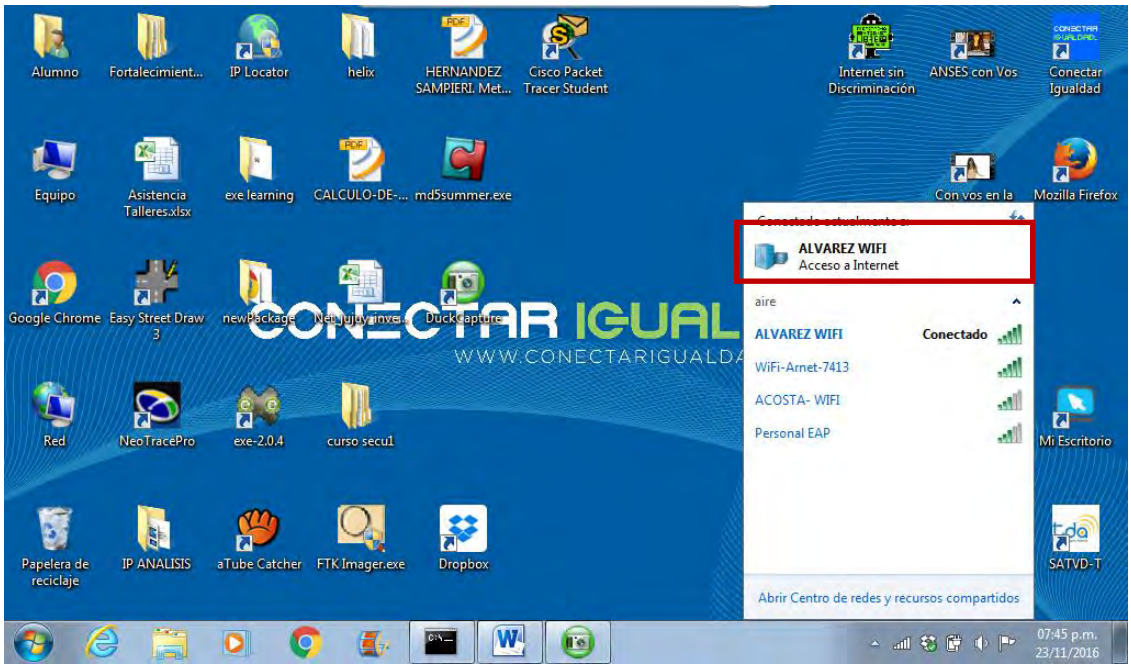
Captura de pantalla N° 7.7: Al realizar la búsqueda de la dirección IP sospechosa en el relevamiento anterior, se logra determinar que la dirección IP **192.168.0.100** corresponde al nombre "**192.168.0.100**"

CONFIRMACIÓN

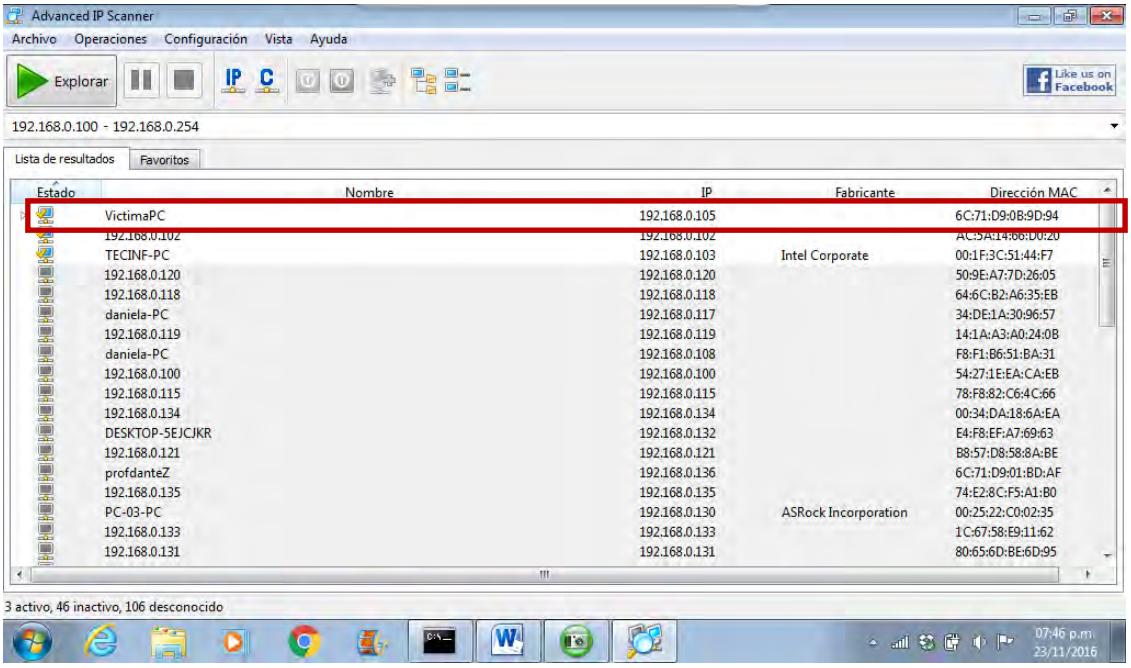


Se observa cambio de la dirección IP de 192.168.0.101 a 192.168.0.100; pero que si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC anteriormente podemos confirmar que se trata de la misma que en un primer momento: **54:27:1E:EA:CA:EB**.

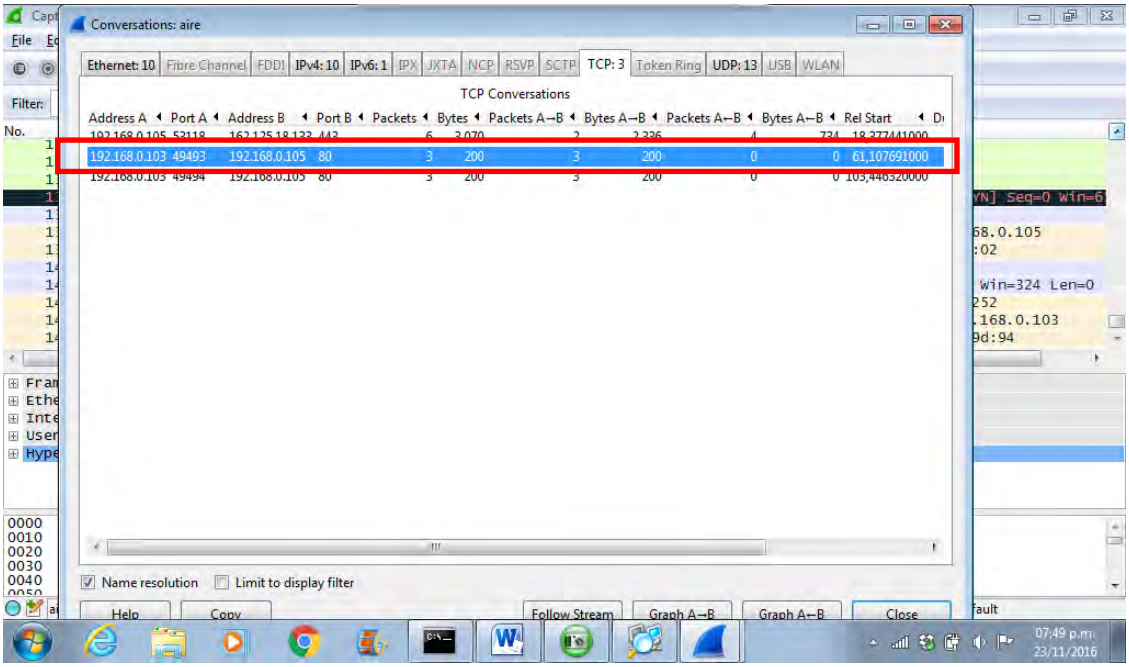
Caso N° 8: 23/11/16



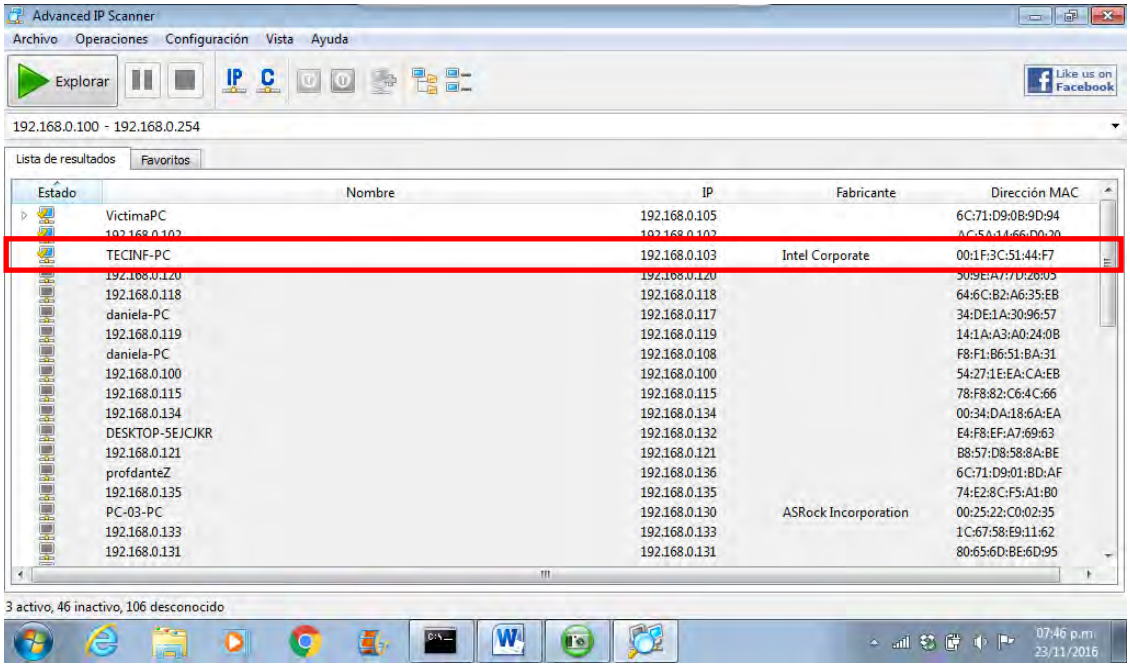
Captura de pantalla N° 8.1: Se establece conexión efectiva con la red "ALVAREZ WIFI".



Captura de pantalla N° 8.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.105**, la cual va a ser la computadora receptora de las acciones ilicitas.

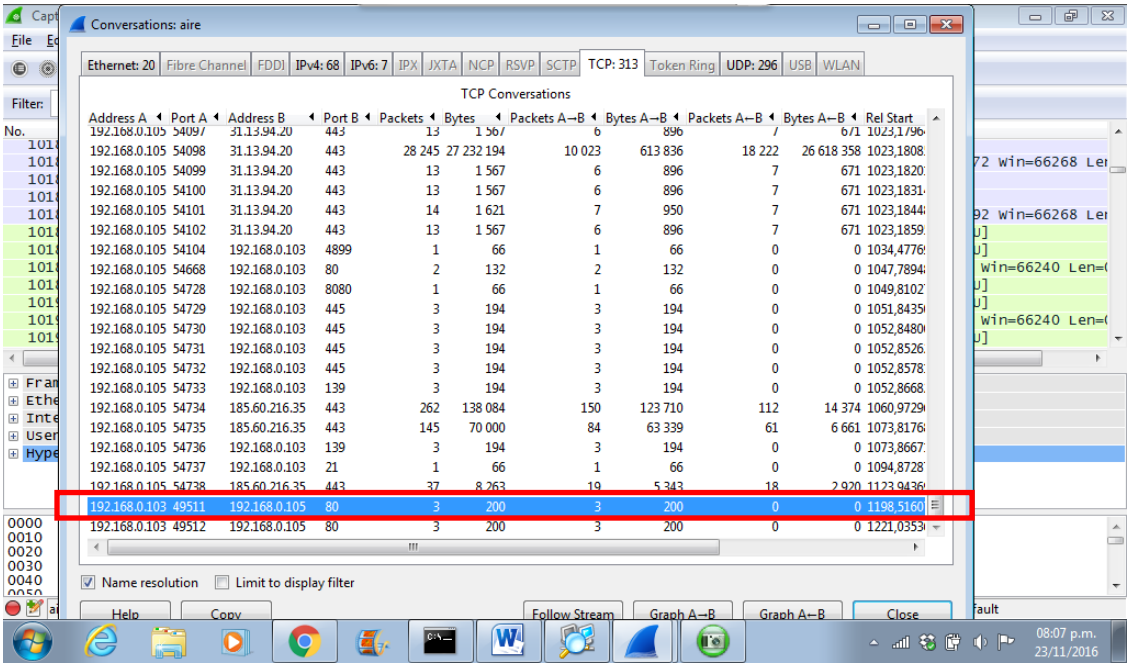


Captura de pantalla N° 8.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.103** con la direccion IP **192.168.0.105**.

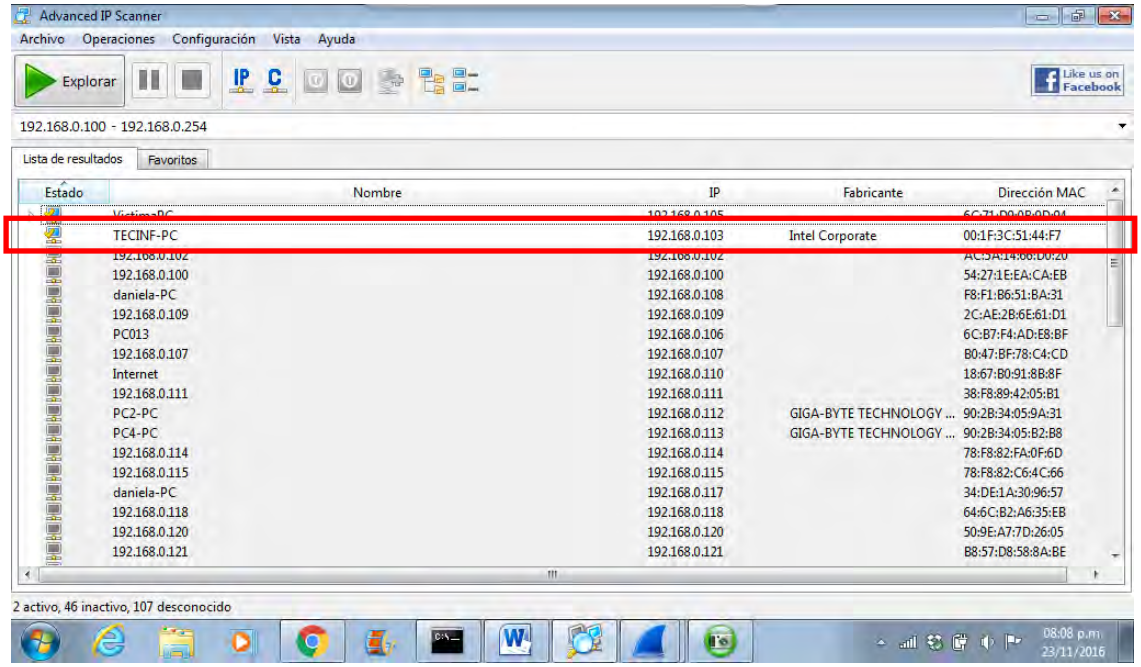


Captura de pantalla N° 8.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.103** la asignada al hosts "**TECINF-PC"** con direccion MAC **00:1F:3C:51:44:F7**.

Desconexión de "TECINF-PC": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

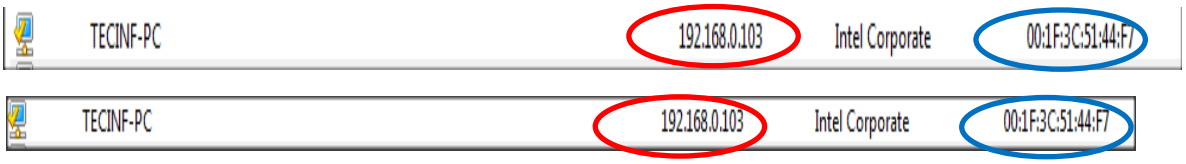


Captura de pantalla N° 8.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora "VictimaPC" como de la sospechosa: **192.168.0.103**.



