CARRERA DE COMPUTACIÓN

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

TEMA:

EVALUACIÓN DE PROTOCOLOS DE SEGURIDAD DE LAS APP DE REDES SOCIALES EN DISPOSITIVOS MÓVILES ANDROID

AUTORES:
TERESA MARIBEL GARCÍA MOLINA
JORGE ALBERTO MOREIRA PÁRRAGA

TUTOR:
ING. FERNANDO RODRIGO MOREIRA MOREIRA, MBA.

CALCETA, JULIO 2016

DERECHOS DE AUTORÍA

Teresa Maribel García Molina y Jorge Alberto Moreira Párraga, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

_____ _____

TERESA M. GARCÍA MOLINA **JORGE A. MOREIRA PÁRRAGA**

CERTIFICACIÓN DE TUTOR

Fernando Rodrigo Moreira Moreira certifica haber tutelado la tesis **EVALUACIÓN DE PROTOCOLOS DE SEGURIDAD DE LAS APP DE REDES SOCIALES EN DISPOSITIVOS MÓVILES ANDROID**, que ha sido desarrollada por Teresa Maribel García Molina y Jorge Alberto Moreira Párraga, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____

ING. FERNANDO R. MOREIRA MOREIRA, MBA

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **EVALUACIÓN DE PROTOCOLOS DE SEGURIDAD DE LAS APP DE REDES SOCIALES EN DISPOSITIVOS MÓVILES ANDROID**, que ha sido propuesta, desarrollada y sustentada por Teresa Maribel García Molina y Jorge Alberto Moreira Párraga, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

LIC. JOSÉ G. INTRIAGO CEDEÑO, M. Ge.
MIEMBRO

ING. RAMÓN J. MOREIRA PICO, Mgtr.
MIEMBRO

ING. LUIS C. CEDEÑO VALAREZO, M. Sc.
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López por darnos la oportunidad de tener conocimientos sólidos y motivarnos a seguir mejorando día tras día, para ser unos profesionales eficientes en el ámbito laboral.

A nuestros padres, que con su apoyo nos han orientado por el buen camino de la vida para lograr todos y cada uno de nuestros objetivos y así crecer como futuros profesionales.

A nuestro tutor el Ing. Fernando Rodrigo Moreira Moreira, quien a través de sus conocimientos fue un guía importante para que nuestro trabajo fuera muy íntegro y fundamental para el desarrollo de la sociedad.

LOS AUTORES

DEDICATORIA

A Dios por darme la vida, a mis padres, que día a día me motivan y me llenan de fuerzas para no dejarme vencer por los obstáculos que se puedan presentar en la vida y así lograr las metas propuestas convirtiéndome en un pilar fundamental de mi existencia, también a nuestros catedráticos, ya que gracias a ellos y a los conocimientos que nos brindan estamos fortaleciendo nuestro perfil como futuros profesionales, a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ya que gracias a ella podemos fomentar mucho mejor en sus aulas del saber y ser Orgullosamente Estudiantes Politécnicos.

JORGE A. MOREIRA PARRAGA

DEDICATORIA

Primero a Dios por ser el creador del universo y permitirme llegar hasta aquí, a mis padres y hermanos por que fueron mi primer pilar de apoyo, a mi hijo que es quien me ayudo a esforzarme y ser fuerte para luchar por lo que se quiere para alcanzar todos nuestros objetivo en la vida , a nuestro tutor que nos guio y nos dio el apoyo en todo momento de desarrollo de la misma , a la Escuela Superior Politécnica Agropecuaria de Manabí y a nuestros docentes por ayudarnos y brindarnos los conocimientos básicos en toda la carrera en cada una de sus aulas y en general a cada una de aquellas personas que de una u otra forma me apoyaron e incentivaron a culminar una etapa más en mi vida.

TERESA M. GARCÍA MOLINA

CONTENIDO GENERAL

CONTENIDO DE CUADROS Y TABLAS

CONTENIDO DE IMÁGENES Y FIGURAS

RESUMEN

Los autores de la investigación consideraron los avances de la tecnología y la frecuencia de los riesgos a la que se expone diariamente, realizando un estudio enfocado en los protocolos de seguridad de las aplicaciones móviles Android, procediendo a evaluarlos con sus respectivas métricas mediante el análisis y/o monitoreo de los paquetes de datos enviados y recibidos desde un dispositivo móvil a otro y su afectación. Para esto, fue necesario el uso de herramientas como los programas Wireshark y Cain & Abel, las mismas que permitieron el flujo de la información y así obtener resultados para hacer el análisis correspondiente a los protocolos vulnerados, visualizados y a cada una de las encriptaciones en tiempo real. Se utilizó el método de investigación-experimental, método de la medición y la metodología por fases GQM (Goal Question Metric) que permitió identificar las vulnerabilidades más comunes y las métricas en el uso de los protocolos de seguridad de las Apps en el momento del envío o la recepción de la información y que le dio sustento científico en el período de mostrar datos en los parámetros de pruebas de los protocolos efectuadas respectivamente, verificando que las aplicaciones en Android no son totalmente vulnerables. Además uno de sus resultados muestra que el protocolo más seguro en cuanto a la encriptación de información es el HTTPS en las App móviles que manejan alto grado de transferencia de datos y en los anexos se refleja mediante fotos la respectiva evaluación para llegar a este resultado.

PALABRAS CLAVES

Protocolos de seguridad, evaluación, dispositivo móvil, redes sociales, método GMQ.

ABSTRACT

The authors of the research consider the advances in technology and frequency of risks to which is exposed daily, conducting a study focused on security protocols mobile applications Android, proceeding to evaluate their respective metrics through analysis and / or monitoring of data packets sent and received from a mobile device to another and involvement. For this, it was necessary to use tools like Wireshark and Cain & Abel, the same that allowed the flow of information programs and obtain results for the corresponding protocols violated analysis, displayed and each encryptions time real. the research method-experimental method of measurement and methodology phased GQM (Goal Question Metric) which identified the most common vulnerabilities and metrics in the use of security protocols of the Apps when shipping was used or receipt of the information and gave scientific support in the period of display data on the parameters of tests performed respectively protocols, verifying that applications on Android are not completely vulnerable. Also one of the results shows that the safest in terms of data encryption protocol is HTTPS in mobile App that handle high data transfer and annexes reflected by photos the respective evaluation to achieve this result.

KEYWORDS

Security protocols, evaluation, mobile, social networks, GMQ method.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

En la actualidad mantener la seguridad es el objetivo a lo que más se deben enfocar las redes inalámbricas, ya que la señal se propaga por el aire en todas las direcciones y puede ser captada a distancia, utilizando una notebook con antena o cualquier dispositivo móvil.

Esta debe estar basada en protocolos diseñados para soportar los ataques de carácter malicioso de los hackers y protegerse contra ellos, pero esta protección generalmente tiene ciertas condiciones referentes a los riesgos que el sistema está expuesto a considerar en el momento en que la información está siendo vulnerada.

Entre los tipos de protocolos que existen y que son definidos por las empresas al momento de instalarlo tenemos: WEP, WPA y WPA2, utilizados para la seguridad de redes inalámbricas.

Estas conexiones inalámbricas se han popularizado en el pasar del tiempo y son utilizadas tanto en el hogar, las empresas y espacios públicos a través de dispositivos móviles inteligentes y computadores portátiles que les permite la difusión o transmisión de información, tanto que ha impulsado a que la tecnología esté en constante crecimiento y actualización, siendo reemplazada las redes cableadas por preferencia de los usuarios.

Para hacer posible esta transmisión de información entre redes de computadoras, se utiliza el protocolo de comunicación TCP/IP, que es muy conocido a nivel mundial y ha llegado a ser la base de Internet para la comunicación. De esta manera los dispositivos móviles tienen dos formas de comunicación como son mediante el uso de datos móviles y red WiFi.

Así mismo las redes sociales se han convertido en un fenómeno estos últimos años, ya que no sólo las utilizan las personas en la vida cotidiana para comunicarse e intercambiar información de una forma más rápida en el medio en que conviven, sino que también las utilizan grandes empresas como corporaciones, organizaciones y compañías para dar a conocer sus productos y servicios de una forma amplia a sus consumidores o asociados.

Debido a esta expansión tecnológica, la seguridad de la información se puede volver más vulnerable sino se toma las debidas precauciones por parte de los usuarios al momento de chequear sus archivos en una red Wi-Fi.

ESET, s.f. refiere que en todos estos ambientes en las que son utilizadas las redes inalámbricas, cabe la posibilidad de que el usuario se conecte a una red Wi-Fi insegura, lo que podría causar problemas de diversa índole como el robo de archivos personales o de contraseñas de acceso a bancos, redes sociales u otros servicios, como también otro tipo de incidentes de seguridad, lo que obliga a empresas e ingenieros a realizar una evaluación exhaustiva de los protocolos de seguridad para determinar un nivel de protección y seguridad en base a cada necesidad de las App en redes sociales de dispositivos móvil Android que son las más utilizadas en la actualidad.

Los autores observan que las aplicaciones en redes sociales pueden estar expuestos a la vulnerabilidad de la información en dispositivos móviles Android se plantean la siguiente interrogante:

¿De qué manera verificar el funcionamiento de las App en los dispositivos móviles Android?

1.2. JUSTIFICACIÓN

Según el Art. 8 de la Ley Orgánica de Educación Superior (2010) establece fomentar y ejecutar programas de investigación de carácter científico, tecnológico y pedagógico que coadyuven al mejoramiento y protección del ambiente y promuevan al desarrollo.

Esta investigación beneficiará a las empresas que promocionan sus productos y servicios a través de redes sociales, brindándole seguridad al usuario en el momento de entregar información personal en cualquier medio y/o dispositivo móvil y a la vez ayudará al crecimiento tanto económico como en la fiabilidad para el consumidor.

Debido a los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi por la masificación de usuarios, hace que haya mucha interferencia en la conexión ya que estas redes son diseñadas para un corto alcance y se expone a un alcance mayor su riesgo de interferencia es excesivo también.

Por este motivo los protocolos de aplicaciones móviles se especifican en la norma Wireless Application Protocol (WAP), que es un estándar de seguridad creado para proporcionar los datos interactivos en tiempo real a través de una red de telefonía móvil, mediante la integración de datos inalámbricos y de Internet de manera que la transmisión de datos se ajuste y sea accesible por los dispositivos de mano.

Por lo cual esta evaluación servirá para determinar los protocolos de seguridad con los que cuentan las aplicaciones de redes sociales en dispositivos móviles y de esta manera identificar las vulnerabilidades más comunes en cuanto a seguridad en el uso de App de redes sociales en dichos dispositivos Android.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Evaluar métricas de seguridad en los protocolos de las App de redes sociales para determinar el correcto funcionamiento de las mismas en dispositivos móviles Android.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar los protocolos de seguridad con los que cuentan las aplicaciones de redes sociales en dispositivos móviles.

- Identificar las vulnerabilidades más comunes y métricas en el uso de los protocolos de seguridad de las aplicaciones de redes sociales de dispositivos móviles Android.

- Recolectar los datos de las pruebas de los protocolos de seguridad de los dispositivos móviles Android, mediante diferentes software para la comprobación de la vulnerabilidad de los mismos.

1.4. HIPÓTESIS, PREMISAS Y/O IDEAS A DEFENDER

Los protocolos de seguridad utilizados por las aplicaciones de redes sociales en dispositivos móviles Android tienen vulnerabilidades en el envío y recepción de datos.

CAPITULO II. MARCO TEÓRICO

2.1. DEFINICIÓN EVALUACIÓN

Según Cano (2008) citado por Ruiz (2014) en la definición de evaluación expresa el término de evaluación como una palabra elástica que tiene usos diferentes y que puede aplicarse a una gama muy variada de actividades humanas. Considerada la evaluación en su acepción más amplia, nos encontramos con definiciones como la de la Real Academia Española: evaluar es “señalar el valor de una cosa”. Para el Diccionario del Español Actual, evaluar significa “valorar (determinar el valor de alguien o de algo)”. Y, en cuanto al término evaluativo/va, en el diccionario mencionado se distingue “un uso evaluativo y un uso descriptor”, en el empleo del término. En el uso evaluativo hay un juicio de valor.

Como una primera aproximación a la precisión conceptual del término, podemos decir que la palabra evaluación designa el conjunto de actividades que sirven para dar un juicio, hacer una valoración, medir “algo” (objeto, situación, proceso) de acuerdo con determinados criterios de valor con que se emite dicho juicio. En la vida cotidiana permanentemente estamos valorando sobre todo cuando ponderamos las acciones y decisiones que tomamos. Son formas de evaluación informal, las que no necesariamente se basan en una información suficiente y adecuada, ni pretenden ser objetivas y válidas. Pero cuando queremos evaluar servicios o actividades profesionales no basta la evaluación informal. Debemos recurrir a formas de evaluación sistemática que, utilizando un procedimiento científico, tienen garantía de validez y fiabilidad. (Cano, 2008) citado por (Ruiz, 2014).

En la actualidad, la mayoría de los desarrolladores se basan en las evaluaciones manuales. Solo el 8% de 300 desarrolladores usaban algún tipo de producto de evaluación móvil, esto hace que los desarrolladores que aplican evaluaciones de aplicaciones móviles tengan un porcentaje más de

acierto y menos errores en codificación y aceptación de los usuarios, permitiendo ahorrar tiempo y dinero.

2.2. MÉTRICAS

Por su parte, Peñalva (2014) refiere que una métrica contiene la definición de un método de medición o un método de cálculo y la escala asociada. El método de medición es la secuencia lógica particular de operaciones y posibles heurísticas, especificada para permitir la realización de la descripción de una métrica por una actividad de medición. Por otro lado, la escala se define como un conjunto de valores con propiedades definidas.