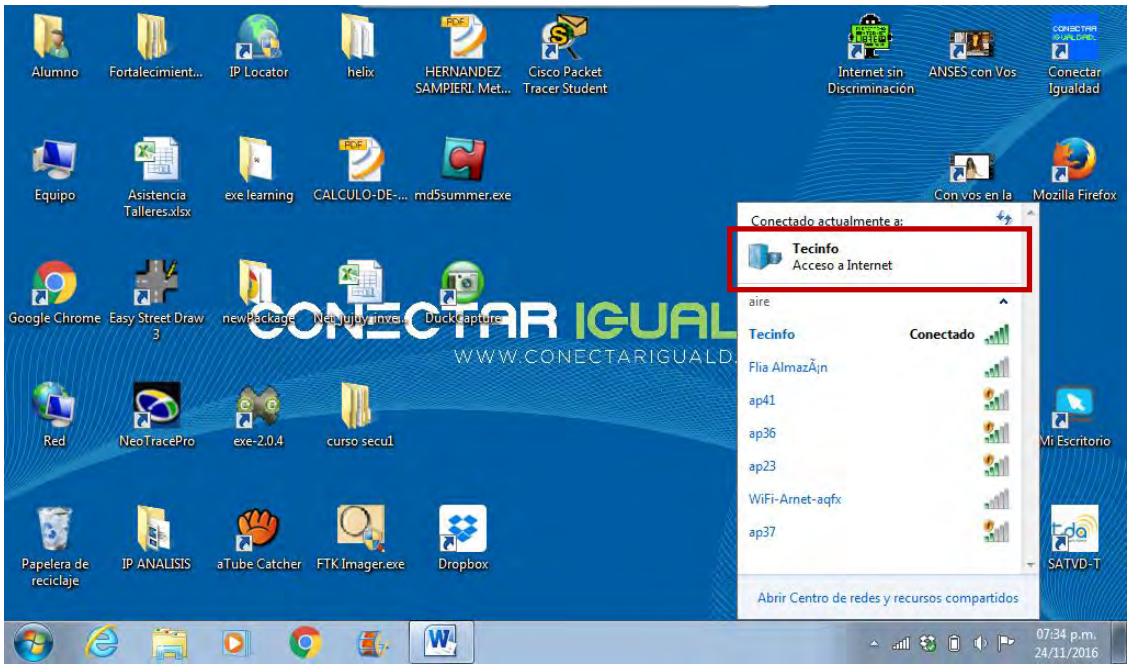
Captura de pantalla N° 8.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.103** corresponde al nombre **"TECINF-PC"** identificado anteriormente.

CONFIRMACIÓN

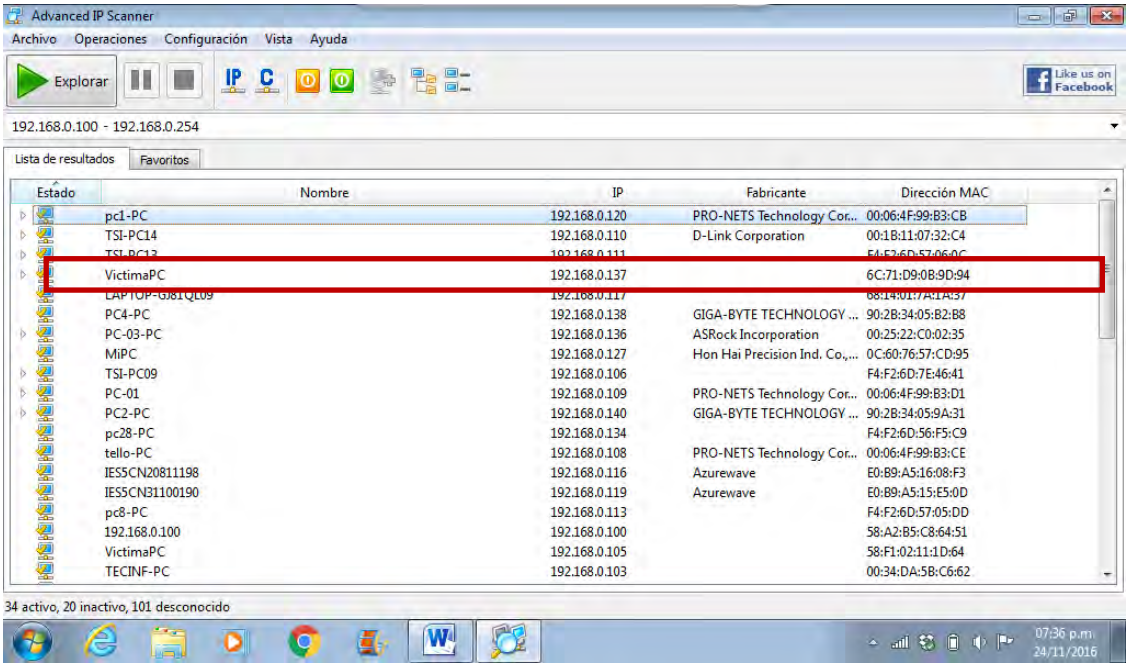


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.103 y comparando la dirección MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **00:1F:3C:51:44:F7.**

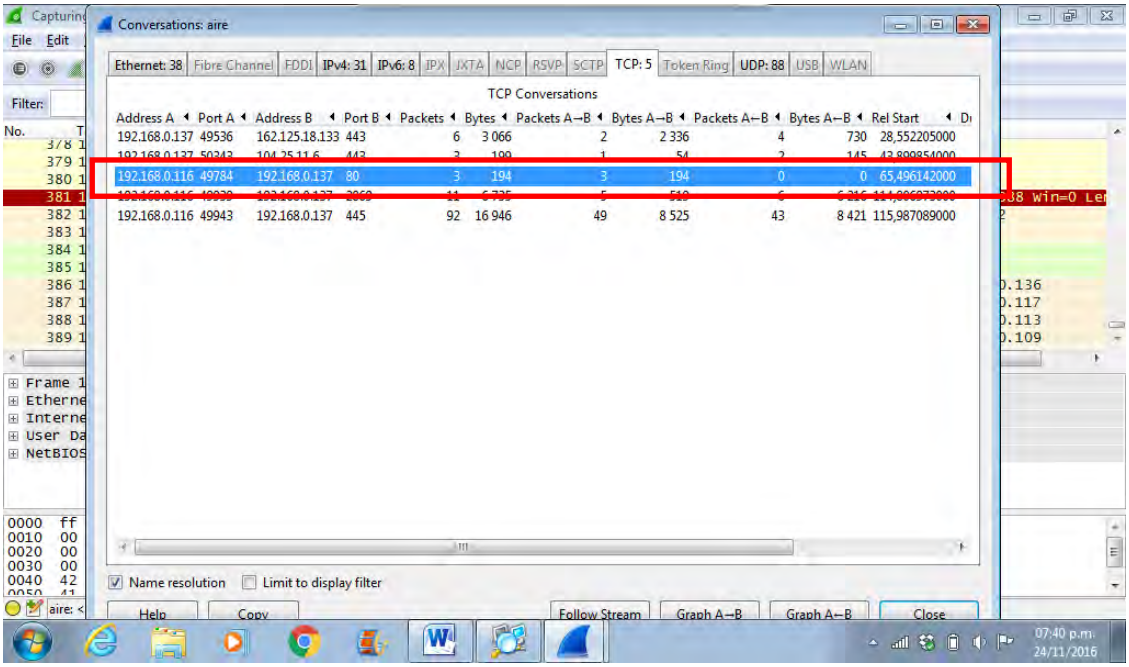
Caso N° 9: 24/11/16



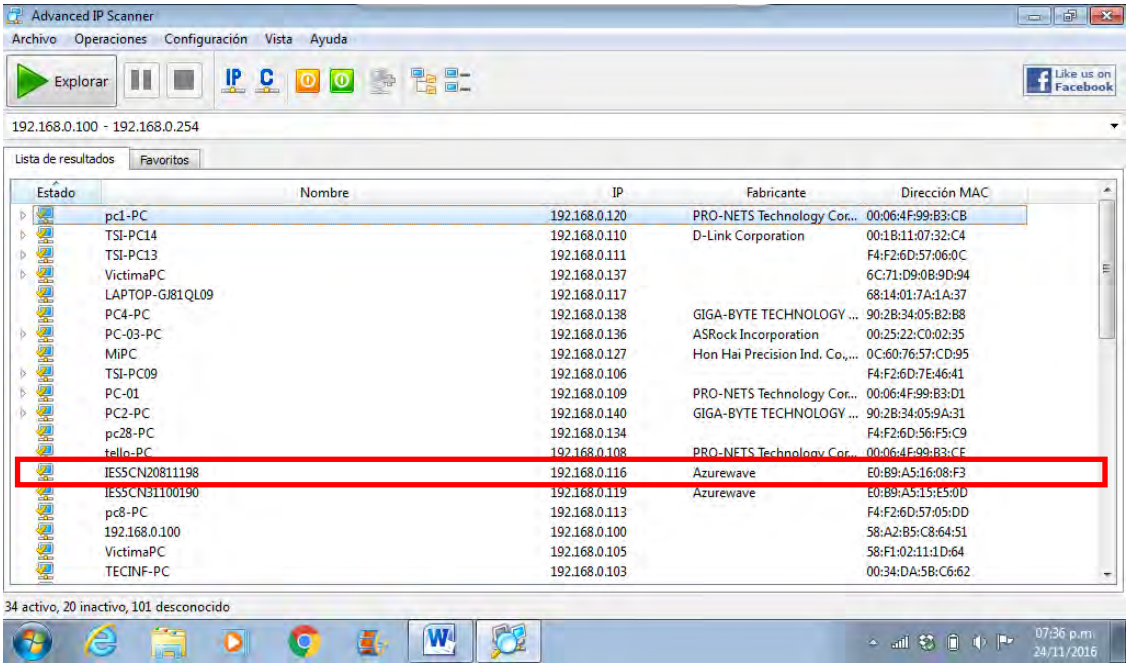
Captura de pantalla N° 9.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 9.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.137**, la cual va a ser la computadora receptora de las acciones ilicitas.

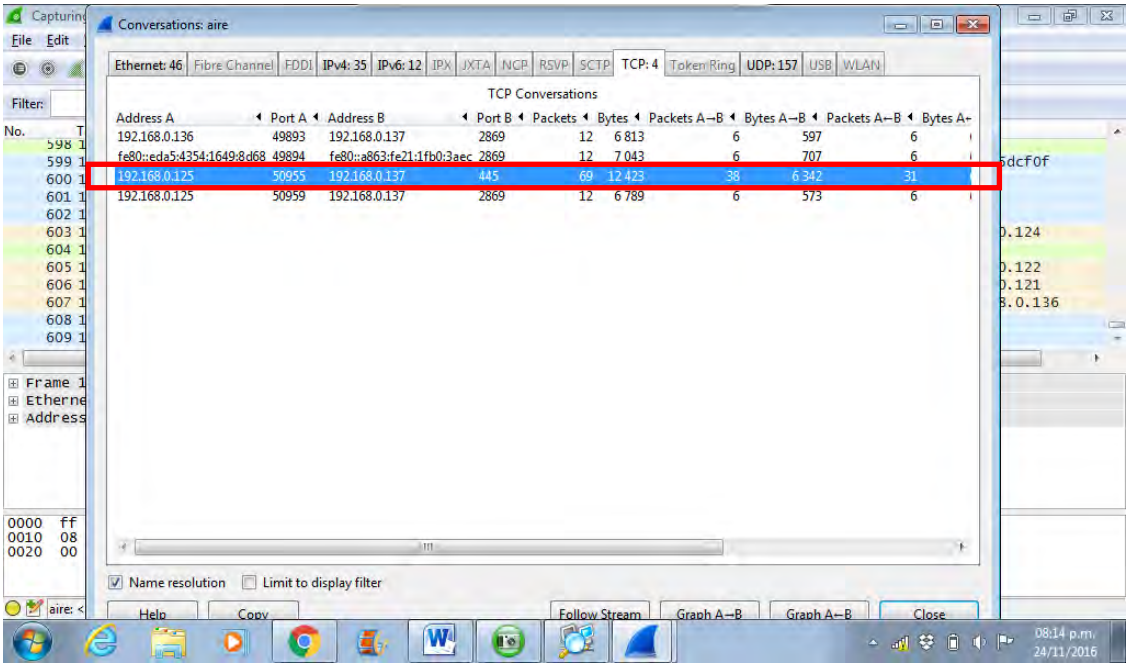


Captura de pantalla N° 9.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.116** con la direccion IP **192.168.0.137.**

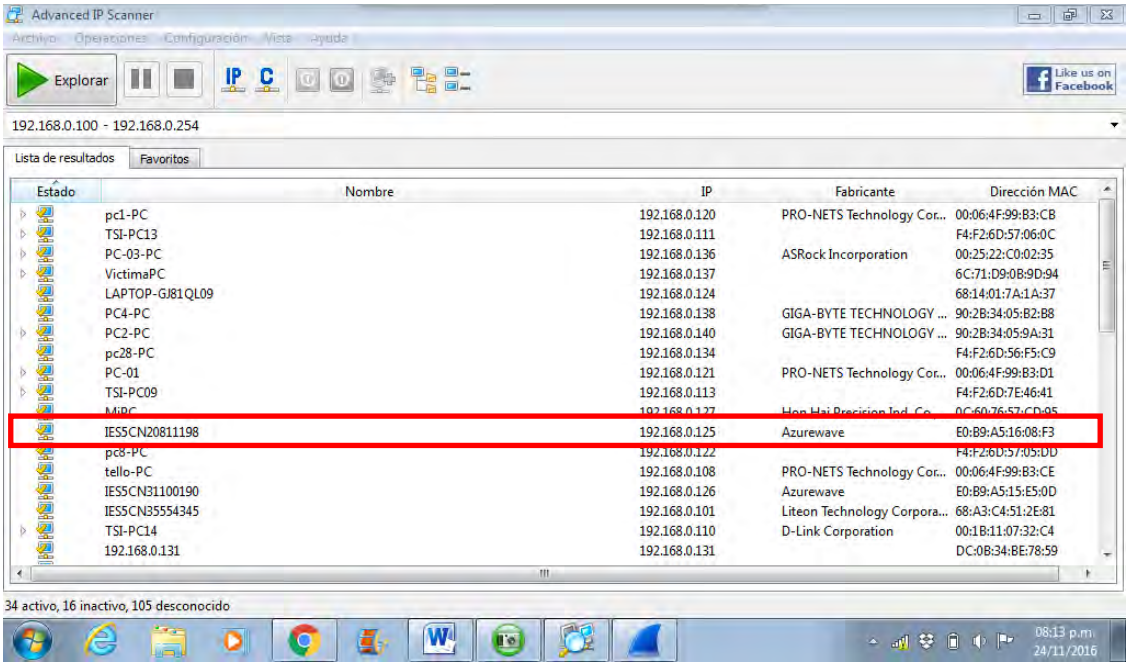


Captura de pantalla N° 9.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.116** la asignada al hosts **"IES5CN20811198"** con direccion MAC **E0:B9:A5:16:08:F3**.