Las métricas que se usan para los sistemas orientados a objetos se enfocan en la medición que puede aplicarse a cada clase y a las características de diseño (encapsulación, herencia, etc.). Estos indicadores se construyen en base a métricas y la importancia de su construcción es que proporcionan información con mayor nivel de abstracción útil para las decisiones. Los indicadores globales se construyen como agregación de indicadores individuales. Para los indicadores es importante establecer el criterio de aceptabilidad por ejemplo rango: de insatisfacción, de aceptación mínima, y de satisfacción (Peñalva, 2014).

MEDICIÓN DE LA SEGURIDAD

La seguridad es una preocupación constante, cuando no creciente, tanto para los técnicos a cargo de los sistemas, como para los gestores de la organización. La seguridad técnica de los sistemas es un requisito indispensable; pero más allá de la técnica, los gestores necesitan tener confianza en que el sistema de información permitirá alcanzar los objetivos propuestos y establecer relaciones fructíferas con otras organizaciones. En este contexto, las métricas aparecen como necesarias para conocer el estado actual de la seguridad (Steffens, 2010).

Según estos conceptos los autores consideran que para aplicar estas métricas, se lo debe hacer mediante la combinación de la metodología GQM tomando en cuenta la medición de seguridad que aparecen en las mismas, la cual va ser detallada a través de niveles en el desarrollo metodológico de esta investigación.

2.3. PROTOCOLOS DE SEGURIDAD

Según Bolois (2013) un protocolo de seguridad (también llamado protocolo criptográfico o protocolo de cifrado) es un protocolo abstracto o concreto que realiza funciones relacionadas con la seguridad, aplicando métodos criptográficos. Los protocolos criptográficos se usan ampliamente para transporte de datos seguros a nivel de aplicación. Un protocolo criptográfico comúnmente incorpora por lo menos uno de los siguientes aspectos:

- Establecimiento de claves
- Autenticación de entidades
- Cifrado simétrico y autenticación de mensajes
- Transporte de datos en forma segura a nivel de aplicación
- Métodos de no repudio.

Según Lara *et al.* (2014) refiere que el primer intento con cierta relevancia en busca de un acceso universal del contenido de Internet en movilidad fue el uso de la tecnología imode, que se hizo muy popular en Japón y servía para generar minipáginas para dispositivos móviles y asistentes digitales personales (PDA). A su vez, comenzaba a despegar el WML (wireless markup language), un metalenguaje que permitía visualizar páginas web en entornos móviles caracterizado por el uso de la tecnología WAP (wireless application protocol), un protocolo de aplicaciones inalámbricas.

Posteriormente se extendió el uso del XHTML-MP (extensible hypertext markup language mobile profile) como un lenguaje diseñado exclusivamente para

teléfonos móviles. A partir de este punto, hay que indicar que han existido diferentes evoluciones, para generar un lenguaje que cubriera la necesidad de ubicuidad de la información, propias de las diferentes etapas que han registrado las telecomunicaciones inalámbricas como el GSM o 2G (global system for mobile communications), UMTS o 3G (universal mobile telecommunication system) y LTE o 4G (long term evolution) (Lara, *et al.*, 2014).

2.3.1. TIPOS DE PROTOCOLOS DE COMUNICACIÓN

Dentro de las redes informáticas se conoce bajo el nombre de protocolo al lenguaje, que es un conjunto de reglas formales, que permiten la comunicación de distintas computadoras entre sí. Dentro de las distintas redes, como Internet, existen numerosos tipos de protocolos. Ver **Tabla 2.1.**

PROTOCOLO	DESCRIPCIÓN
TPC/IP	TCP/IP se lo define como el conjunto de protocolos básicos para la comunicación de redes y es por medio de él que se logra la transmisión de información entre computadoras pertenecientes a una red. Gracias al protocolo TCP/IP los distintos ordenadores de una red se logran comunicar con otros diferentes y así enlazar a las redes físicamente independientes en la red virtual conocida bajo el nombre de Internet.
TCP	El TCP (Transmision Control Protocol) es un protocolo orientado a las comunicaciones y ofrece una transmisión de datos confiable. El TCP es el encargado del ensamble de datos provenientes de las capas superiores hacia paquetes estándares, asegurándose que la transferencia de datos se realice correctamente.

HTTP	HTTP (Hypertext Transfer Protocol) protocolo permite la recuperación de información y realizar búsquedas indexadas que permiten saltos intertextuales de manera eficiente. Por otro lado, permiten la transferencia de textos de los más variados formatos, no sólo HTML. El protocolo HTTP fue desarrollado para resolver los problemas surgidos del sistema hipermedia distribuidos en diversos puntos de la red.
FTP	FTP (File Transfer Protocol) es utilizado a la hora de realizar transferencias remotas de archivos. Lo que permite es enviar archivos digitales de un lugar local a otro que sea remoto o al revés. Generalmente, el lugar local es la PC mientras que el remoto el servidor.
SSH	SSH (Secure Shell) fue desarrollado con el fin de mejorar la seguridad en las comunicaciones de internet. Para lograr esto el SSH elimina el envío de aquellas contraseñas que no son cifradas y codificando toda la información transferida.
UDP	UDP (User Datagram Protocol) es un protocolo de datagrama de usuario está destinado a aquellas comunicaciones que se realizan sin conexión y que no cuentan con mecanismos para transmitir datagramas. Esto se contrapone con el TCP que está destinado a comunicaciones con conexión. Este protocolo puede resultar poco confiable excepto si las aplicaciones utilizadas cuentan con verificación de confiabilidad.
SNMP	SNMP (Simple Network Management Protocol) usa el Protocolo de Datagrama del Usuario (PDU) como mecanismo para el transporte. Por otro lado, utiliza distintos términos de TCP/IP como agentes y administradores en lugar de servidores y clientes. El administrador se comunica por medio de la red, mientras que el agente aporta la información sobre un determinado dispositivo.

TFTP	TFTP (Trivial File Transfer Protocol) protocolo de transferencia se caracteriza por sencillez y falta de complicaciones. No cuenta con seguridad alguna y también utiliza el Protocolo de Datagrama del Usuario como mecanismo de transporte
SMTP	SMTP (Simple Mail Transfer Protocol) protocolo está compuesto por una serie de reglas que rige la transferencia y el formato de datos en los envíos de correos electrónicos. SMTP suele ser muy utilizado por clientes locales de correo que necesiten recibir mensajes de e-mail almacenados en un servidor cuya ubicación sea remota.
ARP	ARP (Address Resolution Protocol) mediante la utilización de este protocolo se logran aquellas tareas que buscan asociar a un dispositivo IP, el cual está identificado con una dirección IP, con un dispositivo de red, que cuenta con una dirección de red física. ARP es muy usado para los dispositivos de redes locales Ethernet. Por otro lado, existe el protocolo RARP y este cumple la función opuesta a la recién mencionada.

Tabla 2.1. Tipos de Protocolos
Fuente: Taopantaurkund, 2011

2.3.2. TIPOS DE PROTOCOLOS DE SEGURIDAD

La tecnología Wi-Fi (Wireless Fidelity) es una de las tecnologías líder en la comunicación inalámbrica, y el soporte para Wi-Fi se está incorporando en cada vez más aparatos: portátiles, PDAs o teléfonos móviles. De todas formas, hay un aspecto que en demasiadas ocasiones pasa desapercibido: la seguridad (Lehembre, 2010). A continuación se detalla los protocolos de seguridad de los métodos de encriptación:

WEP

El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso. RC4 consiste en generar una clave de

forma pseudo-aleatoria que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica XOR (O exclusiva), obteniendo como resultado un texto cifrado. La clave pseudo-aleatoria se genera utilizando una clave secreta que define el propio usuario con una longitud de 40 o 104 bits y un vector de inicialización (IV) de 24 bits que lo genera aleatoriamente el sistema para cada trama. Pero WEP tenía muchos defectos como era la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP. Por lo tanto la IEEE trabajaba en otro algoritmo más potente, pero la Alianza Wi-Fi lanzó un algoritmo alternativo y más potente que WEP, llamado WPA (Ramírez, *et al.*, 2011).

WPA

WPA (Wifi Protect Access) es el protocolo de seguridad que lanzó la Alianza Wi-Fi para solucionar los problemas de seguridad del protocolo WEP.

Este protocolo implementa las siguientes mejoras:

• Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos).

• Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits).

• Utiliza el intercambio dinámico de claves mediante el protocolo TKIP (Temporal Key Integrity Protocol).

• El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code). Posteriormente el IEEE publicó el estándar 802.11i, también conocido como WPA2 (Ramírez, *et al.*, 2011).

WPA2

Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro. Incluye el intercambio dinámico de

la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes:

• Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes (Ramírez, *et al.*, 2011).

Según Sanz (2013) refiere que a la hora de cifrar nuestra conexión Wi-Fi existen dos maneras de cifrarlo con WPA y WPA2 (basado en el nuevo estándar 802.11i).

El **WPA-PSK / WPA2-PSK** (pre-shared key) o clave pre compartido, con dos modos de seguridad:

- **TKIP:** (Temporal Key Integrity Protocol), la cual no es del todo segura, sobre todo si se usa conjuntamente con QoS.
- **AES:** (Advanced Encryption Standard), un algoritmo de cifrado más seguro.

En cualquiera de estos dos tipos de cifrados existe la posibilidad de que un atacante este capturando tráfico en el momento que nos autentiquemos contra el AP y que capture el “handshake”, ya que todas las claves pre compartidas son vulnerables a capturarse e intentar descifrarlas con ataques por diccionario, cosa que no ocurre con un servidor radius, ya que genera las claves aleatoriamente.

DIFERENCIA ENTRE LOS CIFRADOS TKIP Y AES

La diferencia de forma muy rápida: **TKIP** (*Temporal Key Integrity Protocol*) es un conjunto de algoritmos de seguridad que funcionan como un “envoltorio” para WEP. Fue diseñado para obtener la mayor seguridad posible en dispositivos WLAN antiguos equipados con WEP sin necesidad de actualizar el

hardware. El problema del WEP original es que un atacante podría obtener tu clave “esnifando” una cantidad relativamente pequeña del tráfico. TKIP resuelve dicho problema re-negociando una clave nueva cada pocos minutos (el atacante nunca tendría suficiente información para descubrirla) (Sanz, 2013).

En la actualidad TKIP no es fiable ni eficiente para proteger un entorno WLAN. Por eso el estándar 802.11i especifica el protocolo **AES** (*Advanced Encryption Standard*) como un mecanismo adicional de seguridad.

AES ofrece un mayor nivel de seguridad, pero requiere un hardware específico que no es compatible con los dispositivos que sólo funcionaban con WEP y con WPA. Utiliza bloques de cifrado de 128, 192 o 256 bits y es considerado el sistema de cifrado estrella. Es cierto que AES necesita más potencia de cálculo y eso repercute en el consumo de algunos dispositivos móviles. Pero AES no sólo es más seguro, sino también más eficiente ya que necesita menos ancho de banda. Sin duda es la mejor opción para los sistemas WLAN actuales.

Según Sanz (2013) WEP y WPA utilizan TKIP. WPA2 es infinitamente más seguro y utiliza AES, pero también puede usar TKIP por *retro-compatibilidad* (así WPA2 podría aceptar conexiones WPA).

WPA2 EMPRESARIAL (SERVIDOR RADIUS)

En este tipo de configuración, básicamente tenemos una máquina conectada por cable al punto de acceso, el cual manda las peticiones de autenticación a este servidor (normalmente por el puerto UDP 1812 y 1813). Los servidores radius también se utilizan por ejemplo, cuando un *ISP* quiere validar las credenciales de un abonado (Sanz, 2013).

Existe un pequeño inconveniente en este tipo de configuraciones *Wireless* y es que dispositivos multimedia como pueden ser una PlayStation 3, Xbox 360, un NAS o una BlackBerry (no es el caso de Android e IOS), o en general un dispositivo de uso doméstico, no tienen la capacidad de conectarse directamente a un servidor radius ya que carecen de la posibilidad de tener una

configuración con certificados, ya sea porque el fabricante no la ha incluido o porque el dispositivo no lo permite. Para estos casos siempre existe la opción de conectarlos por cable a un segundo dispositivo que sí que sea capaz de conectarse a un servidor radius y comparta la conexión, haciendo de puente, o tener doble *SSID* en nuestra red donde uno de los *SSID* funciona con WPA-PSK (Sanz, 2013).

2.4. APLICACIONES MÓVILES

De acuerdo a González (2013), una aplicación móvil o App es una aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles. Por lo general se encuentran disponibles a través de plataformas de distribución, operadas por las compañías propietarias de los Sistemas Operativos Móviles como Android, iOS, BlackBerry OS, Windows Phone, entre otros.

Según Roca (2014) las redes sociales forman parte del conjunto de medios sociales, o social media, que están a disposición de la sociedad y de sus ciudadanos y agentes y que están produciendo una revolución a gran escala. Gracias a su extraordinario potencial, las redes sociales presentan enormes posibilidades para todo: para el individuo como ciudadano del mundo, para el ciudadano como consumidor, para el individuo que tiene necesidades de comunicación, y para las empresas y organizaciones.

Según Vizuete (2012) refiere a que los estudios efectuados revelan que los usuarios han realizados las compras de sus dispositivos móviles considerando como funciona una determinada aplicación. Desde el 2007 empezó la era de las aplicaciones móviles siendo iPhone un pionero, pues uno de cada tres usuarios móviles descargan aplicaciones, por lo tanto estas descargar se pueden convertir en un negocio muy rentable en el país.

Muchos usuarios creen que el uso de las aplicaciones móviles puede mejorar su vida, pues buscan aquellas que les sean más útiles para sí mismo. Varias

de estas aplicaciones en línea recolectan datos de sus usuarios y de esta manera obtienen estadísticas e información necesaria para actualizar sus aplicaciones o desarrollar nuevas y de esta manera mantenerse en el mercado siendo los más descargados los siguientes:

- ✓ Los juegos con el 38% de descargas.
- ✓ Redes sociales con el 35% de descargas.
- ✓ Música con el 29% de descargas.
- ✓ Las más descargadas a nivel global son redes sociales con el 31%, juegos 29% y utilidades 25% siendo estas las más utilizadas (Vizuete, 2012).