Desconexión de "IES5CN20811198": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

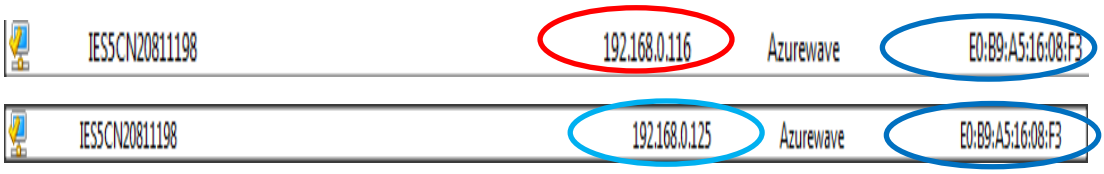


Captura de pantalla N° 9.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora "VictimaPC" y una IP hasta ahora desconocida: **192.168.0.125.**



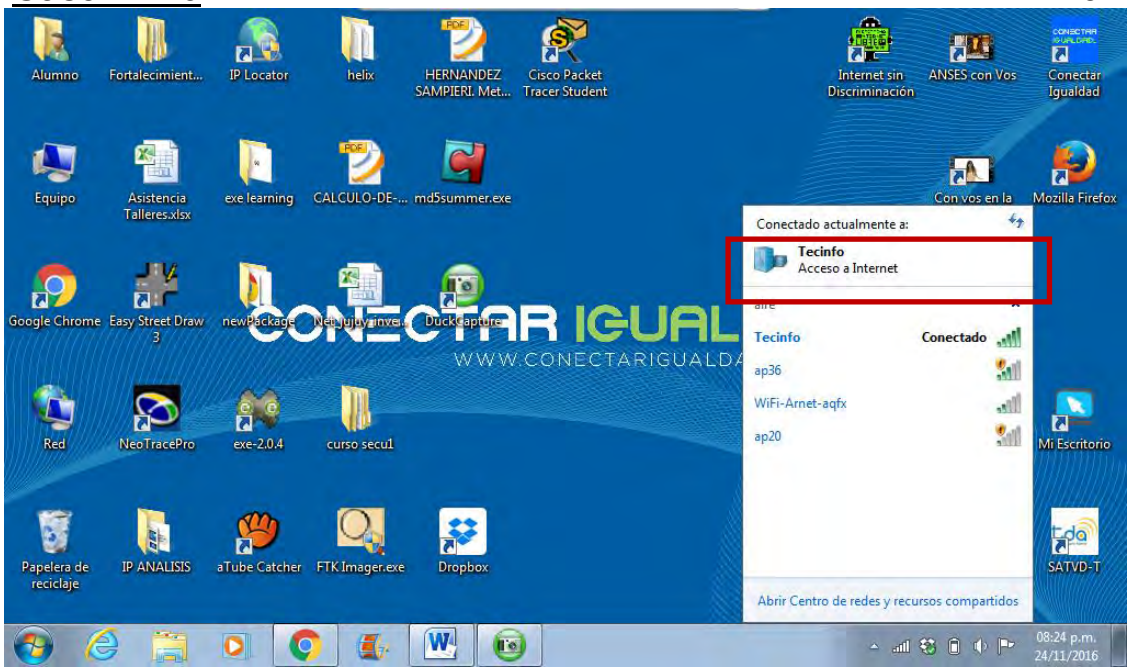
Captura de pantalla N° 9.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.125** corresponde al nombre **"IES5CN20811198"** identificado anteriormente.

CONFIRMACIÓN:

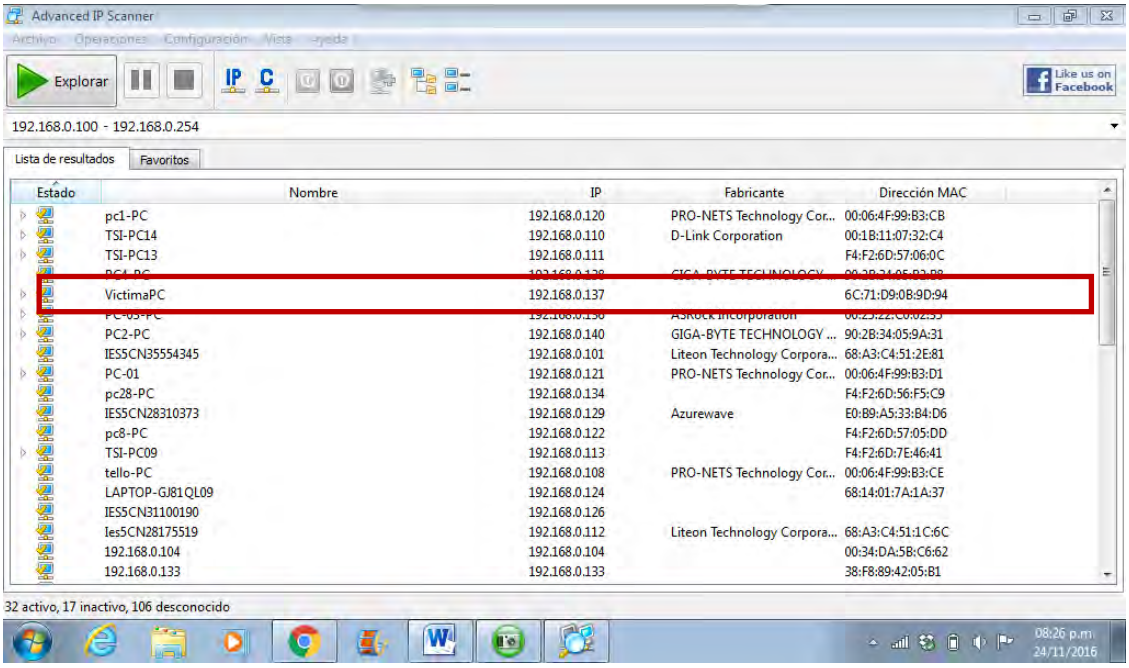


Se observa cambio de la dirección IP de 192.168.0.124 a 192.168.0.125; pero si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento: **E0:B9:A5:16:08:F3** . Correspondiente a una misma computadora.

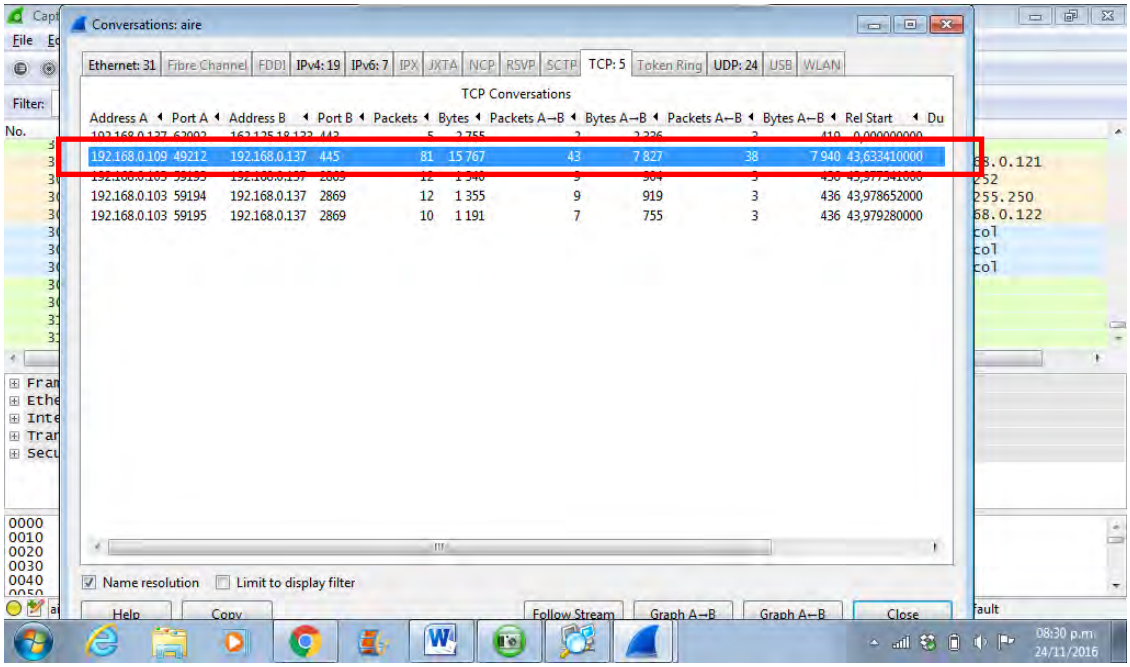
Caso N°10: 24/11/16



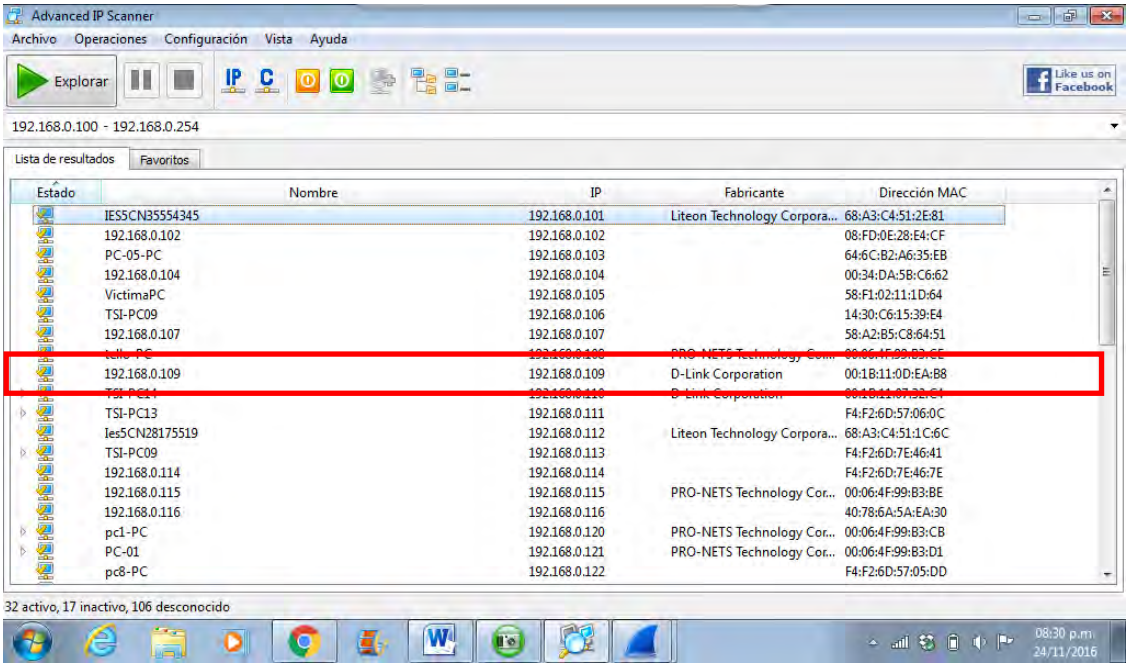
Captura de pantalla N° 10.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 10.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.137**, la cual va a ser la computadora receptora de las acciones ilicitas.

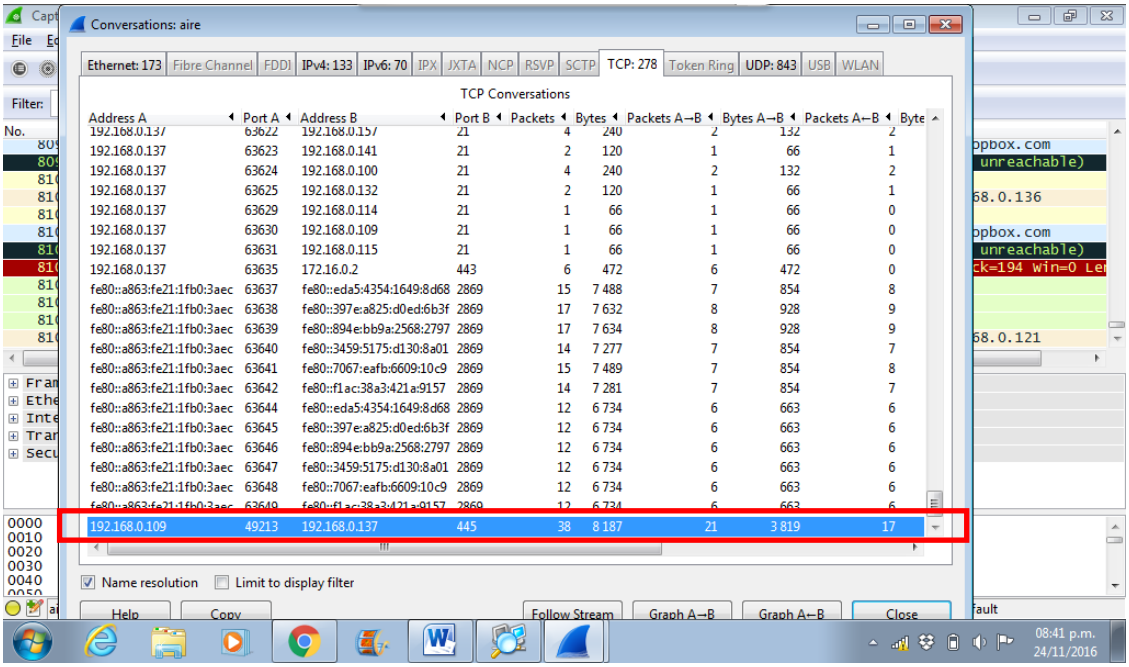


Captura de pantalla N° 10.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.109** con la direccion IP **192.168.0.137**.

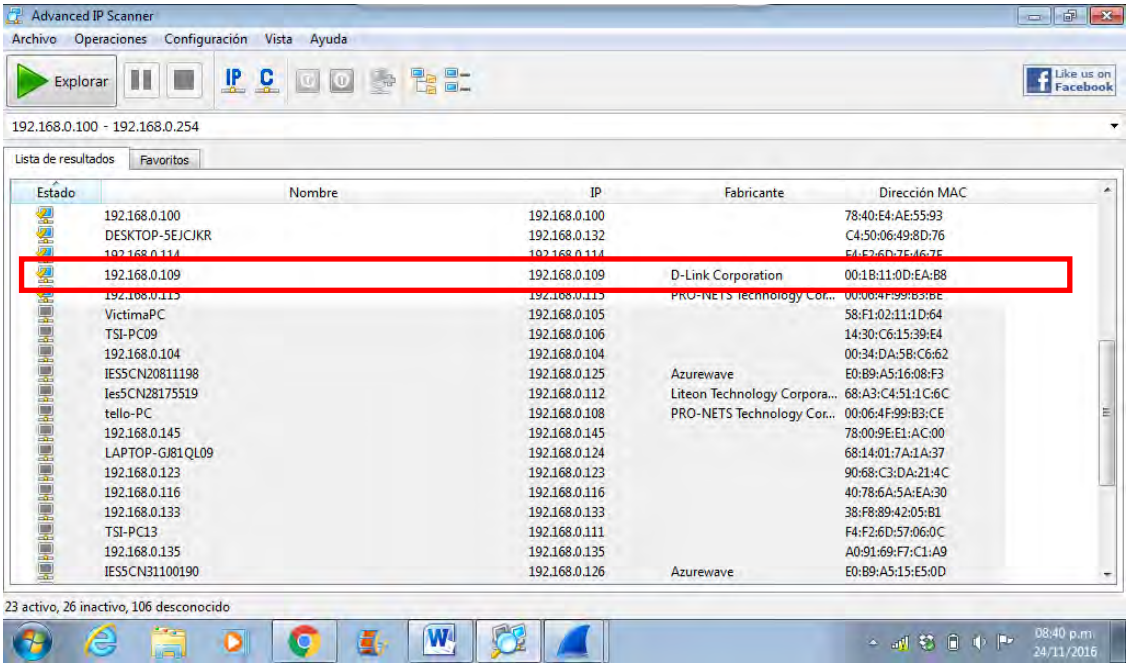


Captura de pantalla N° 10.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.109** la asignada al hosts **"192.168.0.109"** con direccion MAC **00:1B:11:0D:EA:B8.**

Desconexión de“192.168.0.109”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

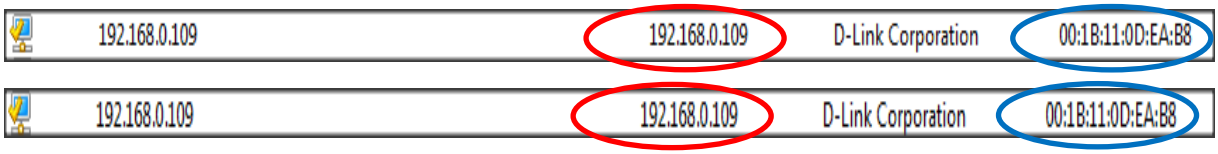


Captura de pantalla N° 10.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora “VictimaPC” como de la sospechosa: **192.168.0.109.**



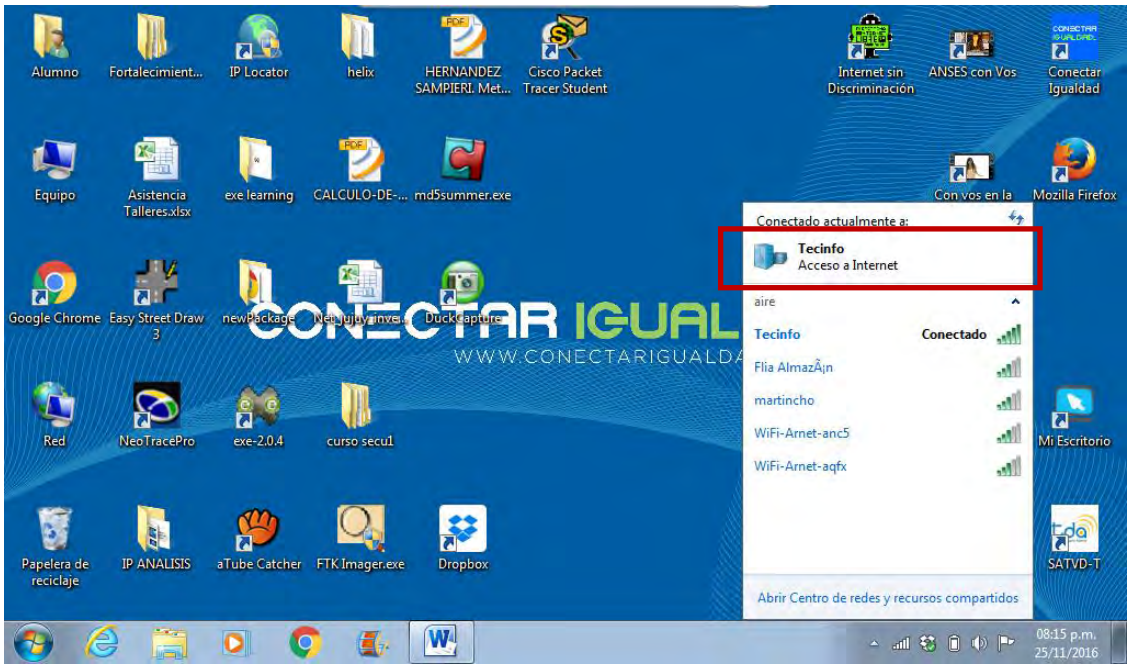
Captura de pantalla N° 10.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.109** corresponde al nombre **“192.168.0.109”** identificado anteriormente.

CONFIRMACIÓN

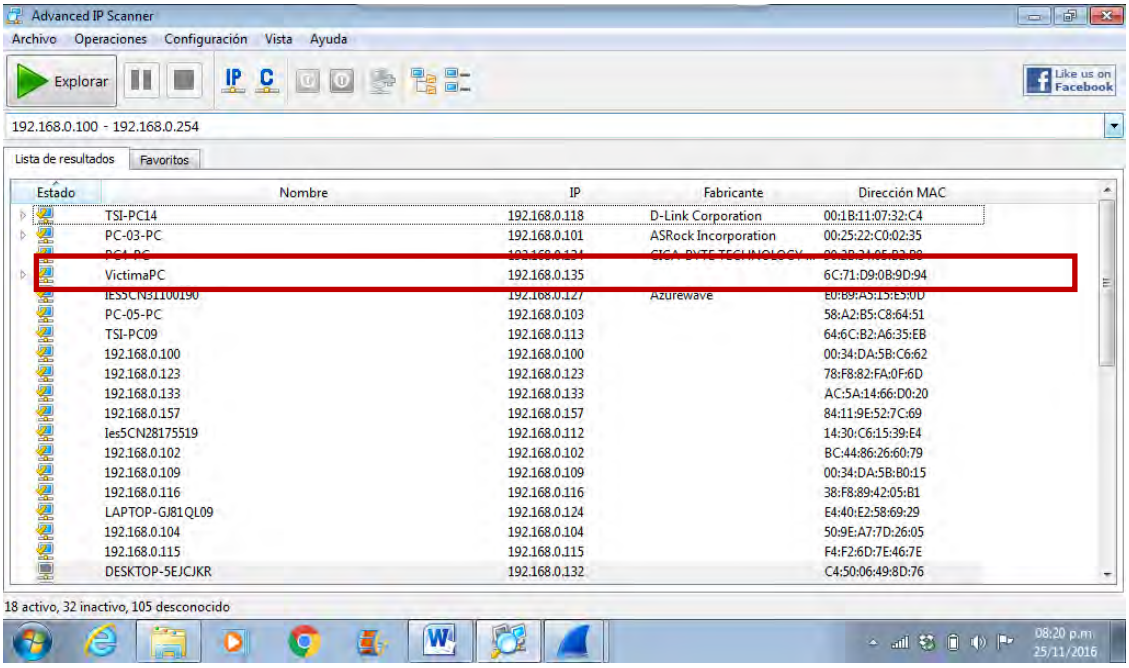


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.109 y comparando la dirección MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **00:1B:11:0D:EA:B8.**

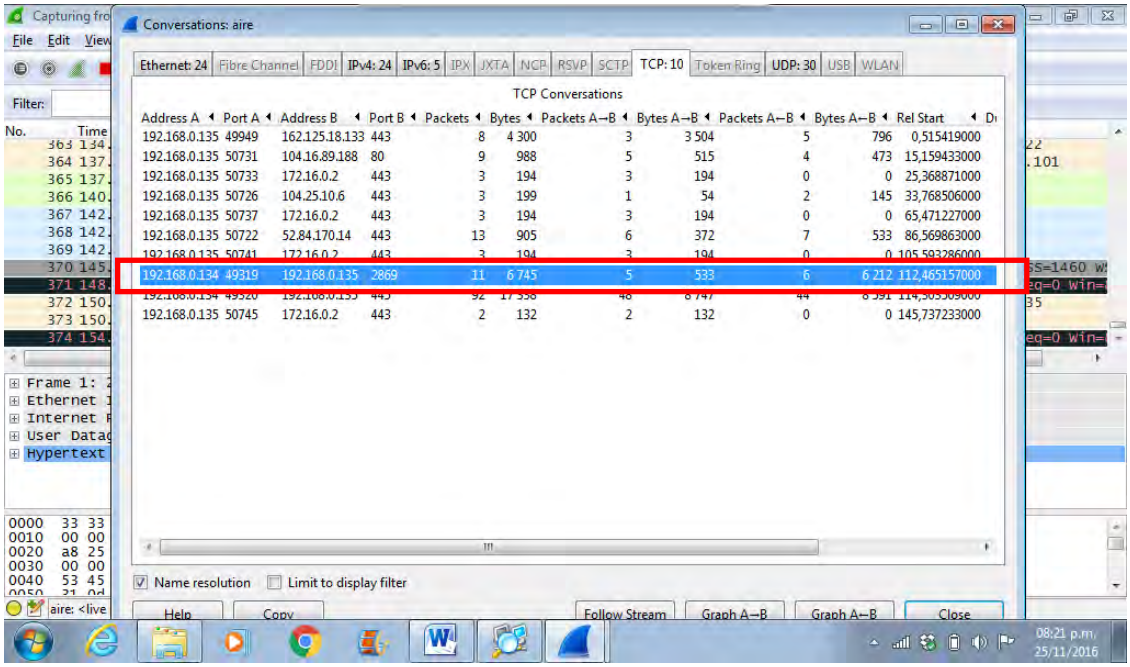
Caso N° 11: 25/11/16



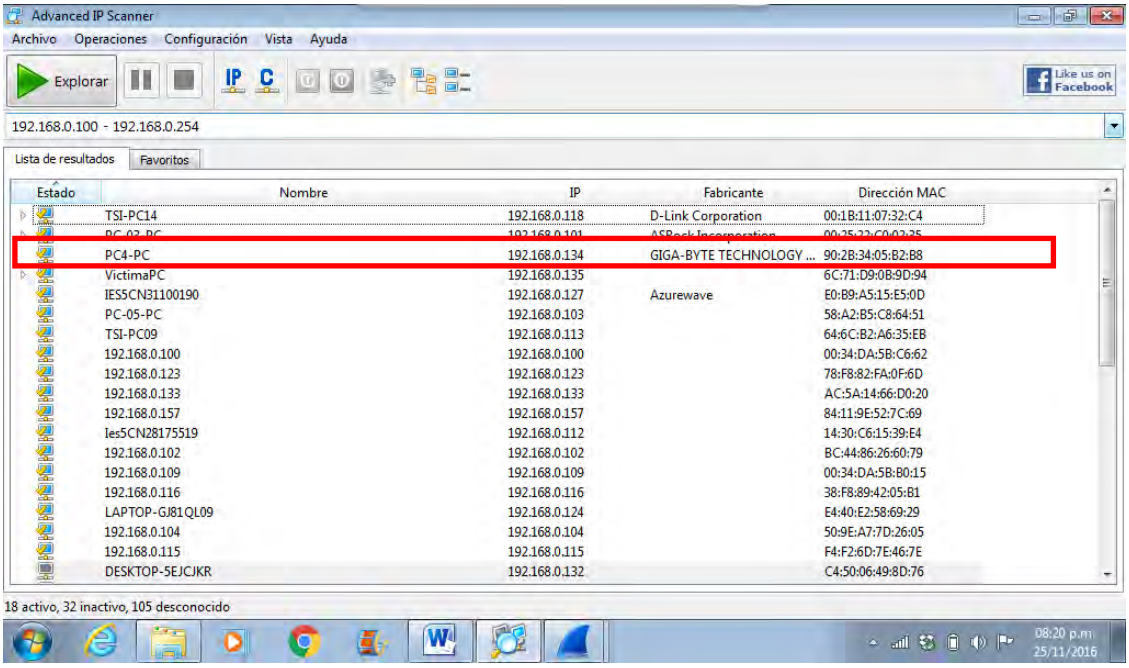
Captura de pantalla N° 11.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 11.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.135**, la cual va a ser la computadora receptora de las acciones ilicitas.

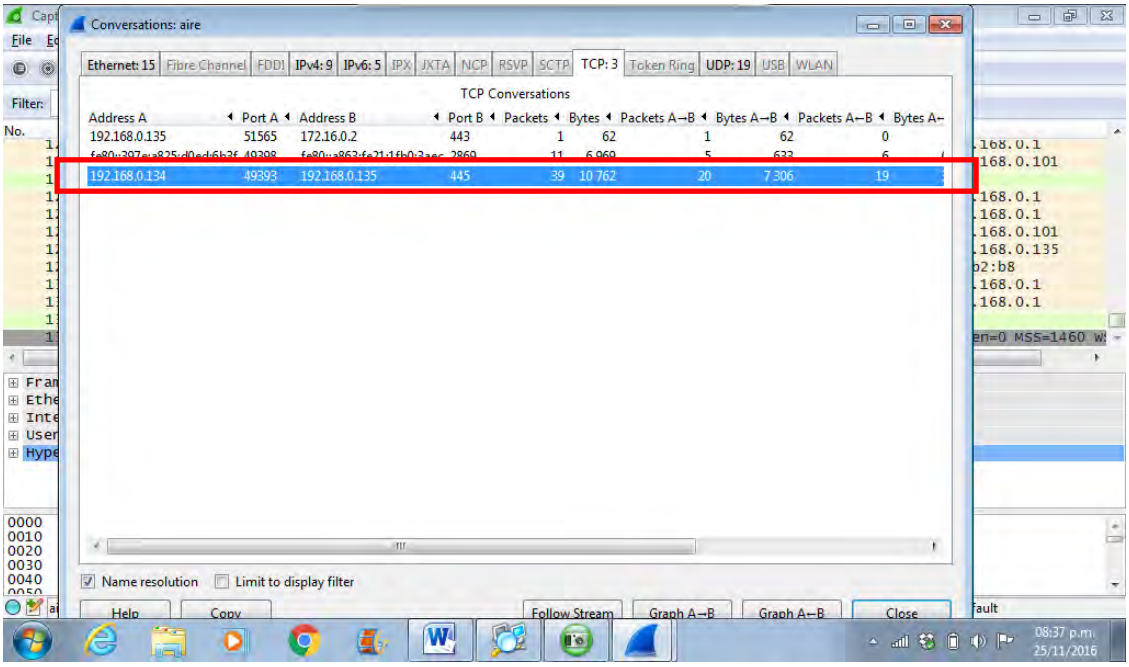


Captura de pantalla N° 11.3: Al ejecutar el programa Wireshark, en la ventana “Conversations: aire”, dentro de la pestaña “TCP” se registra comunicación de la direccion IP **192.168.0.134** con la direccion IP **192.168.0.135**.

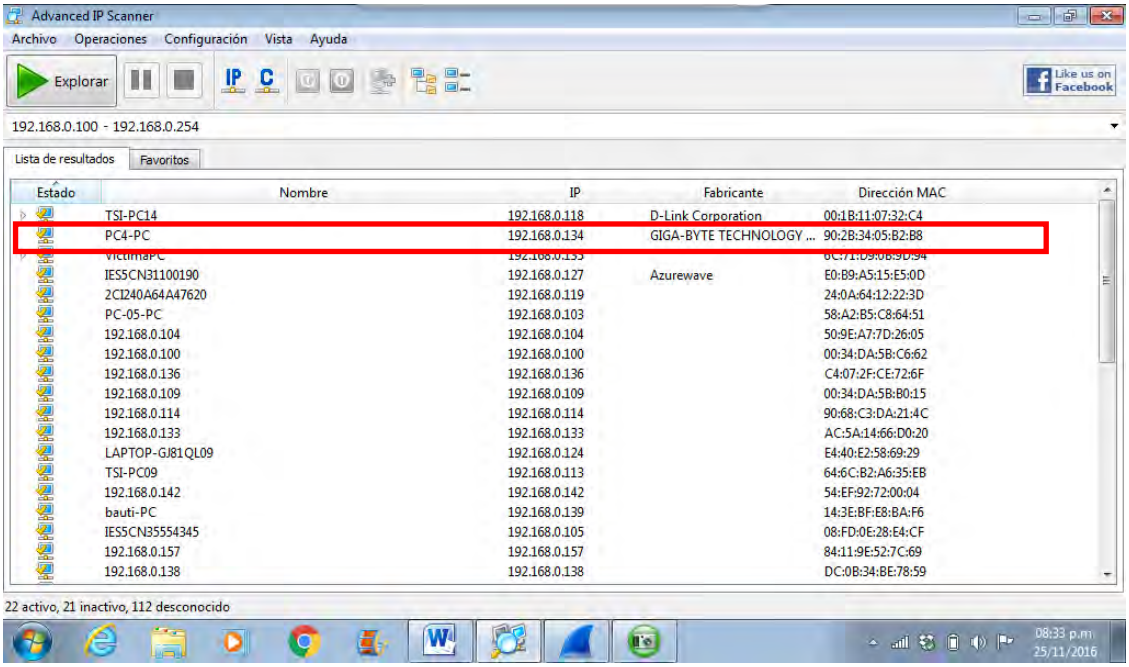


Captura de pantalla N° 11.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.134** la asignada al hosts **“PC4-PC”** con direccion MAC **90:2B:34:05:B2:B8.**

Desconexión de “PC4-PC”: computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

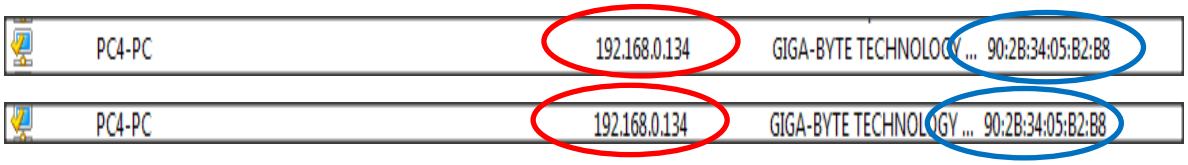


Captura de pantalla N° 11.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora “VictimaPC” como de la sospechosa: **192.168.0.134.**



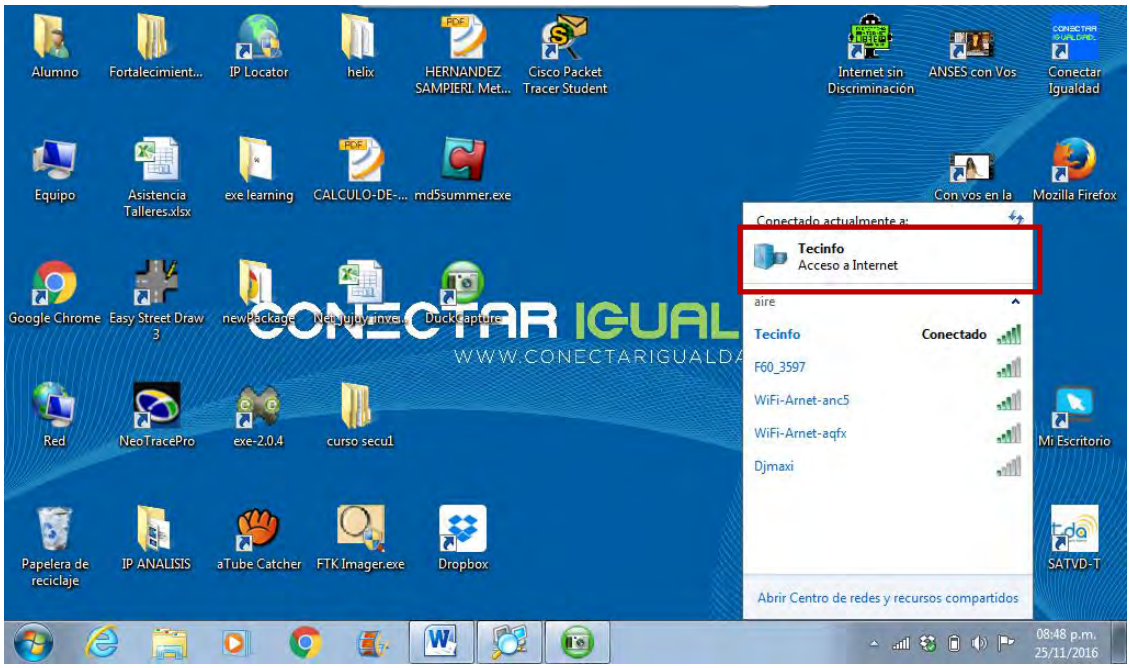
Captura de pantalla N° 11.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.134** corresponde al nombre **"PC4-PC"** identificado anteriormente.