Sei (2014) menciona que no hay forma de saber si una aplicación puede dañar tu celular de forma exacta y precisa pero, sí te mantendrá más seguro instalar desde el App Store que el software (Android, Apple, Microsoft y Blackberry) recomienden siempre para la descarga segura. Si es el caso, no te olvides de verificar su reputación y, sin importar de donde provenga la App, verificar que sus permisos no sean abusivos y absurdos.

En Android Jefe casi siempre ofrecemos aplicaciones que están en Google Play, que son probadas personalmente por nosotros, y que cumplen con el resto de lo dicho aquí. Los escasos archivos APK ofrecidos aquí también son probados. Adicionalmente, estos son extraídos de fuentes fiables donde el feedback de usuarios reales es positivo (Sei, 2014).

2.5. TIENDAS MÓVILES

Para descargar o ver una aplicación, se necesita un Smartphone o algún otro aparato móvil con acceso a Internet. No todas las aplicaciones funcionan en todos los aparatos móviles. Cuando usted compra uno de estos aparatos debe usar el sistema operativo y el tipo de aplicaciones que corresponde a ese aparato. Los sistemas operativos móviles Android, Apple, Microsoft y BlackBerry tienen tiendas de aplicaciones que operan en línea en las cuales usted puede buscar, descargar e instalar las aplicaciones. (González, 2013).

Según Martínez (2012), estas tiendas de aplicaciones o más conocidas como App Store han logrado convertirse en los últimos tiempos en un importante canal para la distribución de todo tipo de aplicaciones. Esta infografía detallada llevada a cabo por los responsables de shoutem.com ilustra la historia y evolución de las cinco tiendas más exitosas en aplicaciones móviles las cuales son: **Ver Imagen 2.1**

- ✓ Android Market
- ✓ iPhone App Store
- ✓ Ovi Store
- ✓ BB App World
- ✓ Windows Phone Marketplace.
- ✓ HP App Catalog
- ✓ Amazon Appstore.

	Apple App Store	Android Market	Windows Phone Marketplace	BlackBerry App World	Nokia OVI Store	HP App Catalog	Amazon Appstore
Fecha de apertura	10/07/2008	22/10/2008	21/10/2010	01/04/2009	26/05/2009	06/06/2009	22/03/2011
Sistema Operativo	iOS	Android	Windows Phone	BlackBerry OS	Symbian, MeeGo, Maemo, S40	webOS	Android
Número de aplicaciones	550.000 (ene'12)	400.000 (ene'12)	61.500 (ene'12)	43.000 (nov'11)	116.000 (dic'11)	10.000 (dic'11)	27.000 (ene'12)
Aplicaciones gratuitas	37%	67%	61%	26%	26%	-	37%
Precio medio por aplicación	3,84 $ (sep'11)	3,30 $ (sep'11)	3,29 $ (sep'11)	4,17 $ (sep'11)	-	-	-
Número de descargas	18.000 M (oct'11)	11.000 M (ene'12)	-	2.000 M (ene'12)	4.000 M (ene'12)	108 M (ago'11)	-
Número de desarrolladores	~ 185.000	~ 67.000	~ 15.000	-	-	-	-
Cuota de suscripción	99 $/año	25 $	99 $/año	Gratis	1 €	Gratis	99 $/año
Comisión para la compañía	30%	30%	30%	30%	30%	30%	30%
Países en que está disponible	123	135	41	124	232	10	1

Imagen 2.1. Cuadro de Comparación entre las Tiendas Móviles
Fuente: Martínez (2012)

2.6. TIPOS DE APLICACIONES MÓVILES

Las aplicaciones se ejecutan directamente en el dispositivo, actualmente hay tres tipos de aplicaciones móviles las cuales son:

- ✓ Nativas
- ✓ Web
- ✓ Híbridas

2.6.1. APLICACIONES NATIVAS

El autor Branding (2012) manifiesta que las nativas son las aplicaciones diseñadas para el sistema operativo de cada dispositivo móvil. Sus desventajas es que son más complicadas y costosas de desarrollar porque hay que programar una versión para cada sistema operativo. En cuanto a sus ventajas hay que destacar que pueden utilizar servicios integrados en el dispositivo como la cámara, la agenda.

2.6.2. APLICACIONES HÍBRIDAS

Estas aplicaciones se desarrollan también con lenguajes de programación estándar pero posteriormente son traducidas mediante programas informáticos a lenguajes de programación concebidos para sistemas operativos de smartphones. Esto permite que sean instaladas en el dispositivo como las nativas (Branding, 2012).

2.6.3. APLICACIONES WEB

De acuerdo a lo mencionado por Branding (2012) se denominan así porque son aplicaciones que se programan con lenguaje estándar (web) y funcionan desde un servidor externo. Su ventaja es que son compatibles con todos los sistemas operativos, con lo cual los costes de desarrollo, en cuanto a tiempo y dinero se refiere, disminuyen considerablemente. Entre sus desventajas está que no

pueden utilizar las herramientas del dispositivo y que no pueden instalarse para utilizarlas sin internet por ejemplo.

Menéndez y Barzanallana (2012) refieren que desde la perspectiva de un usuario, puede ser difícil percibir la diferencia entre un sitio web y una aplicación web. Según el **Diccionario Oxford** en línea, nos enteramos que una aplicación es "un programa o conjunto de programas para ayudar al usuario de un ordenador para procesar una tarea específica". Una aplicación web es básicamente una manera de facilitar el logro de una tarea específica en la Web, a diferencia de un sitio web estático que es más bien una herramienta, no menos importante, para la comunicación. El término más decisivo de esta definición es "tarea específica". La aplicación web por lo tanto permite al usuario interactuar directamente contigo y tus datos, todo en forma personalizada.

2.7. REDES SOCIALES

Según el Observatorio Nacional de las telecomunicaciones y de los sistemas de información (2011) existen múltiples definiciones y teorías sobre qué son y qué no son las redes sociales, pero existe poco consenso todavía sobre las mismas. La gran mayoría de autores coinciden en que una red social es: “un sitio en la red cuya finalidad es permitir a los usuarios relacionarse, comunicarse, compartir contenido y crear comunidades”, o como una herramienta de “democratización de la información que transforma a las personas en receptores y en productores de contenidos”.

En España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) en su “Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online”, del año 2009, las define como “los servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo,

disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado" (ONTSI, 2011).

2.7.1. TIPOS DE REDES SOCIALES QUE INTERACTÚAN CON DISPOSITIVOS MÓVILES

Hütt (2012) cita a la autora Celaya (2008), para expresar que existen tres clasificaciones principales de redes sociales:

1. Redes profesionales (por ejemplo, LinkedIn, Xing, Viadeo).
2. Redes generalistas (por ejemplo, MySpace, Facebook, Tuenti, Hi5).
3. Redes especializadas (por ejemplo, Ediciona, eBuga, CinemaVIP, 11870).

Aunque es probable que hayan quedado otros muchos tipos de redes, estas son las que obedecen a una agrupación más general y son las que tienen un mayor nivel de visitas, según registros oficiales (Hútt, 2012).

2.7.2. PRIVACIDAD

Las redes sociales se han convertido en bases de datos en la que se recogen informaciones de carácter personal y documentos sobre las actividades de la vida real de las personas que hacen uso de ellas. Campos como el estado civil y la ciudad de residencia son habituales en este tipo de páginas y mucha gente cree que rellenando este tipo de campos en nuestro perfil, aun cuando no son obligatorios para el registro, van a ser usuarios más activos, pero la realidad es que estamos poniendo al alcance de cualquiera, datos que no hace mucho tiempo evitábamos dar con tanta facilidad (Ortega, 2011).

2.8. METODOLOGÍA

Los autores definen a las metodologías con el conjunto de prescripciones que se explotan a lo largo de una investigación científica, a la que se hace referencia al conjunto de procedimientos basados en principios lógicos, la cual utilizamos para alcanzar una serie de objetivos, los cuales son el objetivo de la

investigación mediante la aplicación de las fases o procesos los cuales nos dispongan la metodología a utilizar para cumplir con culminar un proyecto o trabajo organizado de acuerdo a las fases aplicadas.

De acuerdo con Pérez (2012) en los proyectos de mejora existen numerosas prácticas, técnicas y metodologías que ayudan a cubrir las diferentes necesidades de la organización. La aplicación de unas u otras depende de los requerimientos del negocio y las exigencias del mercado. Es importante considerar una estrategia adecuada y tomar de cada una lo que mejor se ajuste a la organización.

El resumen que se presenta a continuación no pretende cubrir todo el espectro disponible, pero al menos presenta los elementos generales que le permitan evaluar las diferentes alternativas, así como las direcciones de Internet donde puede obtener mayor información.

2.8.1. INVESTIGACIÓN EXPERIMENTAL

Según Serrano *et al.* (2010) en la investigación de enfoque experimental el investigador manipula una o más variables de estudio, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas. Dicho de otra forma, un experimento consiste en hacer un cambio en el valor de una variable (variable independiente) y observar su efecto en otra variable (variable dependiente).

Según Van Dalen y Meyer (2010) expresa que la investigación experimental sigue las siguientes etapas:

1. Delimitar y definir el objeto de la investigación o problema. Consiste en determinar claramente los objetivos del experimento y las preguntas que haya que responder. Después se señalan las variables independientes, las dependientes, los parámetros constantes y la precisión necesaria en la medición de las variables. Se toma en cuenta la bibliografía existente, la región

en que interesan los resultados, el equipo disponible y su precisión, y el tiempo y dinero disponibles.

2. Plantear una hipótesis de trabajo. Toda investigación comienza con una suposición, un presentimiento o idea de cómo puede ocurrir el fenómeno. Estas ideas deben estar suficientemente claras para adelantar un resultado tentativo de cómo puede ocurrir dicho fenómeno: éste resultado tentativo es la hipótesis.

3. Elaborar el diseño experimental. Ya conocida la naturaleza del problema (si es de investigación, ampliación o confirmación), la precisión deseada, el equipo adecuado y planteada la hipótesis de trabajo, se debe analizar si la respuesta a nuestro problema va a ser la interpretación de una gráfica, un valor o una relación empírica; esto nos señalará el procedimiento experimental, es decir cómo medir, en qué orden, y qué precauciones tomar al hacerlo. Una vez determinadas estas etapas se procede a diseñar el experimento mediante los siguientes pasos: Determinar todos y cada uno de los componentes del equipo, acoplar los componentes, realizar un experimento de prueba e interpretar tentativamente los resultados y comprobar la precisión, modificando, si es necesario, el procedimiento y/o equipo utilizado.

4. Realizar el experimento. Una vez realizado el experimento de prueba y la interpretación tentativa de resultados, realizar el experimento final casi se reduce a llenar columnas, preparadas de antemano, con lecturas de las mediciones, a detectar cualquier anomalía que se presente durante el desarrollo del experimento y a trazar las gráficas pertinentes o calcular el o los valores que darán respuesta al problema.

5. Analizar los resultados. El análisis o interpretación de resultados, ya sean valores, gráficas, tabulaciones, etc., debe contestar lo más claramente posible la o las preguntas planteadas por el problema.

6. Obtener conclusiones. Ya logrados los resultados del experimento el investigador debe aplicar su criterio científico para aceptar o rechazar una

hipótesis o una ley; también es posible que haga alguna conjetura acerca de un modelo, o proponga la creación de otro nuevo, lo que conduciría a un nuevo problema. En las conclusiones se responden con claridad las preguntas planteadas en el experimento, comprobar si es o no válida nuestra hipótesis de trabajo o el modelo propuesto. Si hay preguntas sin respuesta, establecer por qué o si amerita, conjeturar acerca de la hipótesis o modelo que describa el fenómeno estudiado.

Esta investigación será aplicada en el desarrollo metodológico mediante el método Goal Question Metrics-GQM (Meta-Pregunta-Métrica).

2.8.2. EL MÉTODO DE LA MEDICIÓN

En la práctica, la especificación o definición requerida del mensurando es función de la exactitud de medida requerida por la medición. El mensurando debe definirse lo más completamente posible respecto a la exactitud requerida, de modo que para todos los efectos prácticos asociados con la medición su valor sea único. Es en este sentido, es en el que se utiliza la expresión “valor del mensurando” (JGCM, 2010).

2.8.3. METODOLOGÍA GQM

Según Pérez (2010), las organizaciones muchas veces requieren mediciones para entender lo que está pasando y generar una base de conocimiento hacia el futuro. Debe ser definida utilizando un enfoque que parte de los objetivos de la organización para llegar al nivel de productos, de arriba hacia abajo. Se considera que una medición es eficaz cuando es:

- Centrada en objetivos específicos.
- Aplicada a todos los productos de ciclo de vida, procesos y recursos;
- Interpretada basado en entendimiento del contexto organizacional, el medio ambiente y las metas existentes.

2.8.3.1. MODELO GQM O META-PREGUNTA-MÉTRICA

Pérez (2010) indica que el modelo GQM es una estructura jerárquica que especifica a partir de un objetivo los efectos de la medición, el objetivo a medir, la cuestión que debe medirse y el punto de vista de donde se toma la medida. Cada objetivo se descompone en varias preguntas para entender los componentes del objetivo y finalmente se obtienen métricas que dan respuesta a cada una de las preguntas. Todo este proceso se descompone a tres niveles:

Nivel conceptual (Meta): Se establece un objetivo para cada elemento de medición, considerando el producto, proceso y los recursos, desde diferentes puntos de vista.

Nivel operativo (Pregunta): Con base en las metas definidas se establece un conjunto de preguntas que permiten caracterizar la evaluación / logro de un objetivo específico.

Nivel cuantitativo (Métrica): A cada pregunta se le asocian datos que permitan dar respuesta cuantitativa a los objetivos, de manera objetiva o subjetiva.