CONFIRMACIÓN

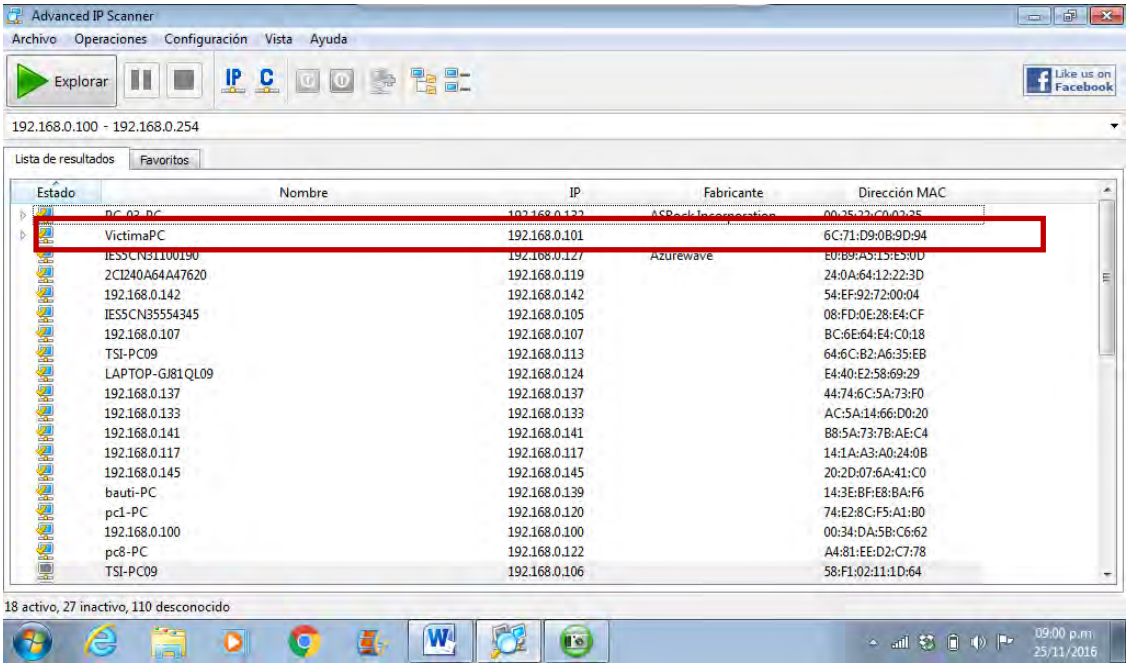


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.134 y comparando las direcciónes MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **90:2B:34:05:B2:B8.**

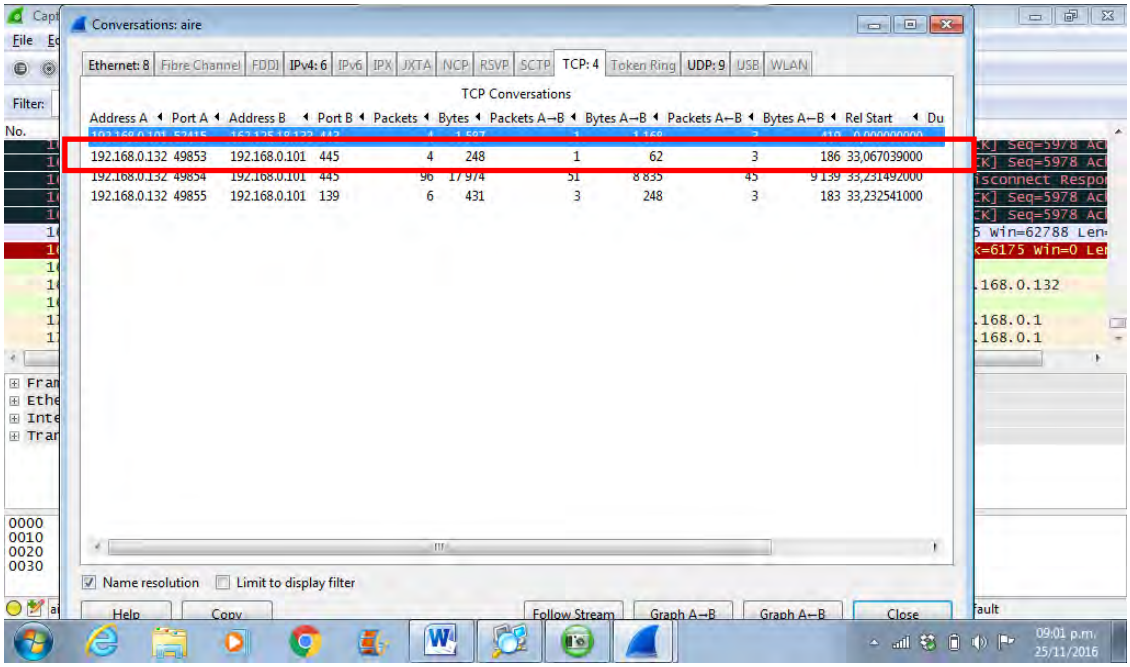
Caso N°12: 25/11/16



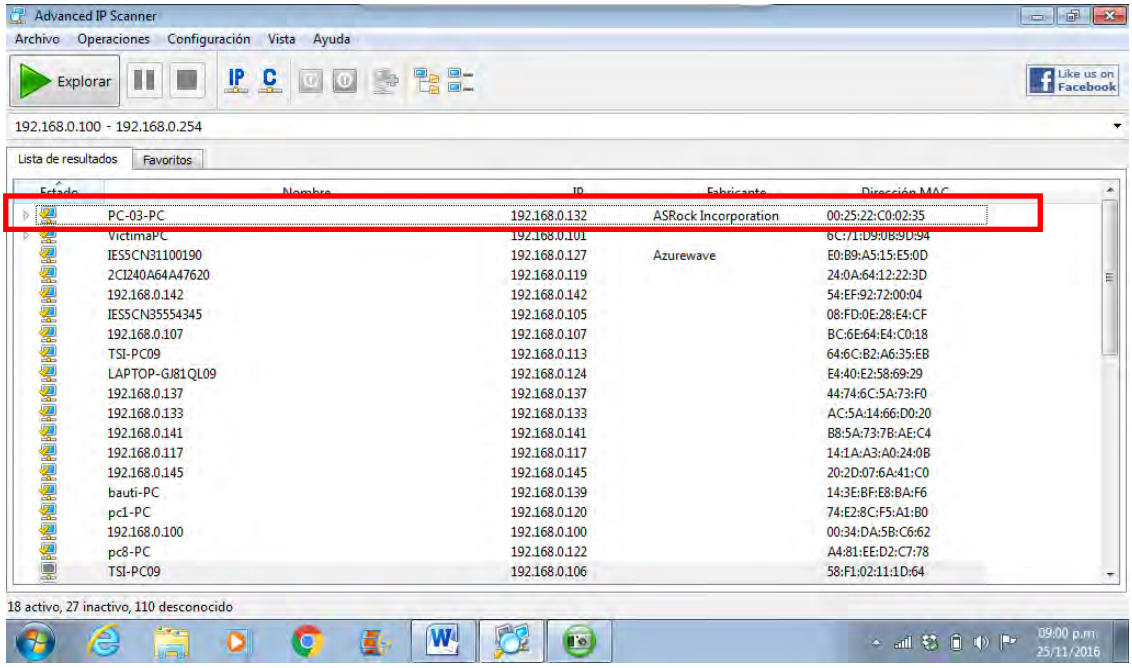
Captura de pantalla N° 12.1: Se establece conexión efectiva con la red "Tecinfo".



Captura de pantalla N° 12.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.101**, la cual va a ser la computadora receptora de las acciones ilicitas.

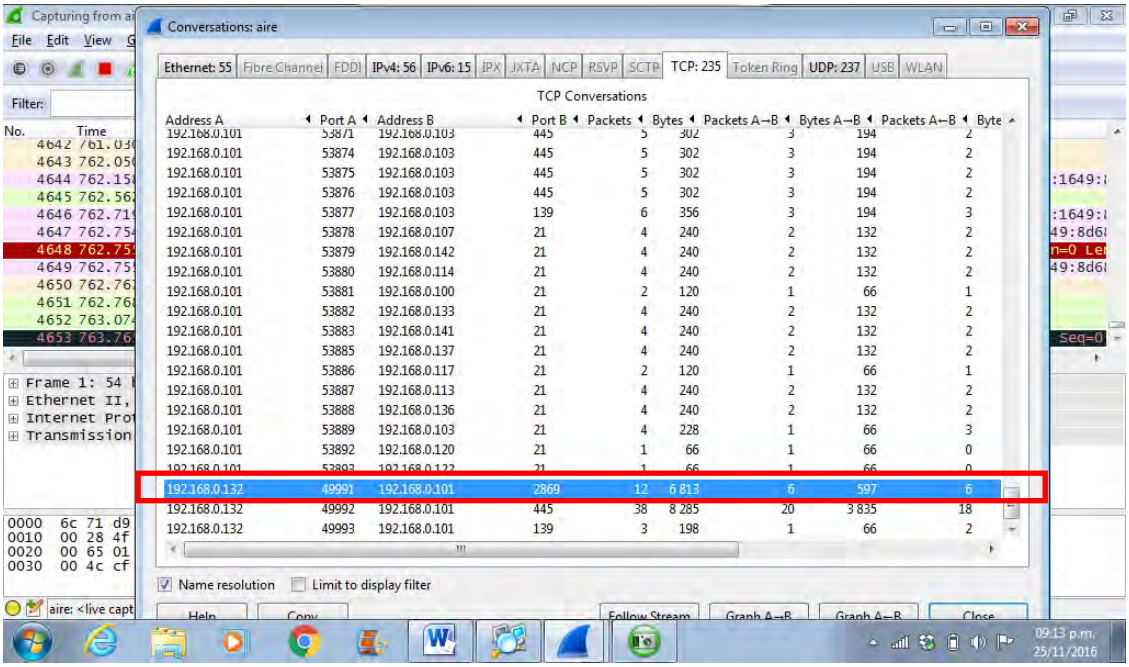


Captura de pantalla N° 12.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.132** con la direccion IP **192.168.0.101.**

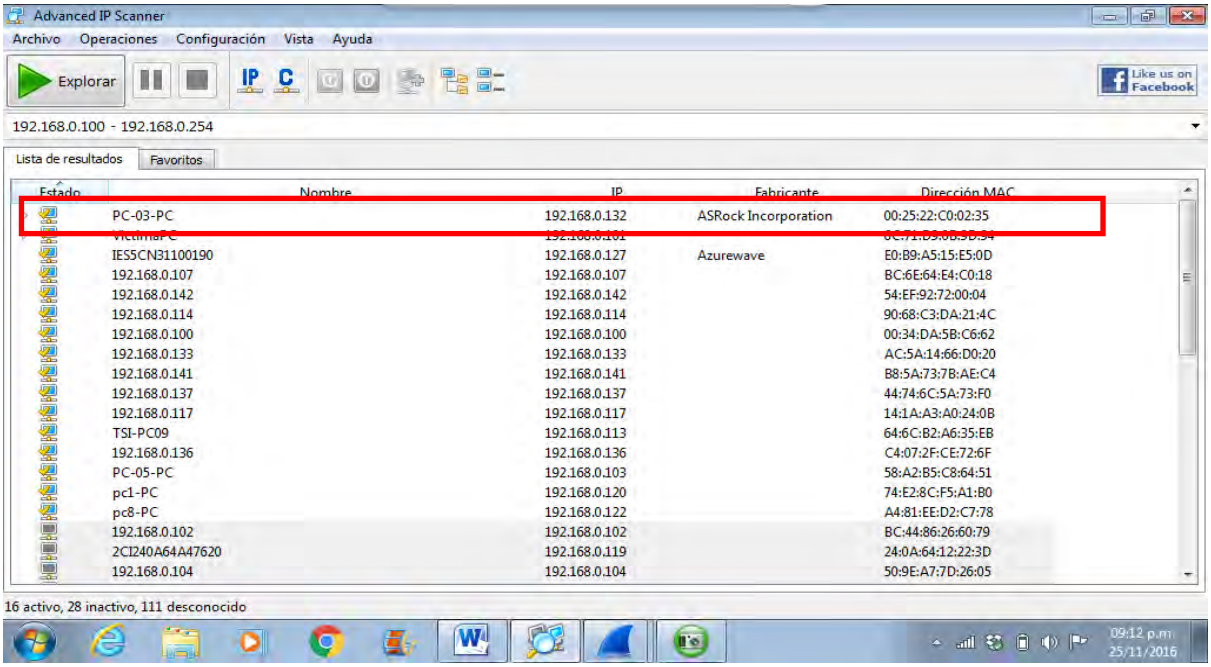


Captura de pantalla N° 12.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.132** la asignada al hosts **"PC-03-PC"** con direccion MAC **00:25:22:C0:02:35.**

Desconexion de "PC-03-PC": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

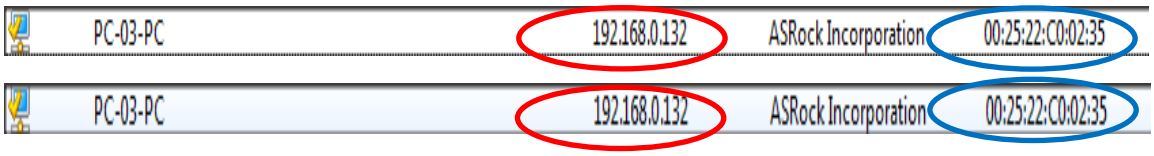


Captura de pantalla N° 12.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora "VictimaPC" como de la sospechosa: **192.168.0.132.**



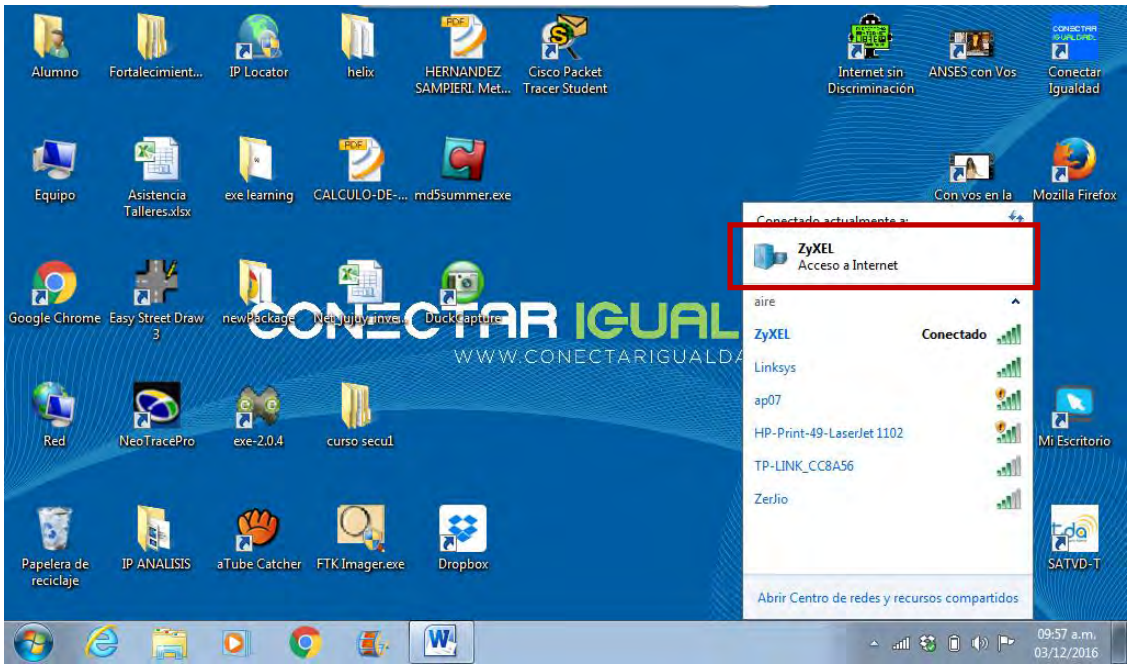
Captura de pantalla N° 12.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.132** corresponde al nombre **"PC-03-PC"** identificado anteriormente.