Además Pérez (2010) expresa que un modelo GQM puede compartir las mismas preguntas y métricas para diferentes objetivos, aunque se obtienen valores diferentes según el punto de vista. El modelo obtenido requiere ser aplicado, recolectados los datos, interpretados y evaluados para determinar el cumplimiento de los objetivos iniciales. Con esto se complementan todos los pasos para cubrir el enfoque de GQM.

Las bases del área de proceso de MA, en el modelo CMMI, se fundamentan en buena medida en las prácticas que establece el enfoque de GQM. Incluso en los ejemplos de formación que se indican en la práctica genérica 2.5 se hace referencia a esto (Pérez, 2010).

CAPITULO III. DESARROLLO METODOLÓGICO

3.1. MÉTODO INVESTIGATIVO

Los autores han empleado este método con el fin de investigar los tipos de protocolos con los que cuentan las Apps móviles Android como es su funcionamiento en cada una de ellas, lo que nos ha permitido tener una mejor visión de cómo interviene la capa OSI dentro las Apps móviles y así desarrollar el primer objetivo de la investigación.

3.1.1. INVESTIGACIÓN EXPERIMENTAL

Como se detalla en el capítulo 2 apartado 2.8.1 los conceptos que comparten un artículo científico y un autor sobre este método y su idea principal que es estudiar una variable experimental no comprobada con el fin de evaluar los protocolos de seguridad de las App móvil Android.

Para realizar esta investigación se efectuaron varias etapas que están referenciadas en la parte teórica del documento y las cuales se van a detallar a continuación:

En el primer paso se delimitó y definió el objeto de la investigación, la misma que señala las variables de estudio tomando en cuenta la bibliografía, el tiempo y los equipos necesarios para obtener los resultados. Seguidamente se planteó la hipótesis de trabajo que permitió a los autores tener una idea clara del fenómeno estudiado.

Conjuntamente a los pasos anteriores se elaboró el diseño experimental donde se hicieron la medición de la seguridad de los protocolos en las App móvil Android utilizando los siguientes equipos:

- 2 Routers

- 3 Dispositivos móviles Android de diferentes versiones y modelos como Alcatel Idol 3, Samsung Galaxy S5 y Hawei.
- 2 Computadoras portátil
- Internet y
- Herramientas software Wireshark y Caín & Abel.

Los mismos que permitieron la interpretación de los resultados de la investigación efectuándose en el segundo nivel de la metodología GQM, durante la ejecución del estudio comparativo.

Se procedió a realizar el experimento con el nivel tres de la metodología GQM, obteniendo los datos de las mediciones que dieron respuestas al problema logrando los resultados que se detallan en el Capítulo IV, donde se hace el respectivo análisis de las métricas y a la vez dan contestación a los objetivos planteados en el mismo.

El último paso de este método fueron las conclusiones que se obtuvieron de los resultados y que se aplicaron de acuerdo al criterio de los autores dando respuesta a la hipótesis hecha que describe el fenómeno estudiado.

3.1.2. MÉTODO DE LA MEDICIÓN

Los autores eligen este método con el fin de determinar los resultados del experimento aplicado a los protocolos de seguridad como se detallan en el tercer nivel de la metodología GQM, como es el nivel operacional, en el cual se desarrolló la determinación de las métricas en cuanto a nivel de seguridad y de vulnerabilidad de los mismos protocolos de las App móvil.

3.2. DURACIÓN DEL TRABAJO

Para la evaluación de protocolos de seguridad de las App en dispositivos móviles, se estimó una duración de nueve meses en los cuales se dio cumplimiento a las actividades y objetivos que los autores tenían planteados.

3.3. VARIABLES DE ESTUDIO

Las variables que se manejaron en esta evaluación funcional fueron las siguientes:

- **Variable Independiente:** la evaluación fue realizada en el sistema operativo Windows 7.
- **Variable Dependiente:** se utilizaron los programas Caín & Abel y Wireshark el cual contaba con varias opciones que permitieron verificar el hallazgo de vulnerabilidades.

3.4. MÉTODO GQM (GOAL QUESTION METRIC)

Para el desarrollo de la evaluación de los protocolos de seguridad de las App de redes sociales en dispositivos móvil Android se utilizó en primer plano la metodología GMQ (Goal Question Metric) o Meta-Pregunta-Métrica que es un enfoque presentado por Víctor Basili de la Universidad de Maryland (1984) que menciona que una organización para medir adecuadamente, debe identificar las metas que desea, derivar objetivos a medir de manera cuantificable y establecer un marco que permita interpretar la información respecto a los objetivos.

Este método se desarrolló para ayudar a decidir qué mediciones tomar y como utilizarlas en los procesos de evaluación en forma ordenada y las que nos permitió dar respuesta a esta necesidad planteada.

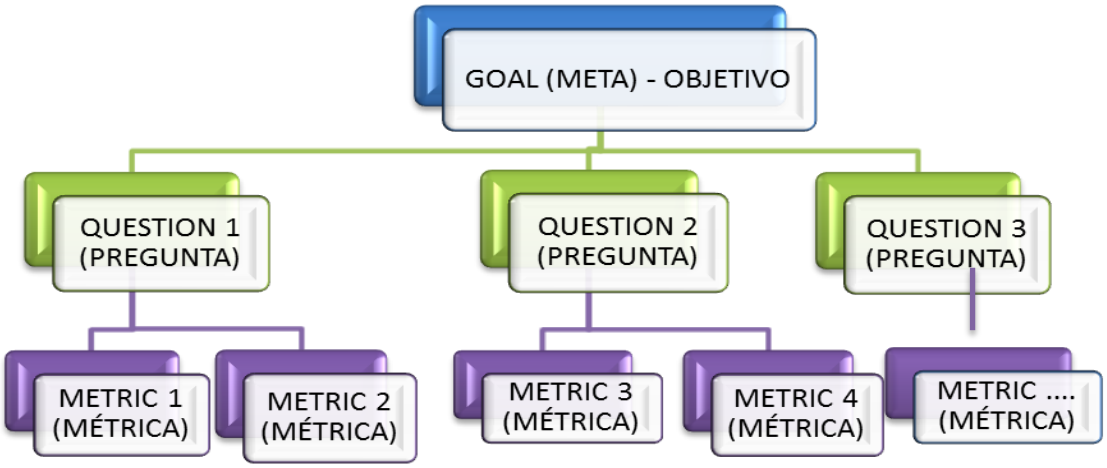


Figura 3. 1. Modelo GQM
Elaboración: Los autores

3.4.1. NIVEL CONCEPTUAL – GOALS

OBJETIVO 1. Determinar los protocolos de seguridad con los que cuentan las aplicaciones de redes sociales en dispositivos móviles.

En este objetivo se constató la información más relevante de los tipos de protocolos que cuentan las aplicaciones móviles y en que capa del modelo OSI trabaja cada uno de estos, tomando en consideración sus niveles de protección y afección (vulnerabilidades), y mediante las actividades se logró esto.

ACTIVIDADES

- Investigar protocolos de seguridad con los que cuentan las aplicaciones móviles. Recolección de información.

Modelo OSI

Debido a que los teléfonos móviles se encuentran conectados a una red global para poder comunicarse entre sí. Es necesario el uso de protocolos que

cooperen simultáneamente para gestionar las comunicaciones. Cada uno de estos protocolos se encarga de una o más capas de acuerdo al modelo OSI (Open Systems Interconnection).

Por esta razón y ante los ataques informáticos y la extracción de información que pueden llevarse a cabo en alguno de los niveles de comunicación entre dispositivos. Es importante que los usuarios conozcan de forma general los niveles de comunicación que existen y así poder determinar algunas medidas de protección. Estos niveles o capas se agrupan en siete: Ver Tabla 3.1.

NIVEL OSI	CARACTERÍSTICAS	MEDIDAS DE PROTECCIÓN
1 Físico	Aspectos mecánicos, eléctricos y ópticos. Todo lo relacionado a la estructura que hace posible la conexión y transferencia de bits entre dispositivos.	• Evitar comprar móviles en tiendas no oficiales y verificar las credenciales del vendedor.
2.Enlace de Datos	Controla el correcto flujo de información regulando la velocidad y estableciendo conexiones. Proporciona parámetros de calidad del servicio Qos, detecta y corrige errores.	• Conectarse a redes Wi-Fi conocidas y seguras, así como verificar el apagado y encendido del Bluetooth sólo cuando se navega en la red.
3.Red	Enrruta y conmuta paquetes de software entre dos Host. Los cuales pueden o no estar ubicados geográficamente en el mismo sitio. Su función es la de asegurarse que los datos lleguen desde el origen	• Acceder al internet a través de contraseñas proporcionadas por el prestador de servicios, así como configurar el móvil para activar la protección en línea.

	hasta su destino.	
4.Transporte	Permite a los usuarios elegir entre distintas calidades de servicio para establecer la conexión de un extremo a otro.	
5. Sesión	Permite la sincronización de diálogos entre dos ETD para el intercambio de datos. Ya sea abriendo o cerrando las conexiones (sesiones).	
6 Presentación	Asigna una sintaxis a los datos para unir las palabras. Codifica los caracteres gráficos y sus funciones de control. Selecciona el tipo de terminal y el formato para representar la información. Sus principales funciones son el formateo, cifrado y compresión de datos.	• Procurar usar un vocabulario sencillo y sin contenido o frases que puedan exponer la confidencialidad de sus usuarios.
7 Aplicación	Permite al usuario la interacción con programas para el intercambio y gestión de datos.	• Usar programas multiplataforma oficiales, que sean conocidos y con garantías de ser seguros. Considerando la compatibilidad entre diferentes dispositivos móviles.

Tabla 3.1. Capas del Modelo OSI
Fuente: https://es.wikipedia.org/wiki/Seguridad_en_telefon%C3%ADa_m%C3%B3vil

- Clasificar los diferentes tipos de protocolos en base a su nivel de seguridad.

Protocolos que intervienen en cada capa del modelo OSI

NIVEL OSI	PROTOCOLO
Enlace de Datos	PPP
	Ethernet
	HDLC
	Frame Relay
	ATM
Red	IP
	SLIP
	ARP
	OSPF
	IGRP
	GGP
	EGP
	BGP
	RIP
	ICMP
	IPX
	X.25
Transporte	TCP
	UDP
	SPX
	NetBEUI
Sesión	LDAP
	RCP
	SCP
	SQL
Presentación	LPP
	XDR
	NetBIOS
	NCP
	X.25 PAD
Aplicación	HTTPS
	HTTP
	FTP
	Telnet
	SMTP
	DNS
	SNMP
	DHCP
	BOOTP
	NTP
	TFTP
	NDS

Tabla 3.2. Protocolos que Intervienen en la Capa del Modelo OSI
Elaboración: Los autores

➢ Determinar los estándares de los protocolos de seguridad al momento de su utilización.

3.4.2. NIVEL OPERACIONAL – QUESTIONS

OBJETIVO 2. Identificaciones de las vulnerabilidades más comunes y métricas en el uso de los protocolos de seguridad de las aplicaciones de redes sociales de dispositivos móviles Android.

ACTIVIDADES

➢ Identificar las Vulnerabilidades de los protocolos de seguridad en dispositivos móvil Android.

De acuerdo a la investigación experimental los autores constataron la realización de pruebas respectivas, mediante los software Cain & Abel y Wireshark, para vulnerabilizar los protocolos de las App móviles.

- Tipos de dispositivos móviles Android

Para efectuar el respectivo proceso de identificación de vulnerabilidades de los protocolos de seguridad, los autores trabajaron con diferentes modelos y versiones de dispositivos móviles Android que se muestra en el **Cuadro 3.1** indicando la respectiva información de cada uno de ellos, lo que permitió desarrollar la investigación.

MODELO DE SMARTPHONE	VERSIÓN DE ANDROID	VERSIÓN DE DATA BASE	VERSIÓN DEL KERNEL	NUMERO DE COMPILACIÓN
Alcatel Idol 3	5.0.2	M8916AAAAANYLD2020509.1	3.10.49	LRX22G RELEASE-KEYS
Samsung Galaxy A5	5.0.2	A500MUBU1BOK1	3.10.49-6694491dpi@SWHD2410 #1 Tue Feb 16 04:51.52 KST 2016	LRX22G.A500MUBU1BPB2
Samsung Galaxy Ace	2.3.4	11060009	3.10.28-g0244f29 jenkins@wuhcitcullx00301 #1 Tue Dec 2 11:17:52 CST 2014	Y550-L03V100R001C00B249
Huawei y 550-l03	4.4.4	S5830BVJKPE	2.6.35.7-perf-CL568065se.infra@SEI-45 #1	GINGERBREAD.VJKPE
Sony Ericsson Xperia Z3 D6603	6.0.1	8975-AAAAANAZQ-00109-57	3.4.0-perf-g3189667BuildUser@BuildHost #1 Thu Mar 17 11:17:37 2016	23.5.A.0.570

Cuadro 3.0.1. Modelos de dispositivos móviles Android
Elaboración: Los autores

- Tipos de conexiones con diferente software.

Un tipo de conexión para efectuar estas pruebas es el conocido **"hombre en el medio"**, este es un modelo de amenaza en la que actúa un intermediario (Atacante) el cual se va a interponer entre el dispositivo móvil (Smartphone) y el router, en este caso el atacante tiene la habilidad de desactivar o controlar las comunicaciones entre las dos partes al interponerse entre el Smartphone y la red WiFi teniendo acceso a todos los datos que en ese momento que están siendo enviados y recibidos, lo que les permitió a los autores evaluar los protocolos por medio del software Caín & Abel para demostrar su nivel de seguridad y vulnerabilidad. Ver **Imagen 3.1.**

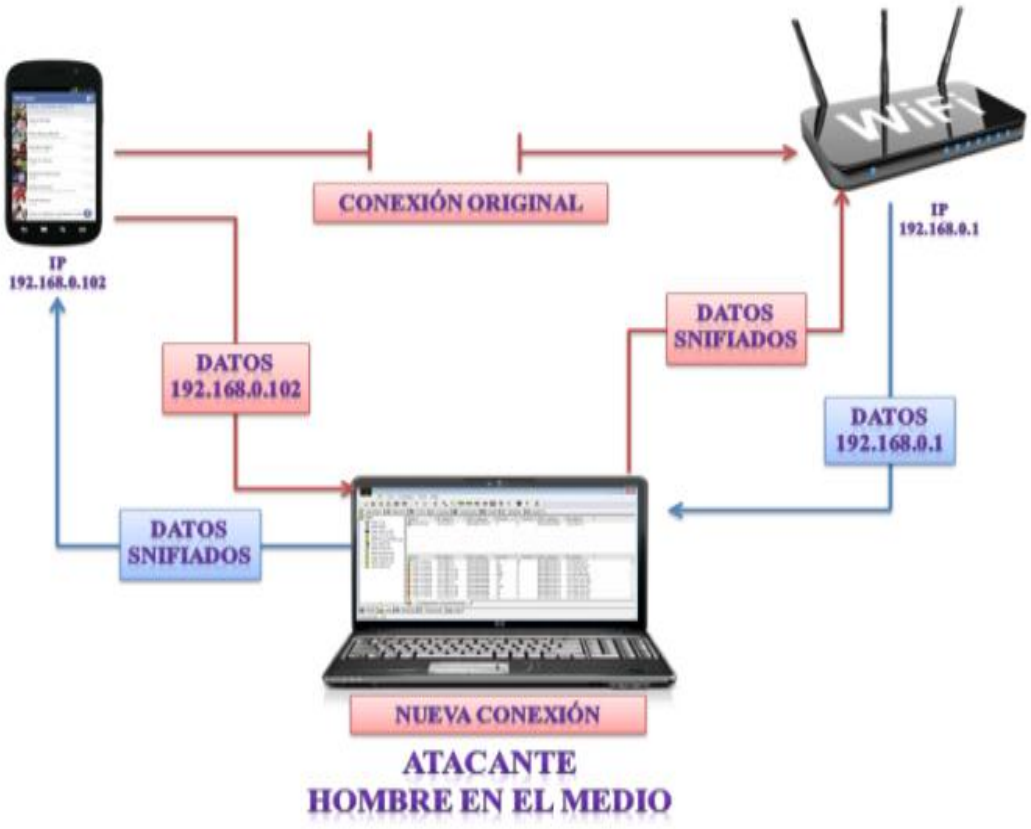


Imagen 3.1. Conexión Hombre en el Medio
Elaboración: Los Autores

Ingresando al modo grafico de Caín y Abel podremos visualizar su entorno de trabajo, pero es necesario antes de utilizar esta aplicación tener desactivado el antivirus y el firewall o los cortafuegos de Windows para que Caín y Abel funcione adecuadamente. **Ver Imagen 3.2.**

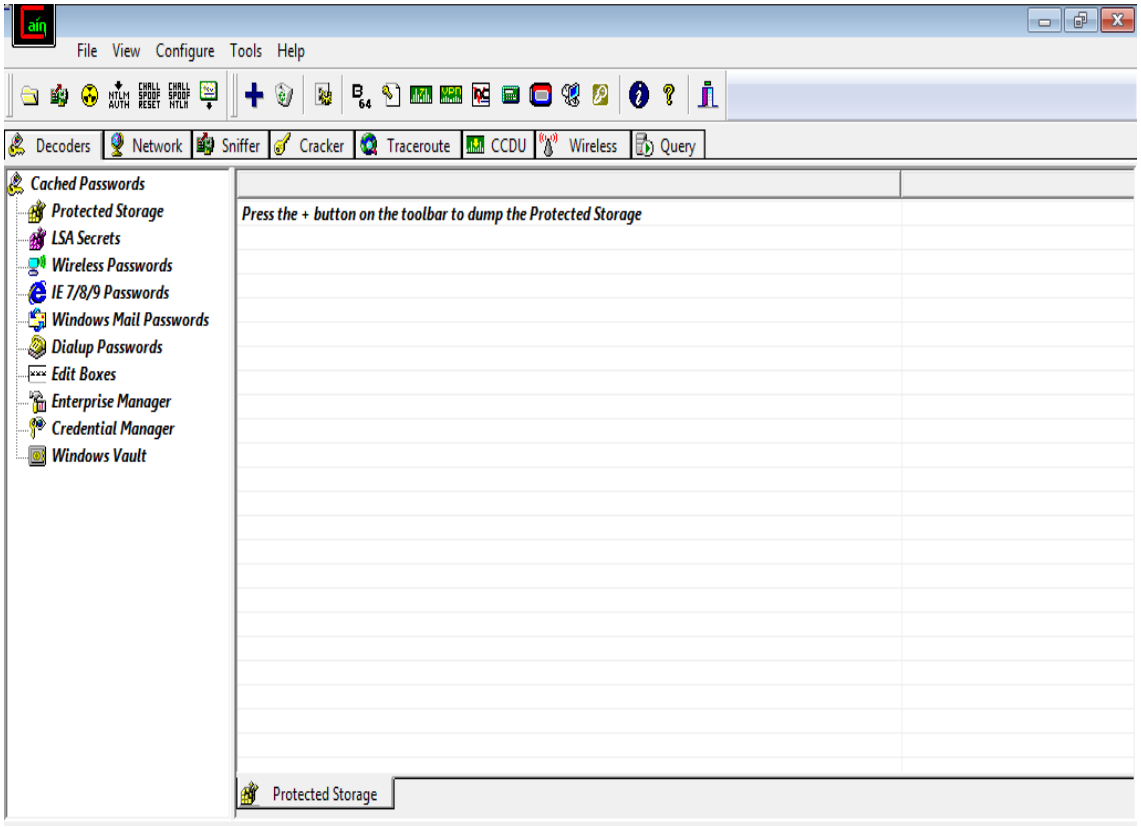


Imagen 3.2. Entorno de trabajo Cain & Abel
Elaboración: Los autores

Se seleccionó el sniffer en donde van a aparecer dos direcciones IP, una es del router y la otra es tarjeta de red, el mismo que se seleccionó para el acceso a la información a través de puertos no seguros.

Si se desconoce la tarjeta de red de la pc entonces se debe ir a CMD y escribimos ipconfig para saber nuestra IP. **(Imagen 3.3.)**

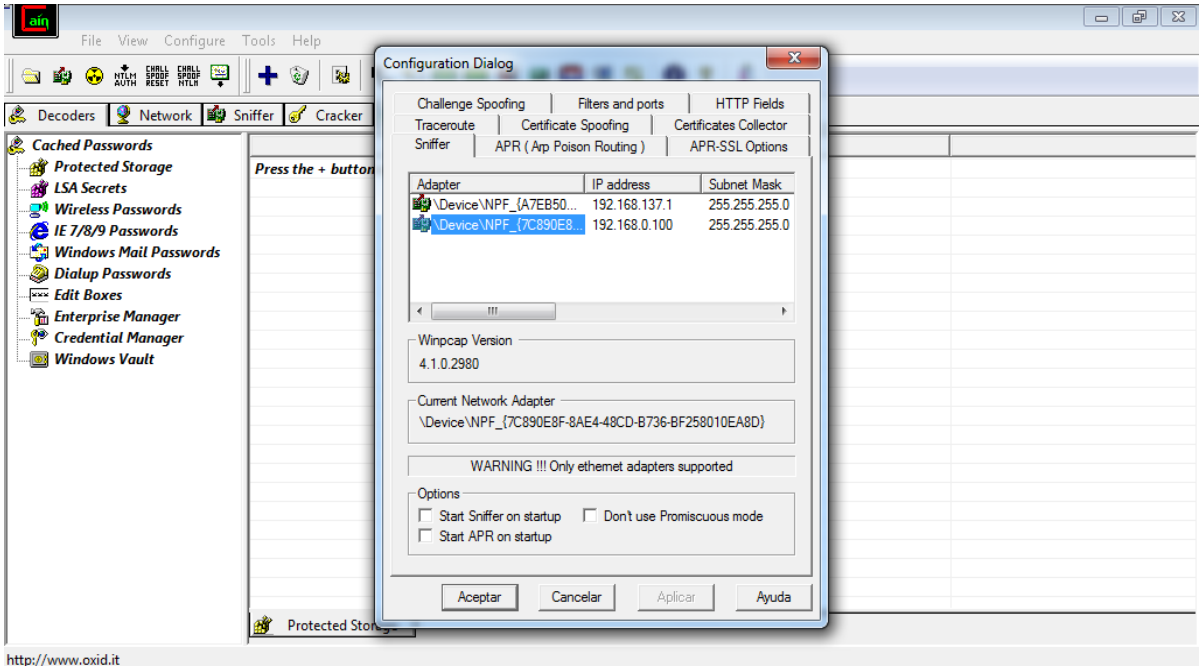


Imagen 3.3. Configuración de nuestra tarjeta de red
Elaboración: Los Autores

Se escogió la pestaña ARP en esta se podrá visualizar la dirección real de la IP y de la MAC si en tal caso no se quisiera que nuestra dirección fuera la real podremos utilizar una falsa para pasar por desapercibido. **Ver Imagen. 3.4.**

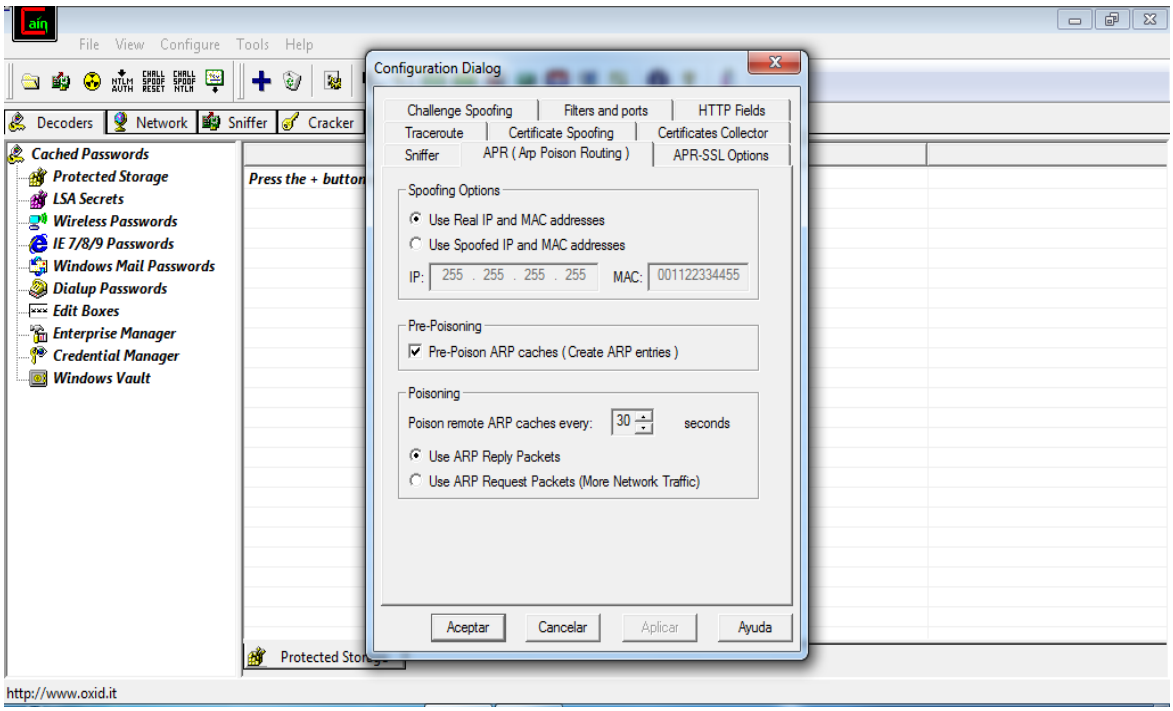


Imagen 3 4. Alternativa de dirección IP y Mac Falsa
Elaboración: Los Autores

A continuación se visualizan las direcciones IP con sus direcciones Mac que están conectados directamente a nuestros router. **Ver Imagen 3.5.**