CONFIRMACIÓN

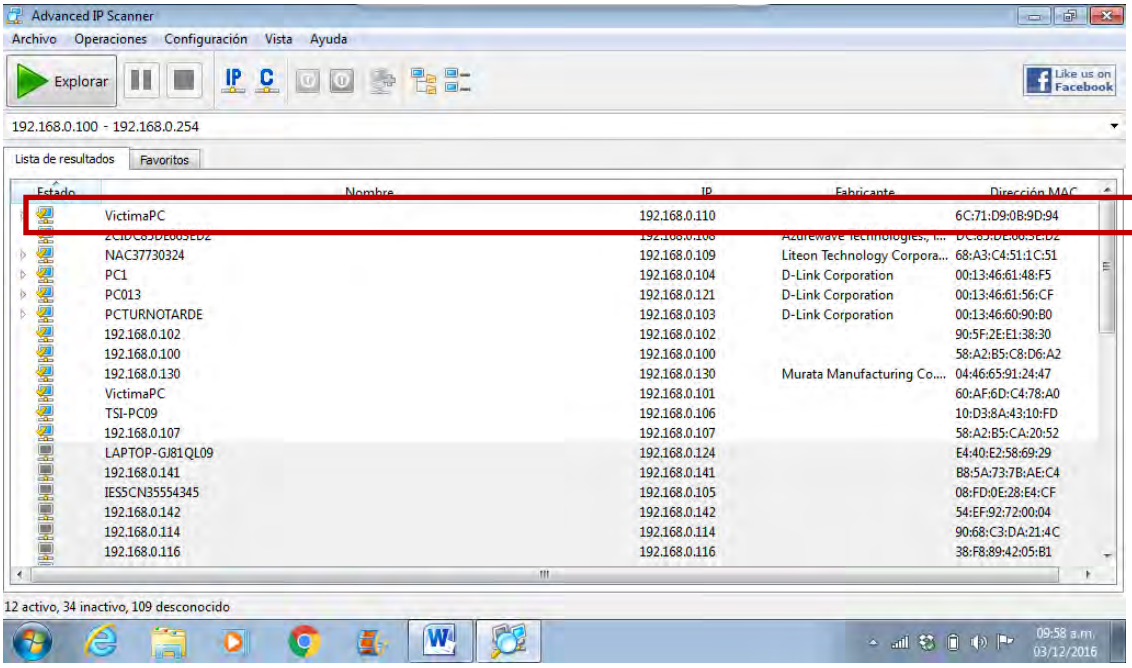


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.132 y comparando la dirección MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **00:25:22:C0:02:35.**

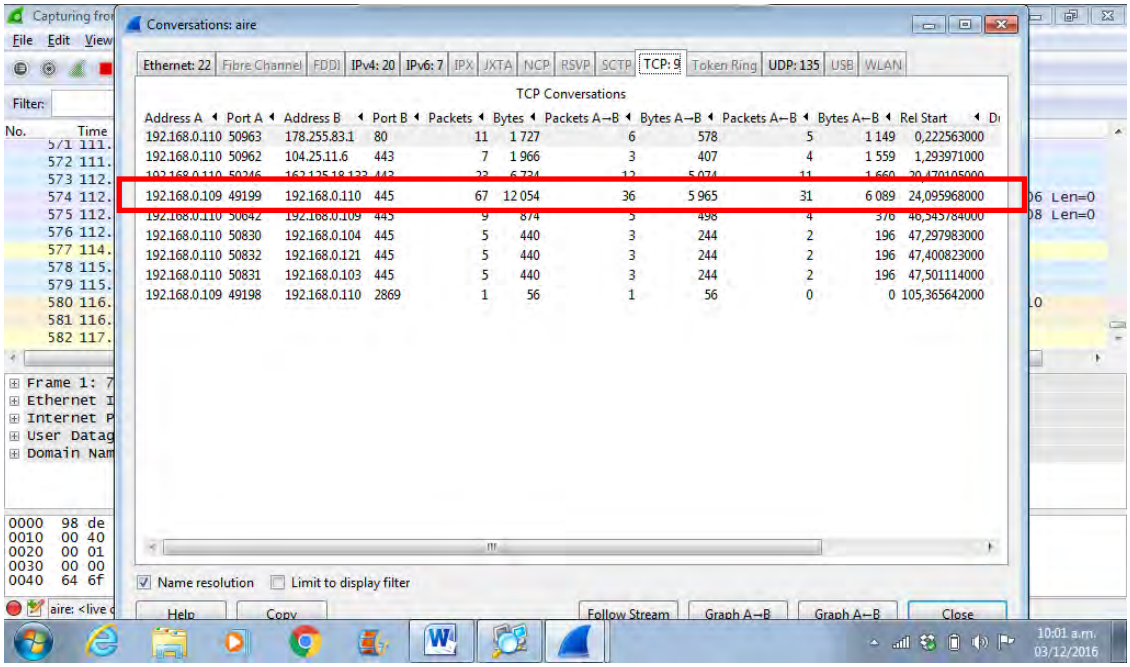
Caso N° 13: 03/12/16



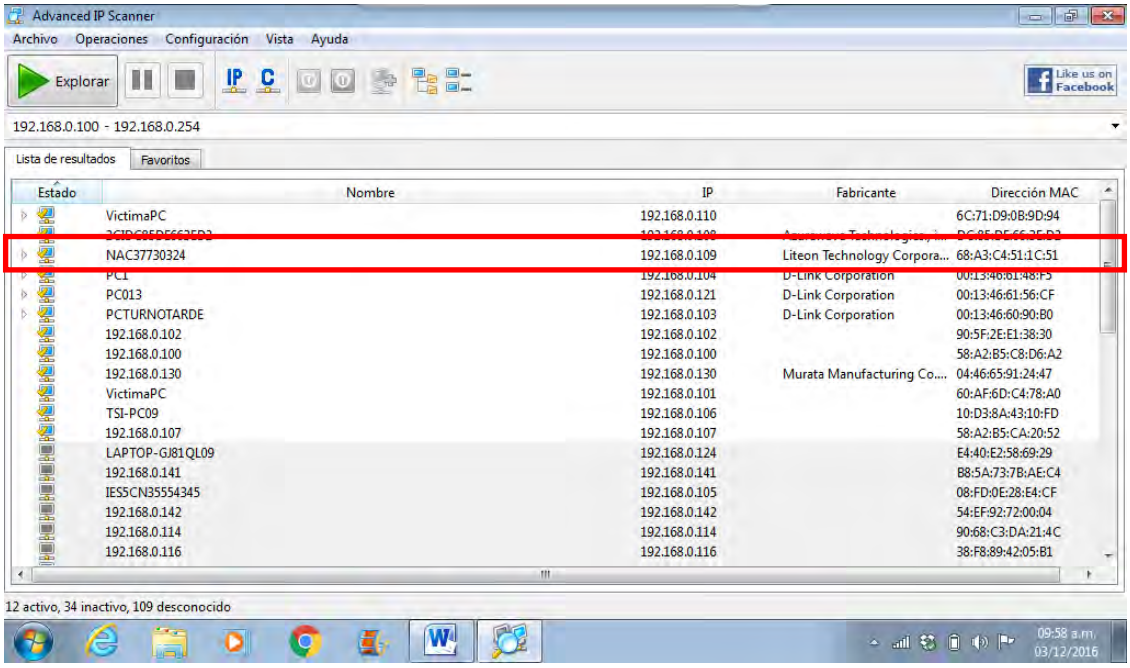
Captura de pantalla N° 13.1: Se establece conexión efectiva con la red "ZyXEL".



Captura de pantalla N° 13.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.110**, la cual va a ser la computadora receptora de las acciones ilicitas.

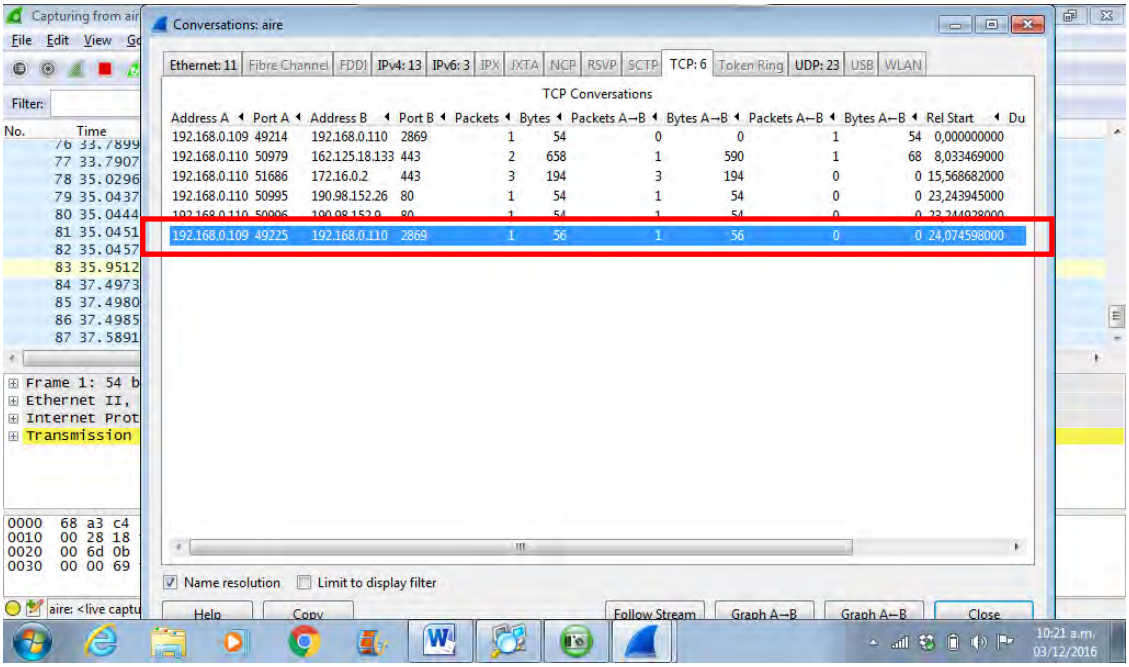


Captura de pantalla N° 13.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.109** con la direccion IP **192.168.0.110.**

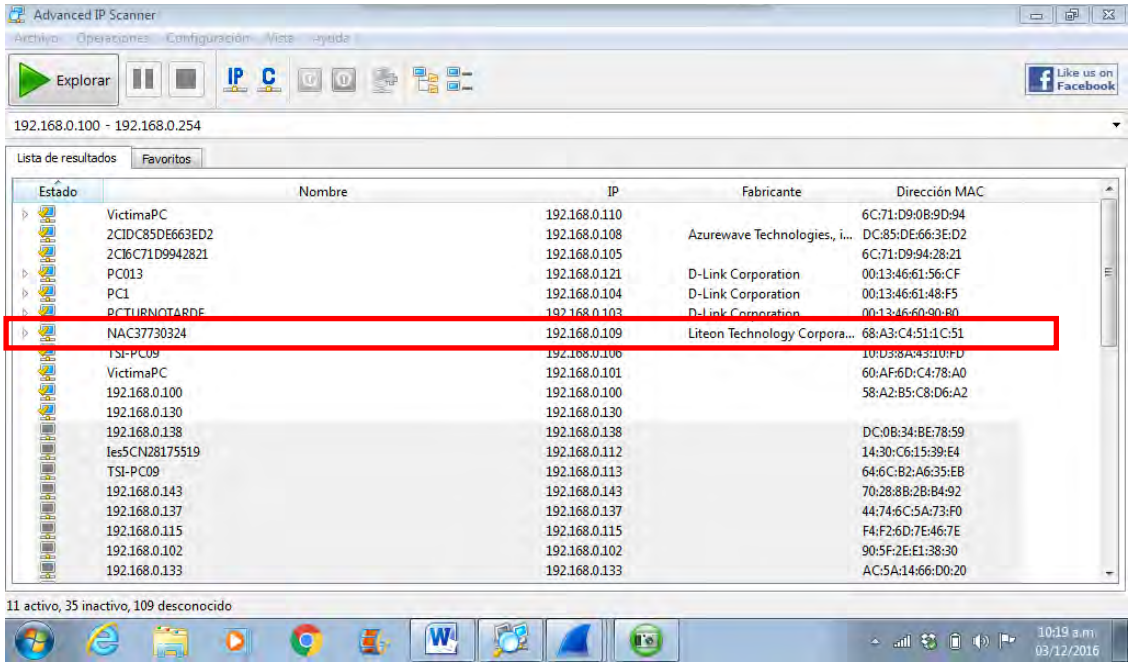


Captura de pantalla N° 13.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.109** la asignada al hosts **"NAC37730324"** con direccion MAC **68:A3:C4:51:1C:51.**

Desconexión de "NAC37730324": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

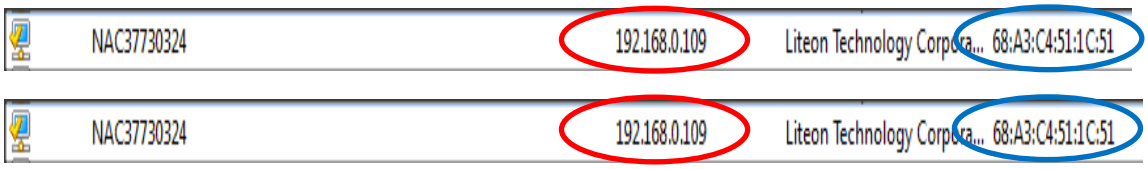


Captura de pantalla N° 13.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora "VictimaPC" como de la sospechosa: **192.168.0.109.**



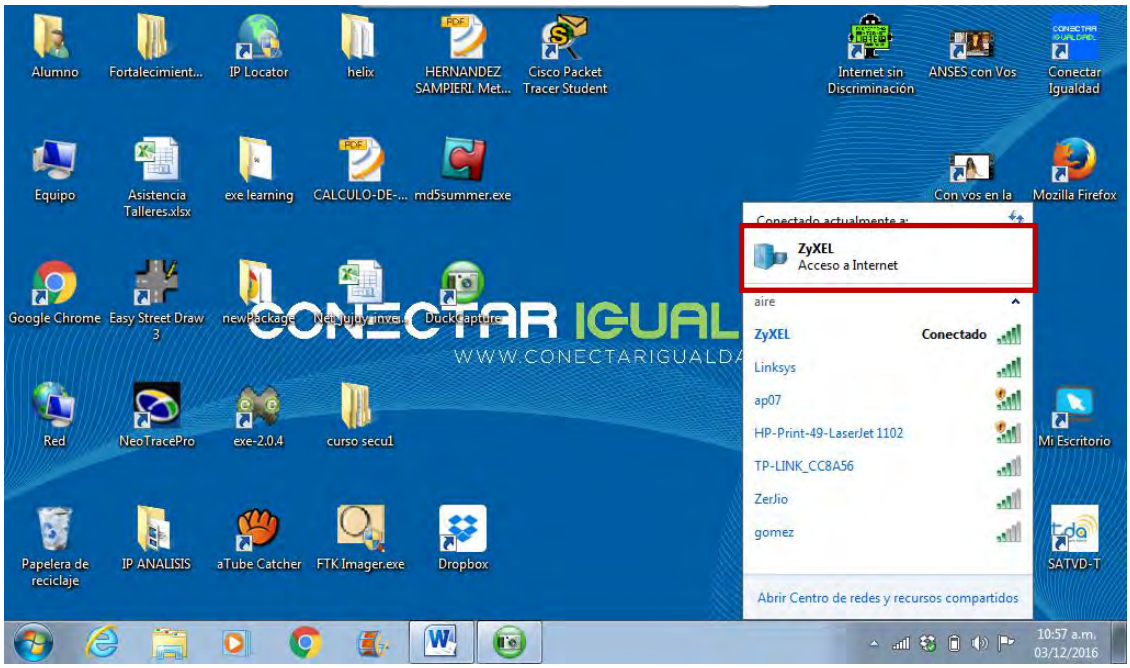
Captura de pantalla N° 13.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.109** corresponde al nombre **"NAC37730324"** identificado anteriormente.