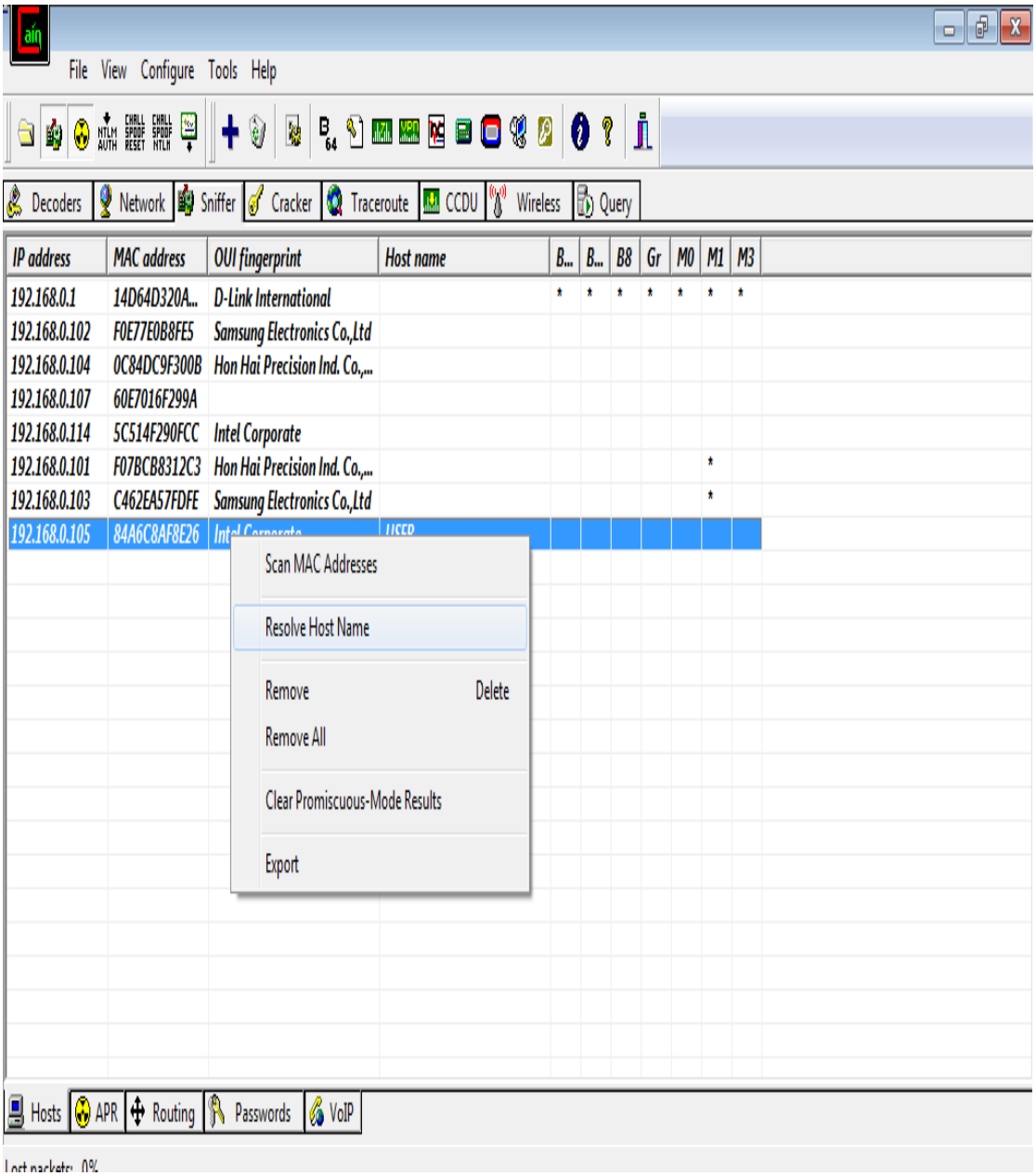


Imagen 3.5. Visualización de las direcciones IP conectadas al router
Elaboración: Los autores

Seguido la selección de la IP 192.168.0.102 que va a ser vulnerada mediante la captura de los paquetes enviados y recibidos mediante la dirección IP del router 192.168.0.1. **(Imagen 3.6.)**

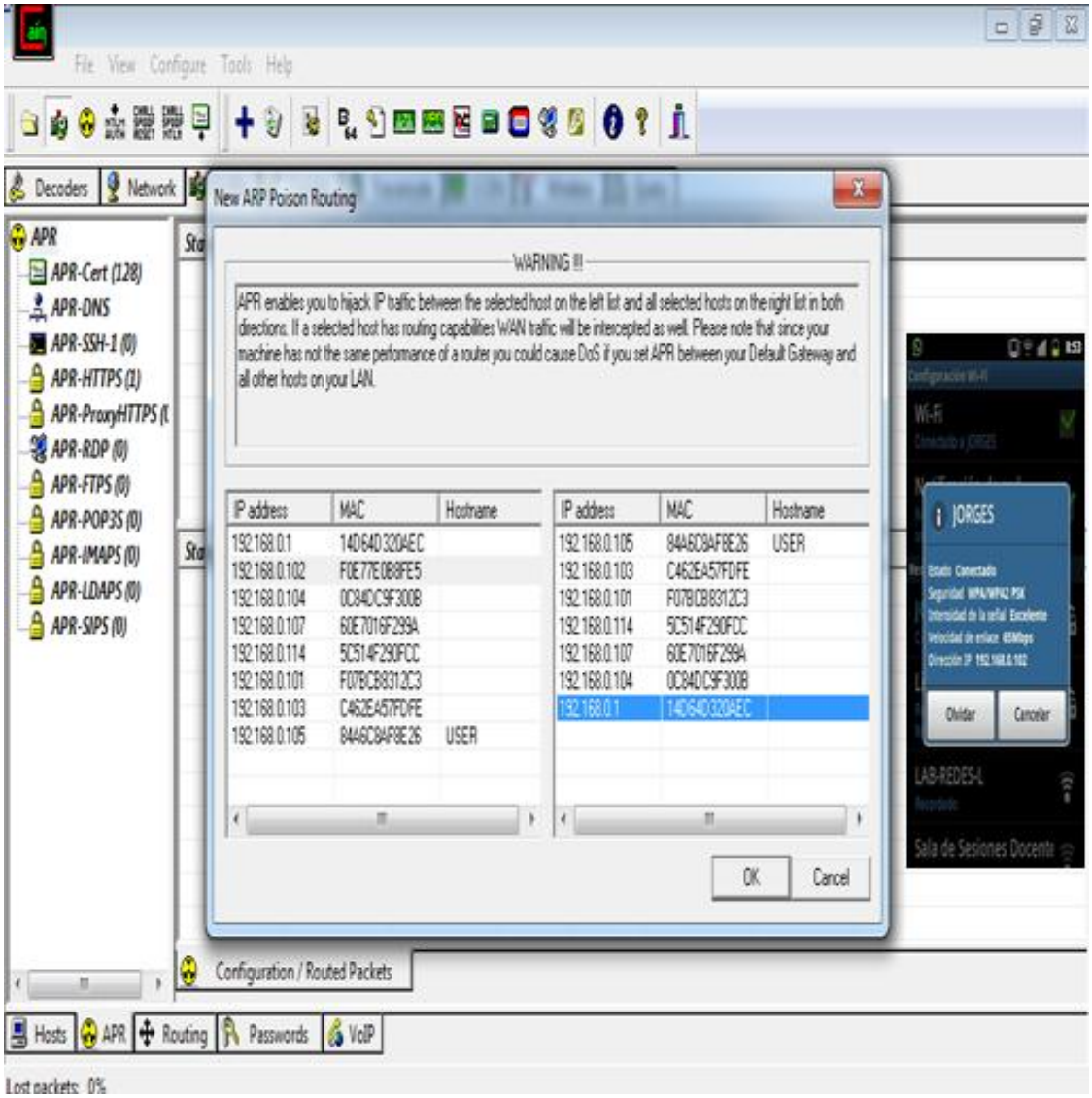


Imagen 3.6. Visualización de las IP que podrían ser víctimas de ataque en la parte identificada
Elaboración: Los Autores

Una vez que se visualizó la dirección IP a la cual se va a atacar que es este caso va a ser la de un dispositivo móvil, ya que esta es la que procederemos a sniffer los paquetes que se envían y se reciben de esta dirección. **Ver Imagen. 3.7 y 3.8.**

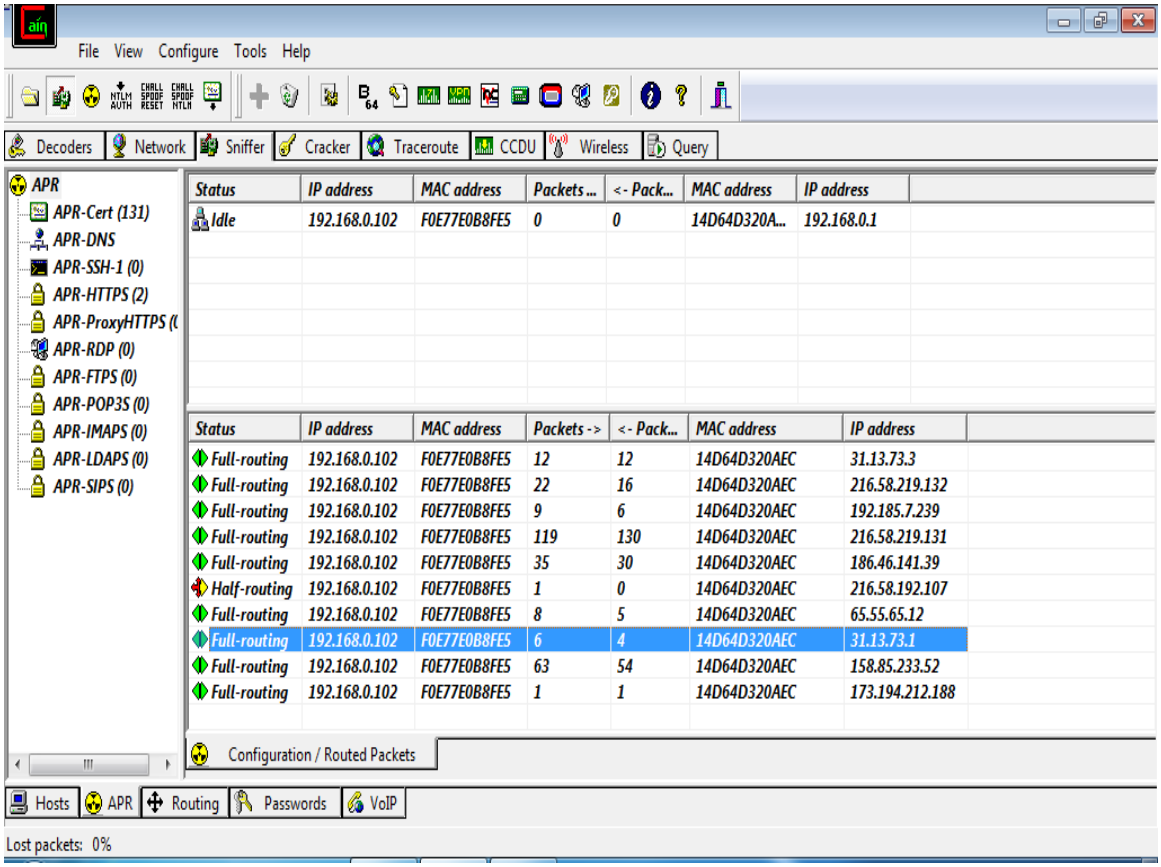


Imagen 3.7. Captura de paquetes que se envían y se reciben
Elaboración: Los Autores

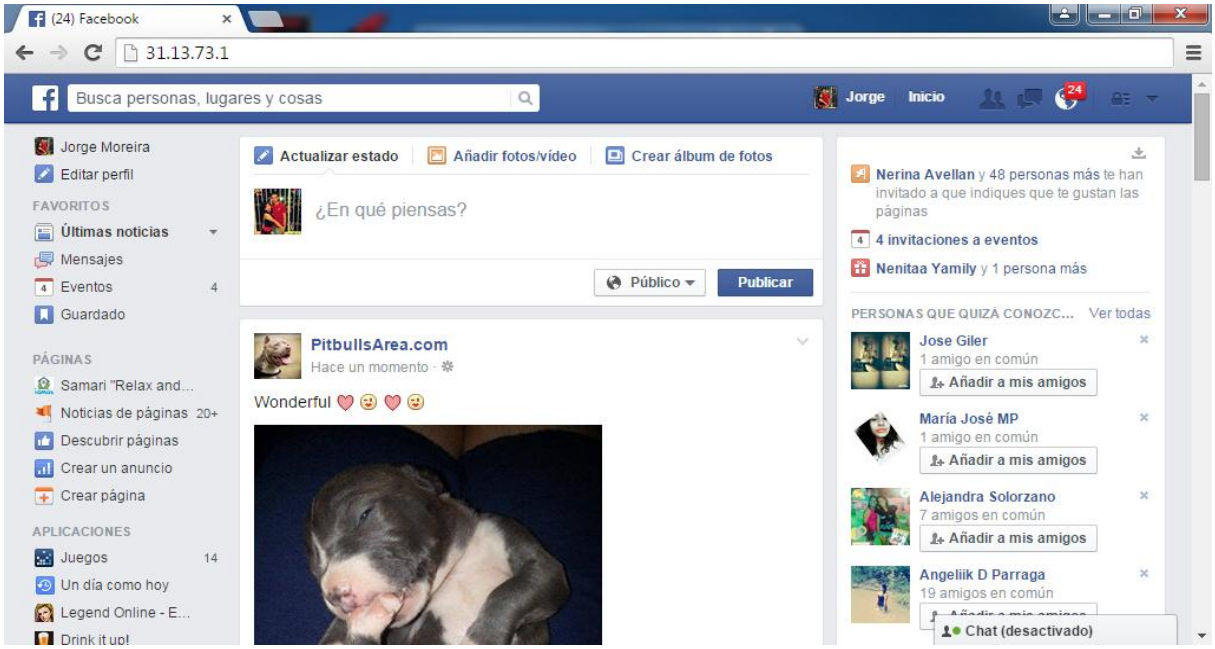


Imagen 3.8. Comprobación de captura de datos enviados a la IP de Facebook mediante una PC
Elaboración: Los autores

A partir del uso de Cain & Abel se procedió a comprobar los protocolos que se estan ejecutando en ese momento ya que este programa permitió visualizar los paquetes que se envian y se reciben sin poder saber el tiempo o el scrip de estos paquetes y mediante la utilización del programa Wireshark se lograron capturar el protocolo y todo el tráfico de paquetes de datos (datos snifiados) que se envían y se reciben en la red en los diferentes dispositivos móviles que están conectados y el protocolo que esta utiliza en el momento de la conexión. Ver **Imagen 3.9.**

Imagen 3.9. Creación de un Acces Point en que la computadora funciona como un host
Elaboración: Los Autores

A continuación se muestra el desarrollo realizado con el programa Wireshark:

Consulta ARP

Durante la captura de tráfico, se logra la consulta ARP (Address Resolution Protocol) de un equipo que intenta obtener la dirección MAC del Default Gateway. Esta consulta se realiza en dos pasos. **Ver Imagen 3.10.**

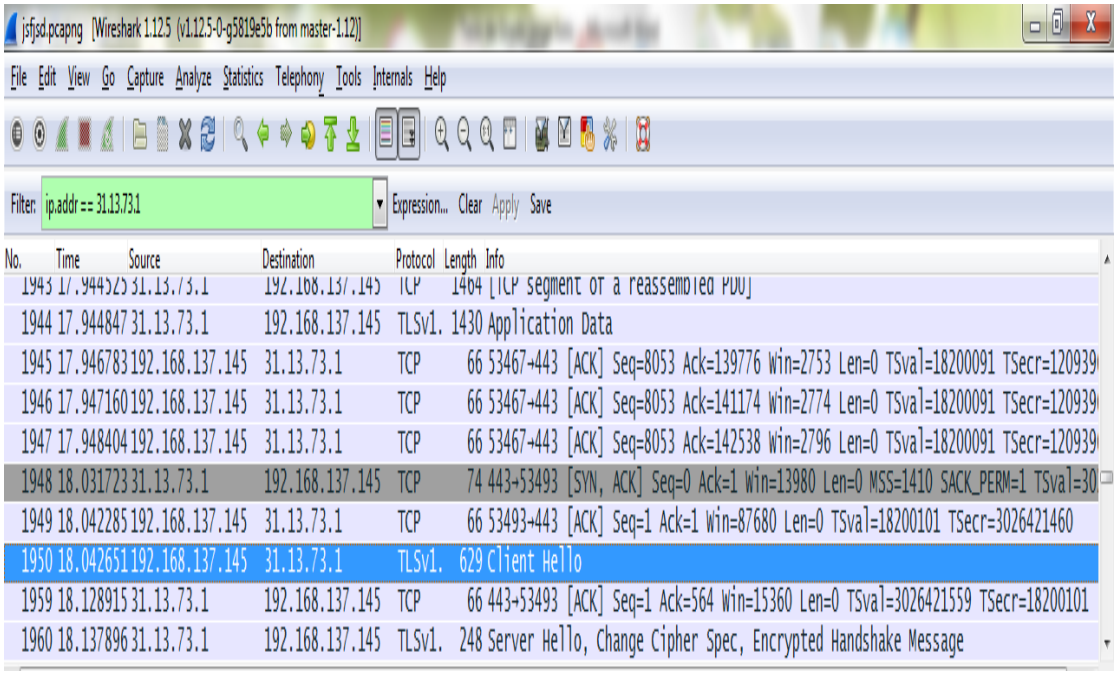


Imagen 3.10. Consulta con el protocolo ARP para obtener las direcciones MAC
Elaboración: Los Autores

En primer lugar el equipo 192.168.137.145, necesita conocer la dirección MAC del Default Gateway, enviando para ello una consulta ARP. **Ver Imagen 3.11.**

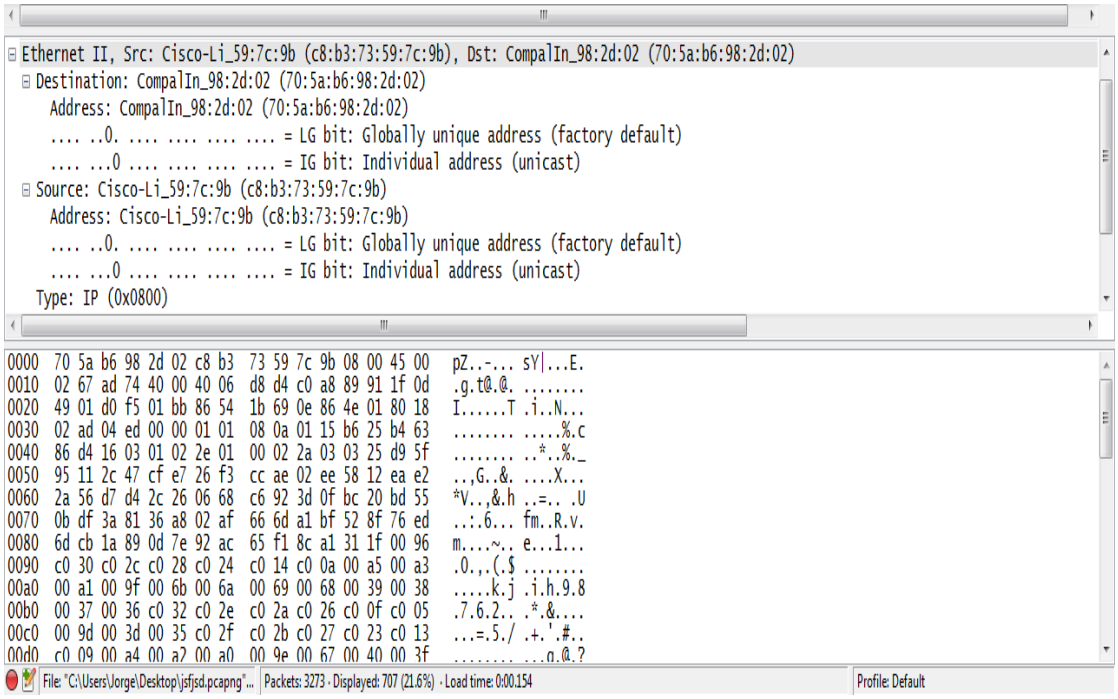


Imagen 3.11. Consulta con el protocolo ARP para obtener las direcciones MAC
Elaboración: Los Autores

Por último, el equipo que ha reconocido su IP (default Gateway, envía una respuesta ARP (ARP Reply) en donde informa su dirección MAC, logrando de esta manera que su dirección sea almacenada en la tabla ARP del equipo, y que otras aplicaciones puedan utilizar esta información para dar curso a sus propios procesos. **Imagen 3.12.**

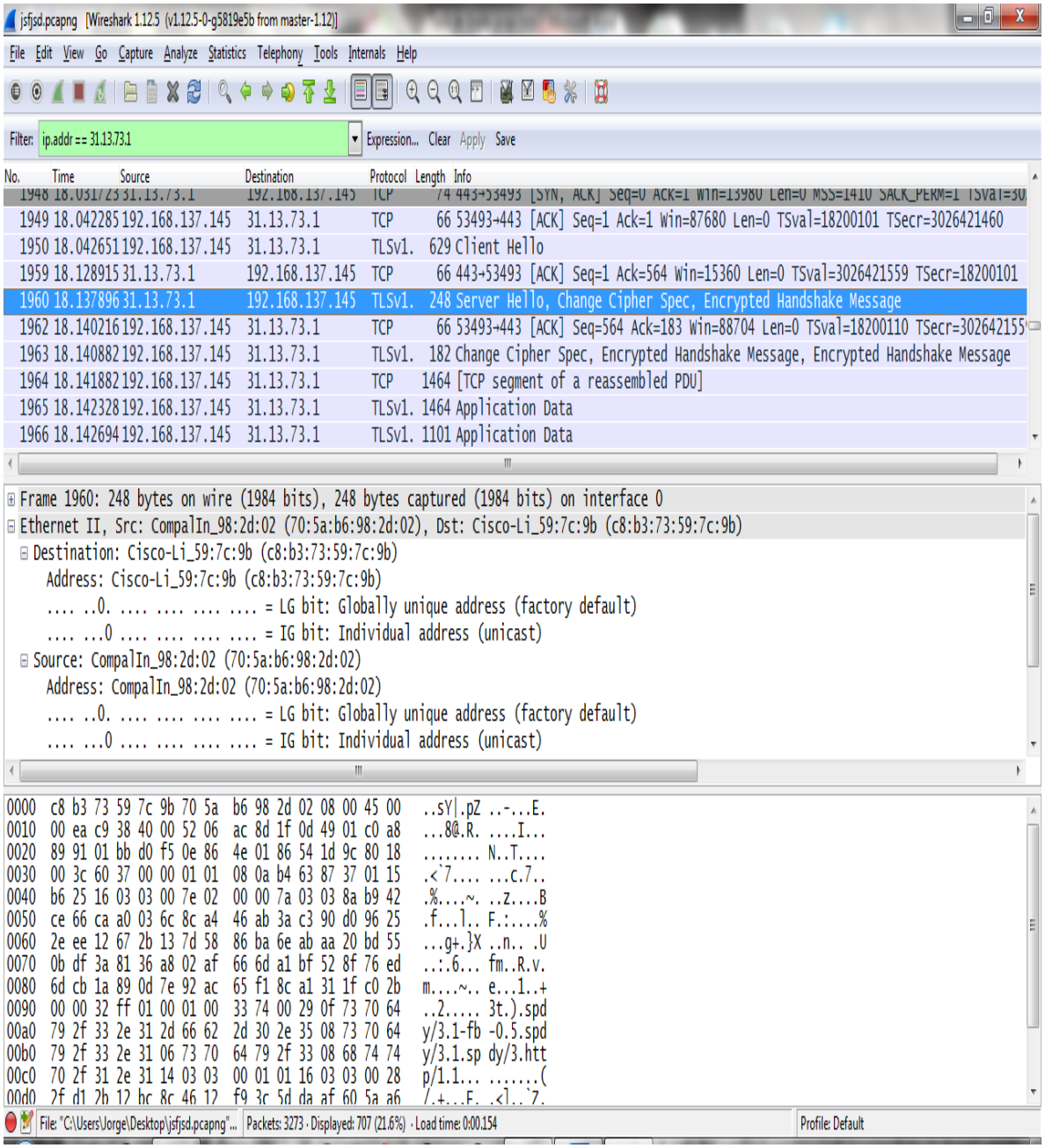


Imagen 3.12. Respuestas de las direcciones MAC
Elaboración: Los Autores

Consulta DNS

En primer lugar, en el paquete 153 de la captura, el equipo realiza una consulta DNS para traducir la url introducida en una dirección IP. Después vemos como en el paquete 306 de la captura el servidor DNS ha entregado su respuesta, informando la dirección IP de www.facebook.com. Ver **Imagen 3.13.**

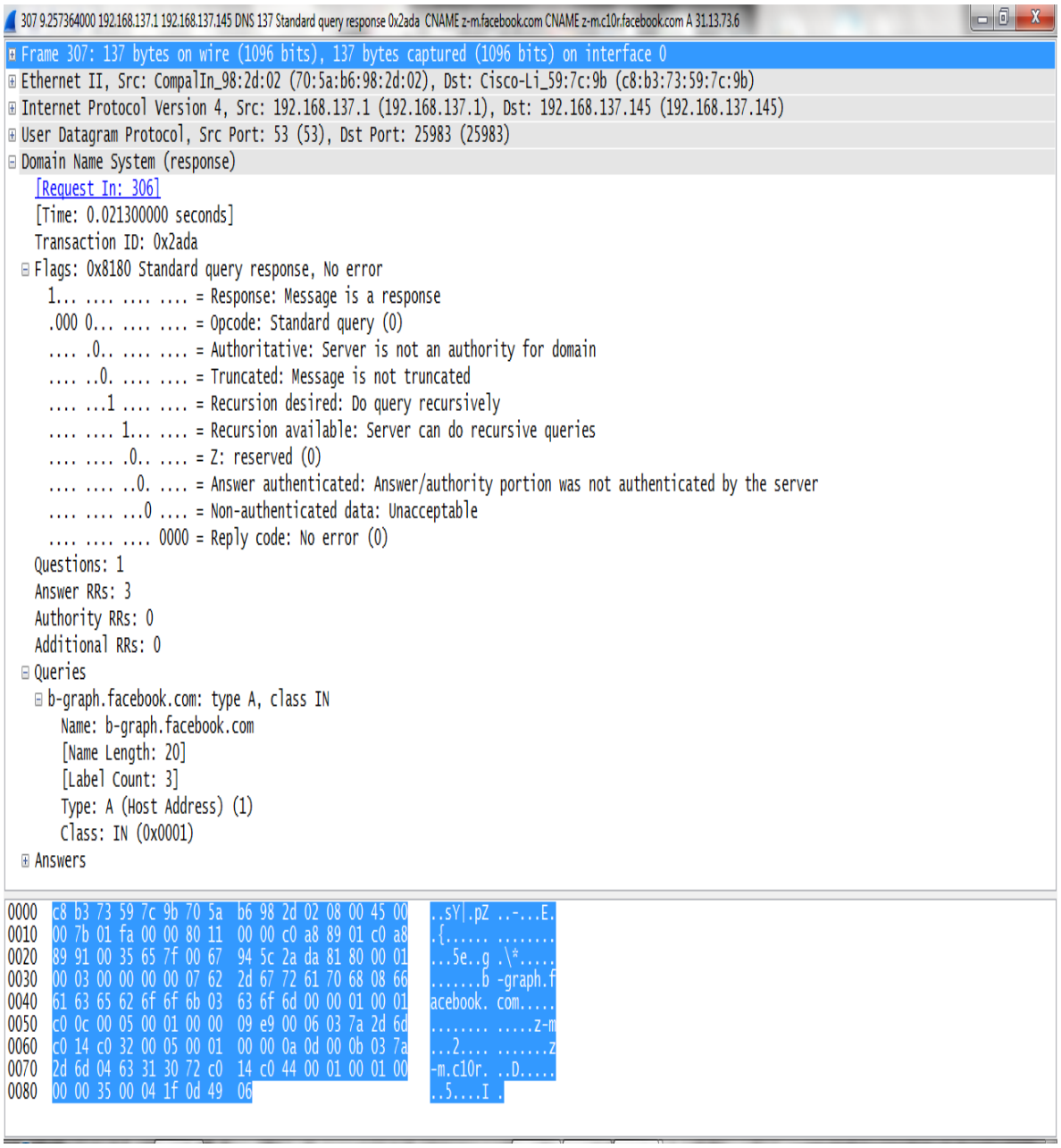


Imagen 3.13. Consulta con el protocolo DNS
Elaboración: Los Autores

Sesión TCP

Se debe tener en cuenta que las direcciones destino registradas por Wireshark son las direcciones locales del Proxy de navegación utilizado (172.19.34.96) y no las IP de Internet. **Ver Imagen 3.14, 3.15, 3.16 y 3.17.**