CONFIRMACIÓN

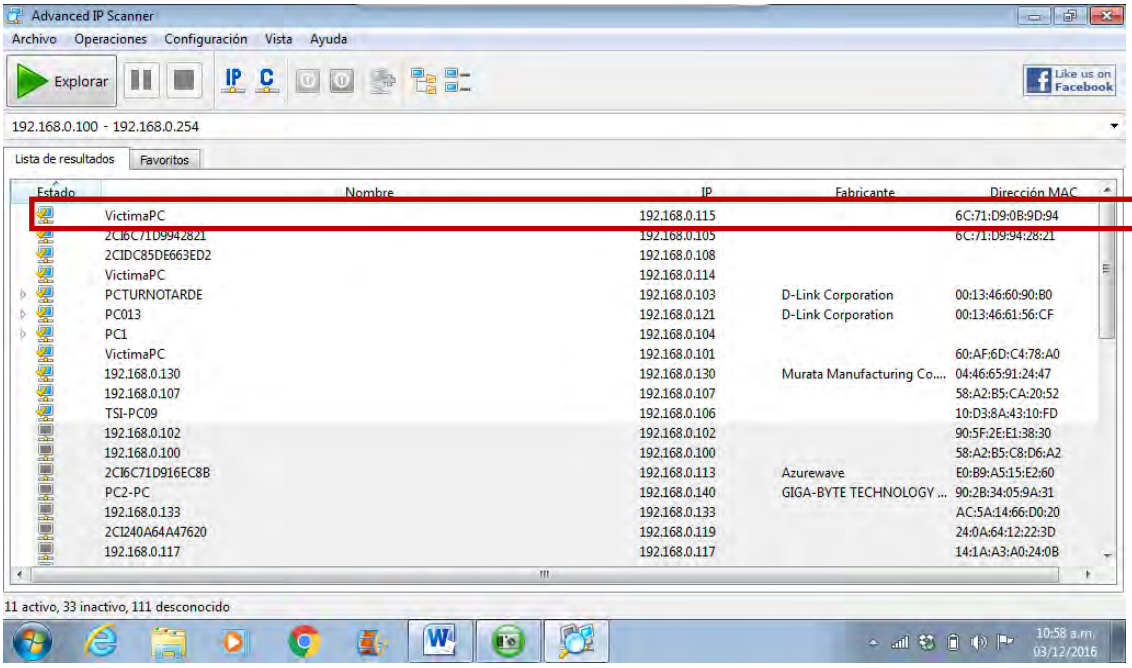


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.109 y comparando la dirección MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **68:A3:C4:51:1C:51.**

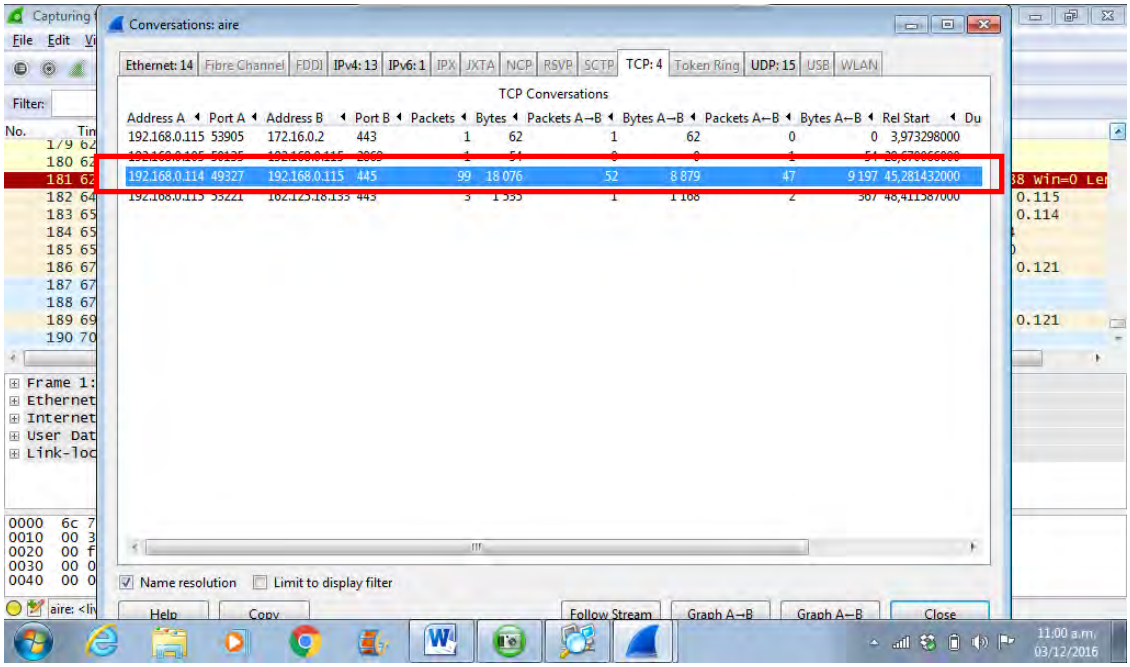
Caso N° 14: 03/12/16



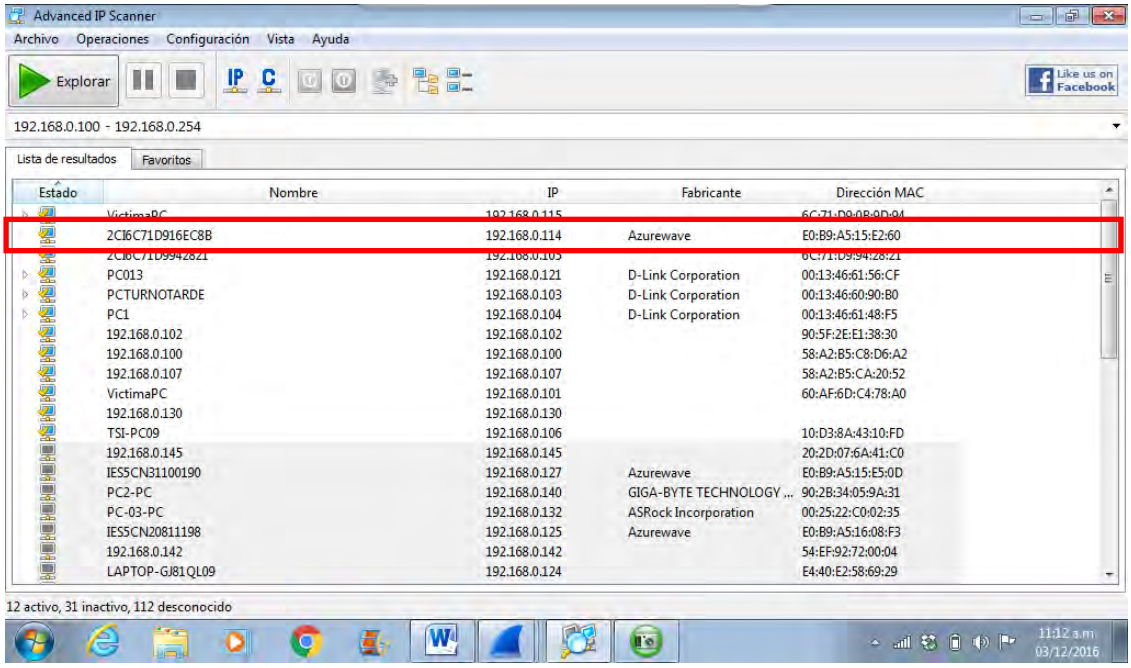
Captura de pantalla N° 14.1: Se establece conexión efectiva con la red "ZyXEL".



Captura de pantalla N° 14.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.115**, la cual va a ser la computadora receptora de las acciones ilicitas.

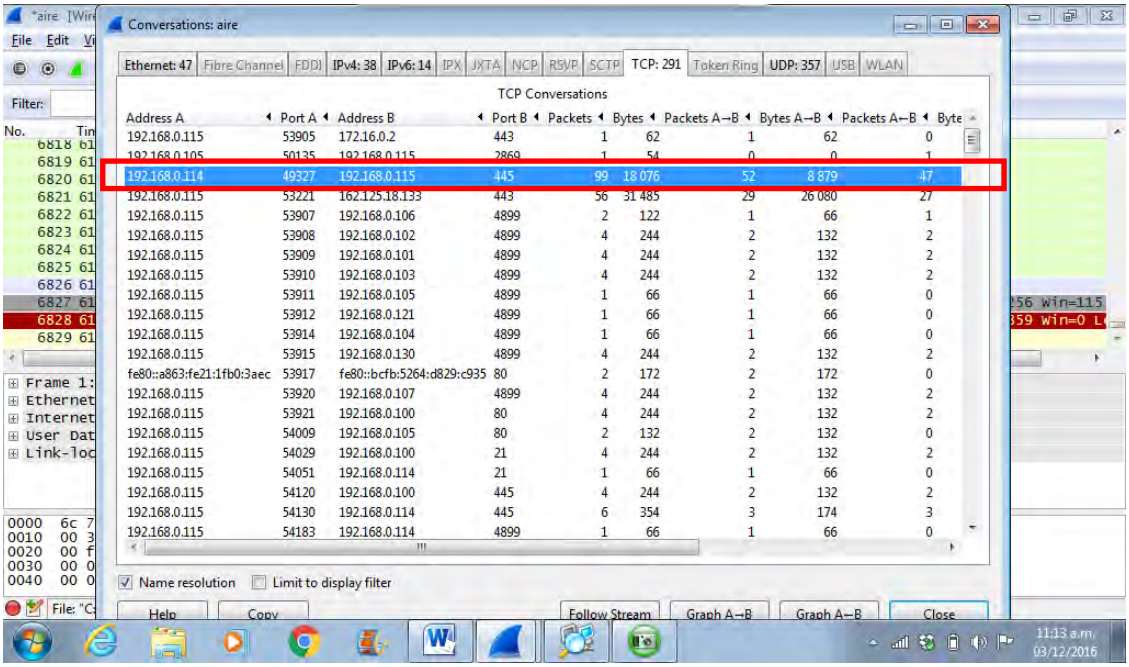


Captura de pantalla N° 14.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.114** con la direccion IP **192.168.0.115**.

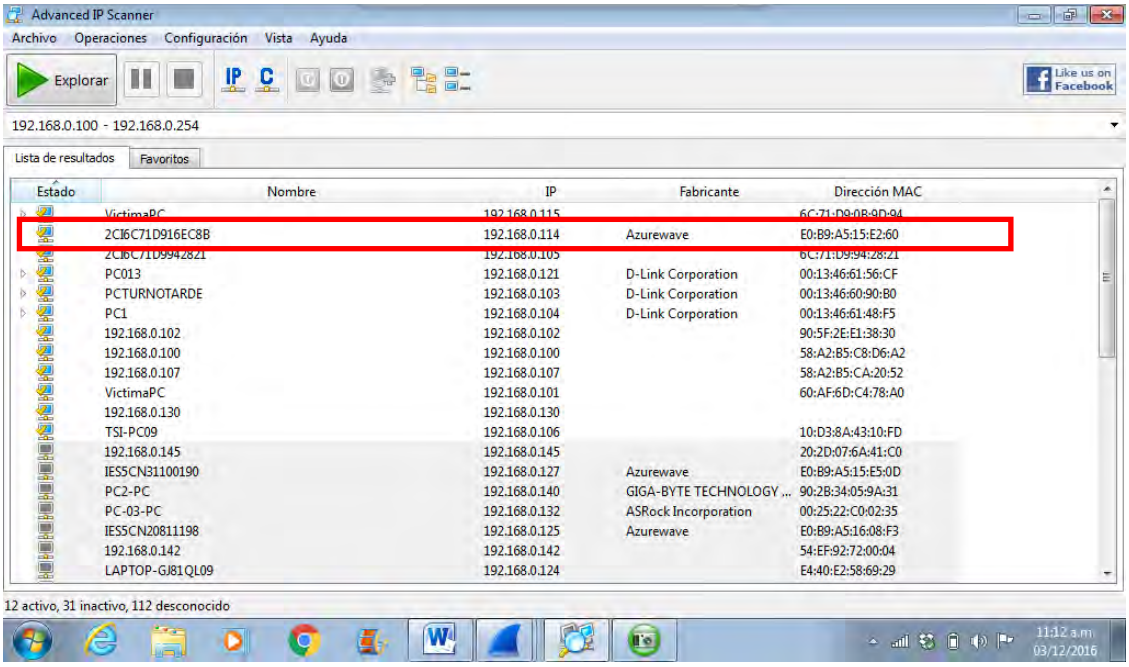


Captura de pantalla N° 14.4 En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.114** la asignada al hosts **"2C16C71D916EC8B"** con direccion MAC **E0:B9:A5:15:E2:60.**

Desconexión de "2C16C71D916EC8B": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte

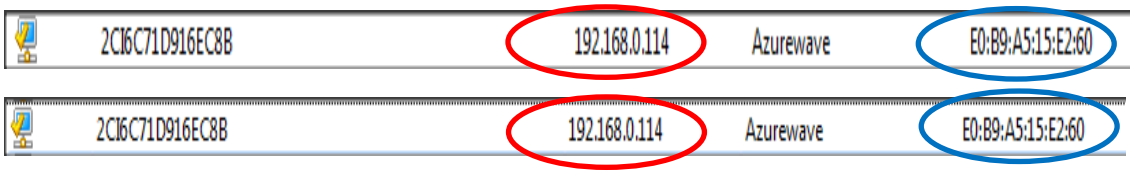


Captura de pantalla N° 14.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre las mismas dirección IPs, tanto de la computadora "VictimaPC" como de la sospechosa: **192.168.0.114.**



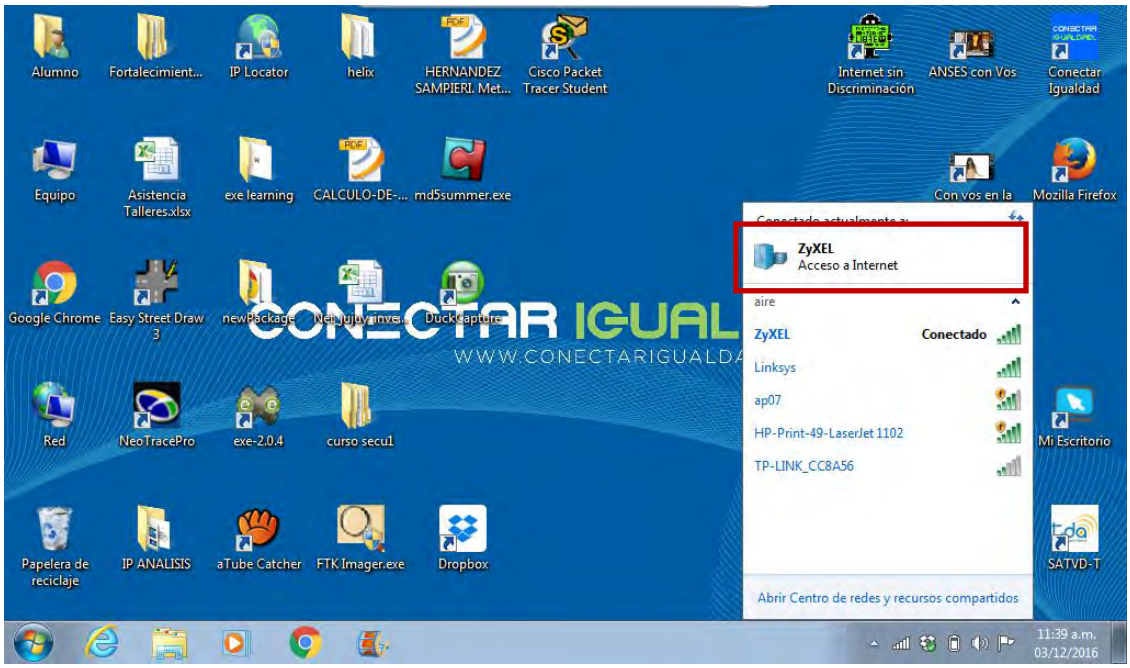
Captura de pantalla N° 14.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.114** corresponde al nombre **"2C16C71D916EC8B"** identificado anteriormente.

CONFIRMACIÓN

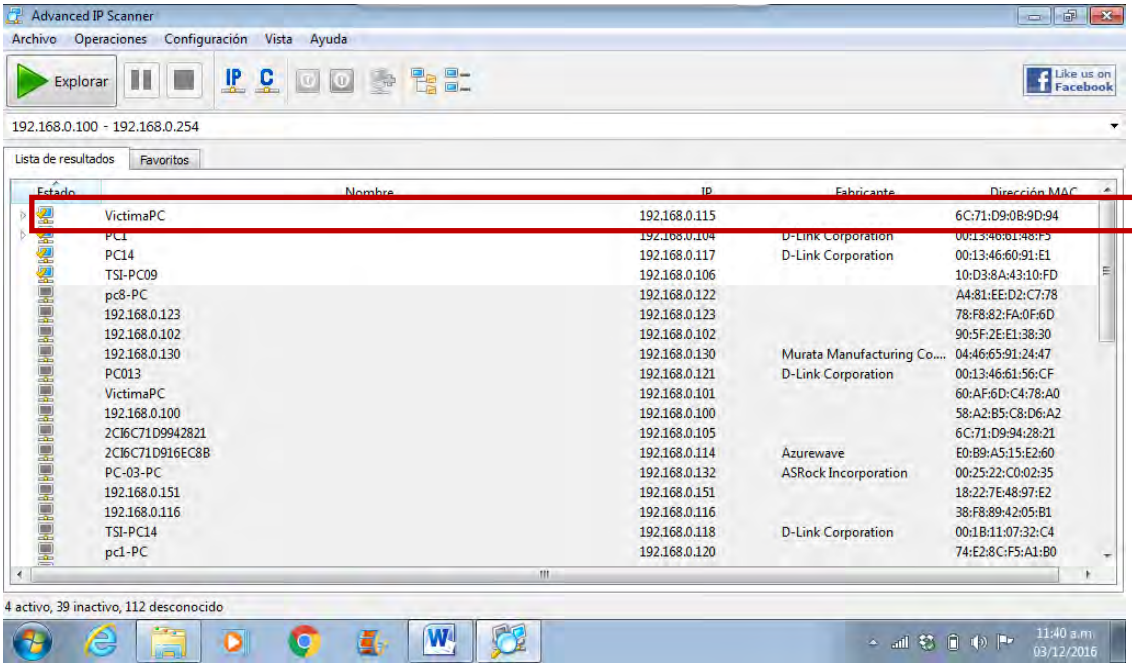


No se registró cambio de la dirección IP luego de la desconexión, permaneciendo esta como: 192.168.0.114 y comparando la dirección MAC podemos confirmar que se trataría de la misma computadora que en un primer momento: **E0:B9:A5:15:E2:60**

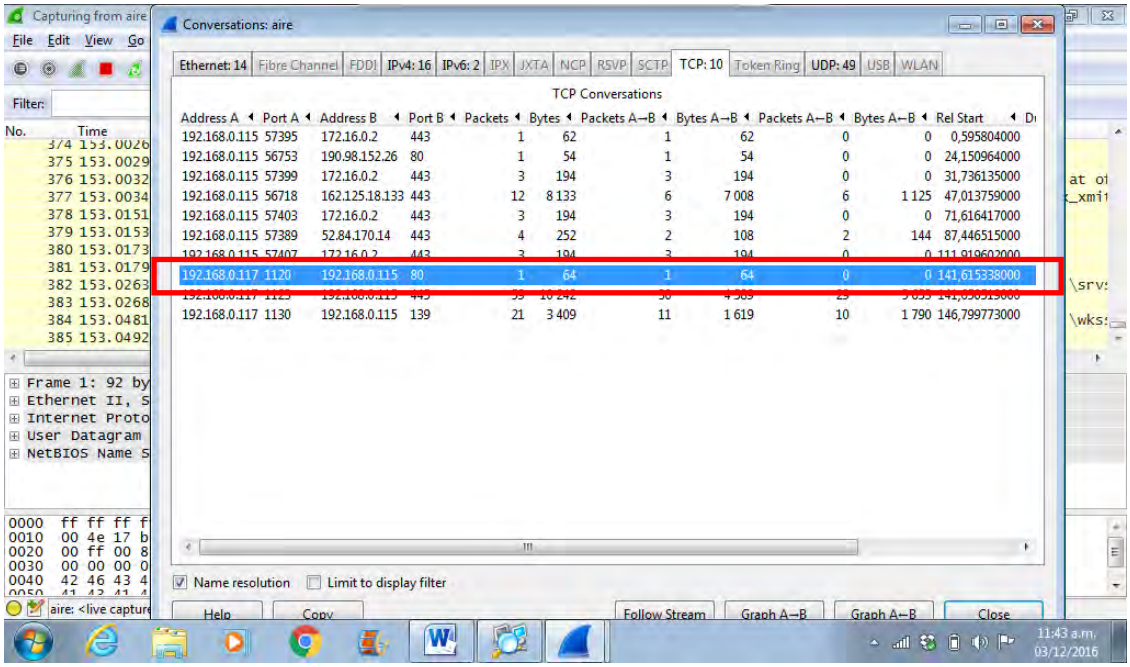
Caso N°15: 03/12/16



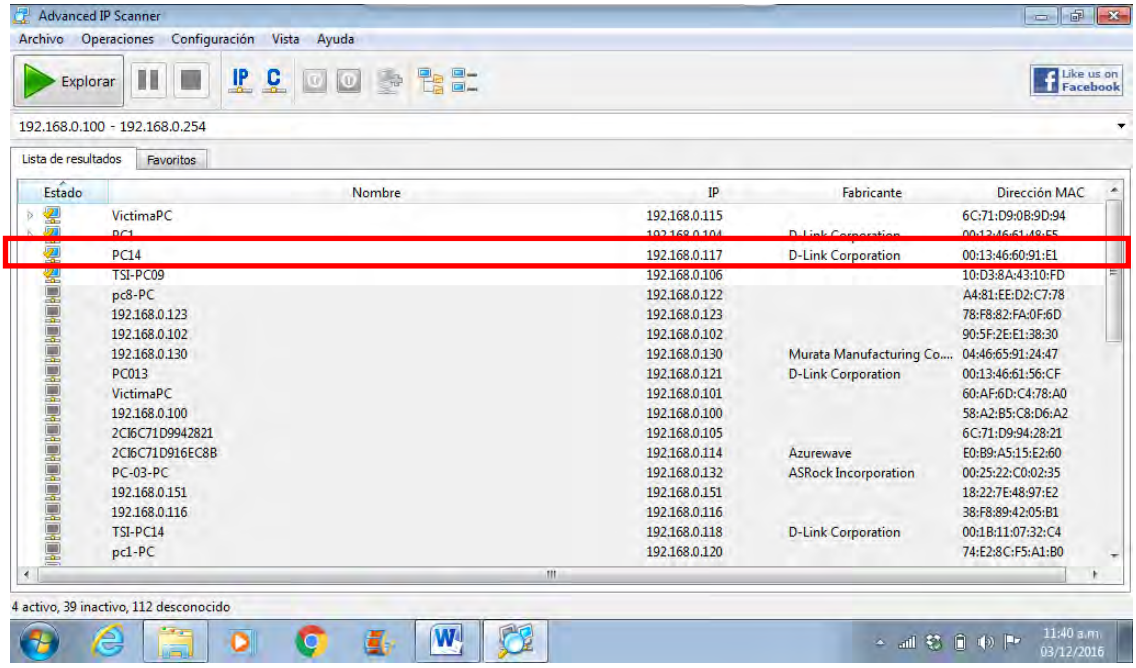
Captura de pantalla N° 15.1: Se establece conexión efectiva con la red "ZyXEL".



Captura de pantalla N° 15.2: Relevamiento de los dispositivos conectados a la red en tiempo real. Se identifica la computadora "VictimaPC" con direccion IP **192.168.0.115**, la cual va a ser la computadora receptora de las acciones ilicitas.

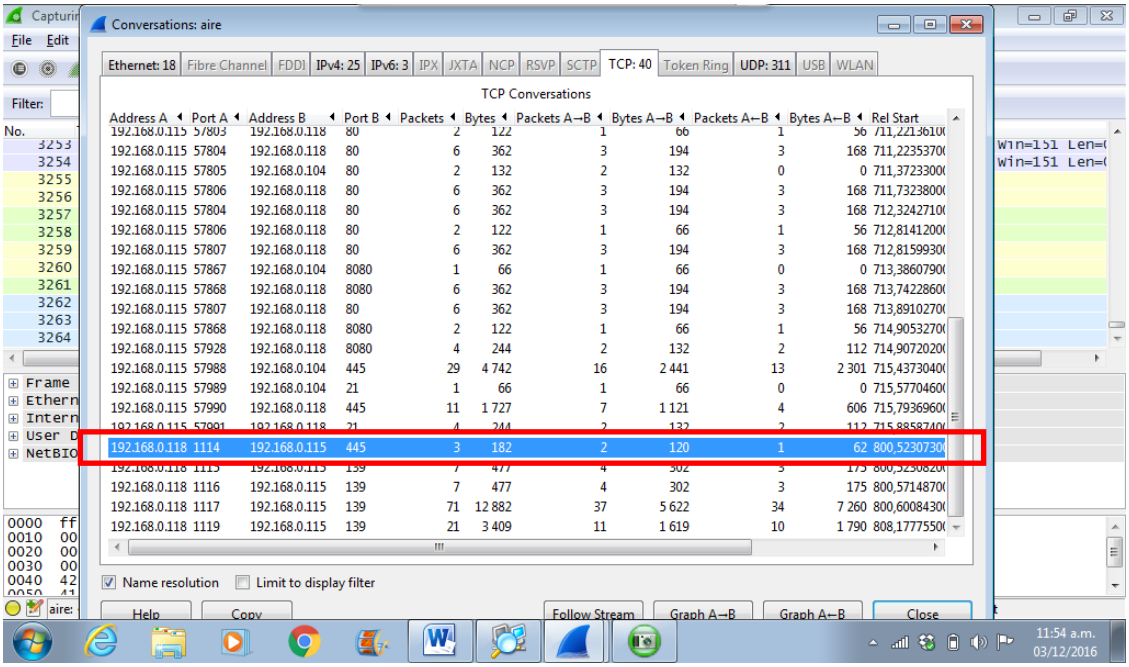


Captura de pantalla N° 15.3: Al ejecutar el programa Wireshark, en la ventana "Conversations: aire", dentro de la pestaña "TCP" se registra comunicación de la direccion IP **192.168.0.117** con la direccion IP **192.168.0.115.**

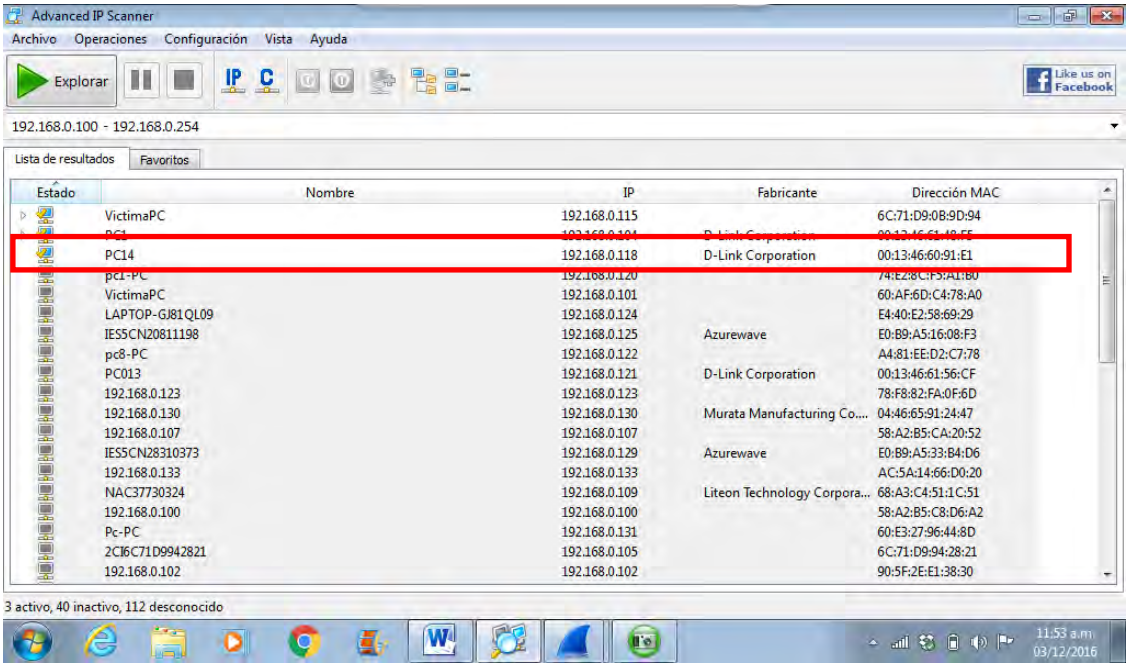


Captura de pantalla N° 15.4: En el relevamiento realizado con anterioridad se identifican las direcciones IP; siendo la IP **192.168.0.117** la asignada al hosts **"PC14"** con direccion MAC **00:13:46:60:91:E1**.

Desconexión de "PC14": computadora indicada como sospechosa de ilícito, para comprobar la dirección IP que le asigna el servidor cuando se reconecte



Captura de pantalla N° 15.5: Dejando correr el programa Wireshark se puede observar una segunda comunicación entre la dirección IP de la computadora "VictimaPC" y una IP hasta ahora desconocida: **192.168.0.118.**



Captura de pantalla N° 15.6: Al realizar un nuevo relevamiento de los dispositivos conectados a la red, se logra determinar que la dirección IP **192.168.0.118** corresponde al nombre **"PC14"** identificado anteriormente.

CONFIRMACIÓN

Se observa cambio de la dirección IP de 192.168.0.117 a 192.168.0.118; pero si se compara la dirección MAC que entablo comunicación con la dirección IP VictimaPC podemos confirmar que es la misma que en un primer momento: **00:13:46:60:91:E1**, correspondiente a una misma computadora.

El Tribunal Examinador otorga al presente Trabajo

La calificación de:…….

Equivalente a: …….

Fecha:……

T R I B U N A L

…….. ……..

Zalazar, Debora D. Ing. Zalazar, Dante

AUTOR DIRECTOR