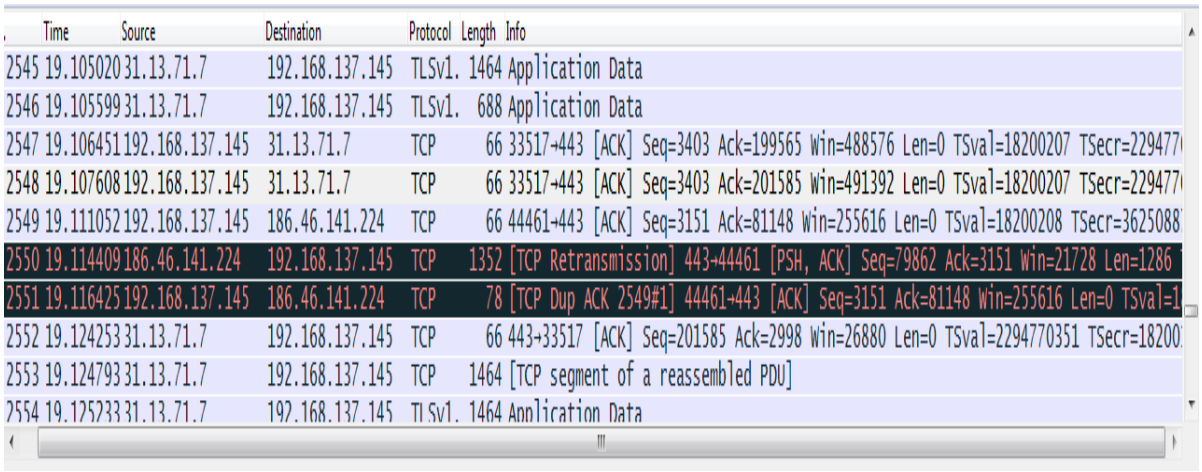


Imagen 3.14. Direcciones MAC para la verificación de la respuesta que envía el cliente al servidor
Elaboración: Los Autores

1. SYN

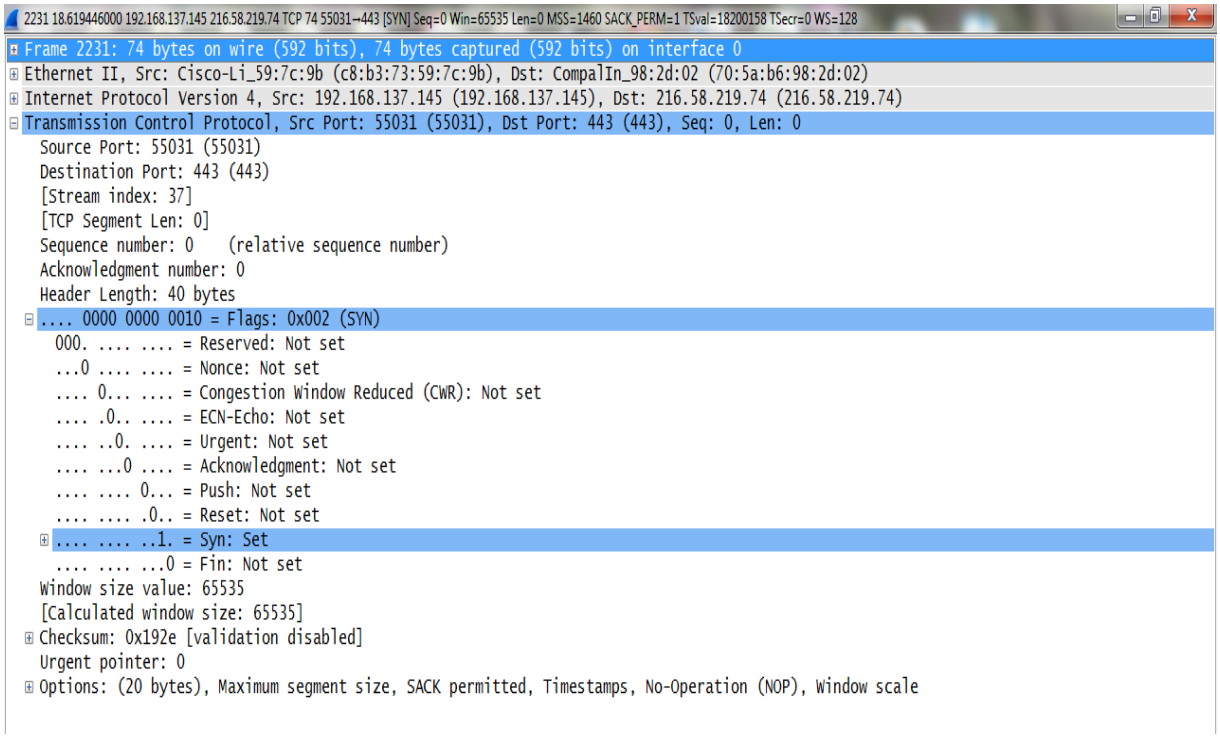


Imagen 3.15. Verificaciones de la respuesta SYN que envía el cliente al servidor
Elaboración: Los Autores

2. SYN /ACK

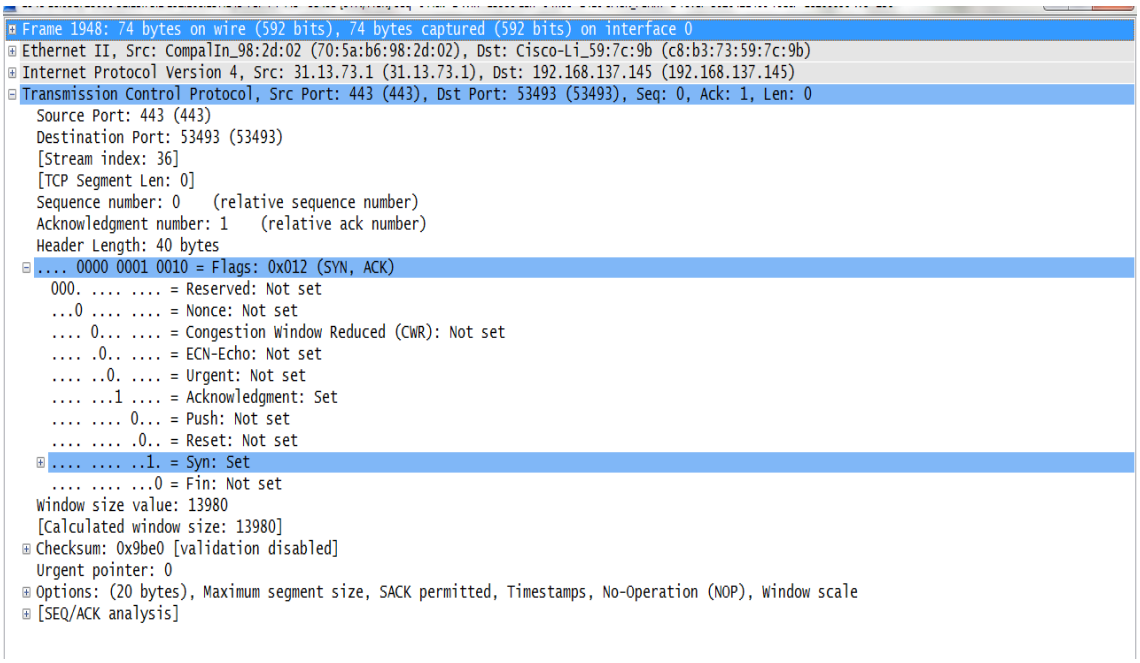


Imagen 3.16. Verificaciones de la respuesta SYN/ACK que envía el cliente al servidor
Elaboración: Los Autores

3. ACK

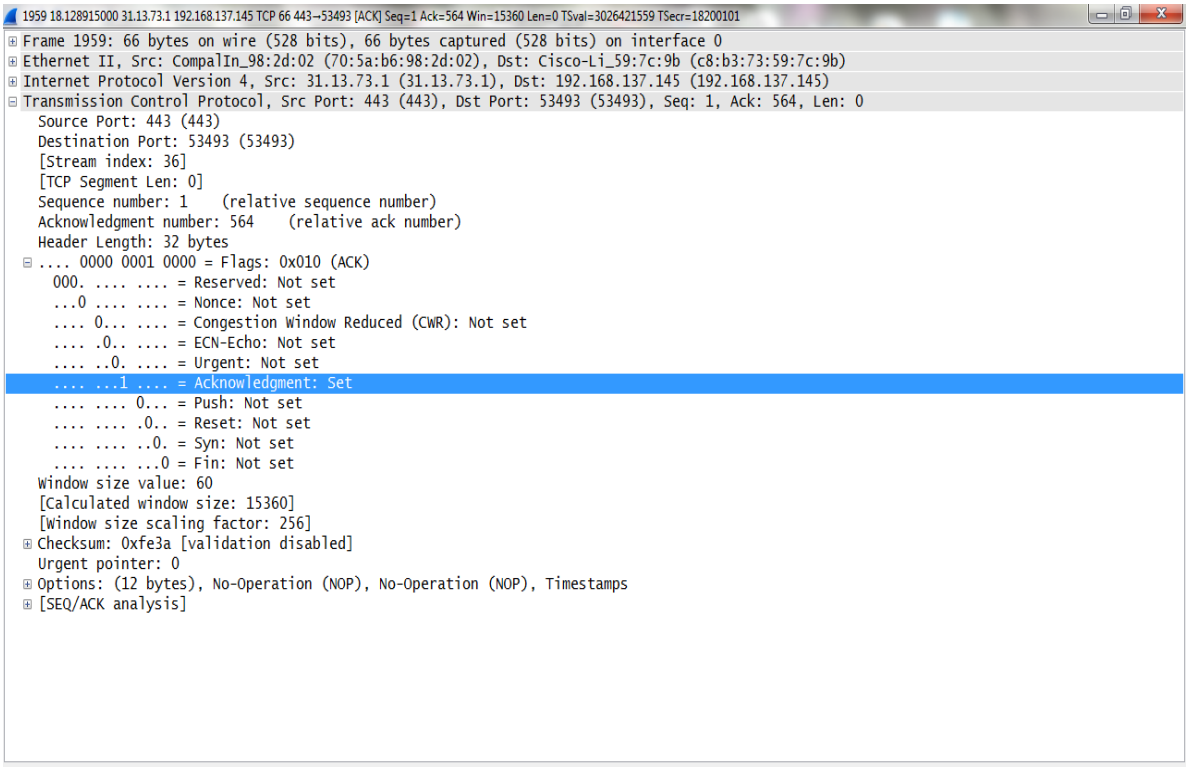


Imagen 3.17. Números de secuencias entre el cliente y servidor
Elaboración: Los Autores

- Identificación de métricas en el uso de protocolos.

Métrica 1

Nivel de Visibilidad

A través de la evaluación de las métrica de visualización, los autores determinaron los protocolos que pueden ser vistos, mediante el uso de programas (Wireshark y Cain & Abel) y así verificar su nivel de vulnerabilidad de cada uno y comprobar la seguridad de las App's móviles.

- Evaluación por el desempeño de los programas utilizados en la practica

Toda App móvil forman parte de nuestra vida diaria, de la misma forma tienen sus ventajas y desventajas por lo que siempre hay que tomar en cuenta el nivel de seguridad y de vulnerabilidad que tiene cada una de ellas, por esta razón los autores realizaron la siguiente investigación, al emplear programas utilizados para la verificación de vulnerabilidad de las App de redes sociales en dispositivos móviles Android. Ver **Tabla 3.3.**

TIPO DE PROGRAMA	NIVEL DE COMPLEJIDAD
Cain & Abel	Fácil manejo (trabaja mediante un router en una misma red)
Wireshark	Complejo (visualización de diferentes tipos de direcciones)

Tabla 3.3. Software utilizados en la práctica Wireshark y Cain & Abel
Elaboración: Los autores

Métrica 2

Nivel de Vulnerabilidad

Al emplear está métrica los autores consiguieron identificar las vulnerabilidades que se presentan en cada uno de los protocolos visualizados que serán atacados con la utilización de programas sniffer como lo son Wireshark y

Cain&Abel estos son indispensables para comprobar el nivel de seguridad de cada protocolo.

- Evaluación del desempeño de los protocolos de seguridad visualizados mediante el software.

En la actualidad todas las App móviles constan con protocolos de seguridad, los cuales ayudan a su desempeño ya que cada uno de ellos tiene una función específica y gracias a estos los mensajes pueden estar encriptados o no. En la siguiente practica los autores lograron mostrar las características de los protocolos visualizados, mediante los programas Cain & Abel y Wireshark, para verificar el estado de vulnerabilidad de las App en redes sociales de dispositivos móviles Android. **Ver Tabla 3.4.**

PROTOCOLO	CARACTERÍSTICAS
HTTP	Hiper texto
SMTP	Seguridad avanzada cifra las transmisiones
DNS	Sistema de Nombres de dominios, base de datos distribuidas
TLSV1	Protocolos de resolución
ARP	Direcciones IP
DHCP	Configuración de direcciones IP

Tabla 3.4. Protocolos Capturados a Través de las Prácticas Realizadas Mediante Software
Elaboración: Los Autores

3.4.3. CUANTITATIVO – METRICS

OBJETIVO 3. Recolección de los datos correspondientes a los parámetros de pruebas de los protocolos de seguridad de los dispositivos móviles Android para la comprobación de la vulnerabilidad de los mismos.

- Evaluación de métricas realizadas a los protocolos de seguridad.

Métrica 1.- Nivel de Visualización

Los autores consiguieron determinar mediante el uso de los software Wireshark y Caín & Abel la visualización de los protocolos que interactúan en los diferentes dispositivos móviles Android. **Ver tabla 3.5**

MODELO DE SMARTPHONE	VERSIÓN DE ANDROID	PROTOCOLOS CON WIRESHARK	PROTOCOLOS CON CAÍN & ABEL
Alcatel Idol 3	5.0.2	HTTP, SMTP, ARP, DNS,TLSV1,DHCP,TCP,UDP	ARP, HTTPS
Samsung Galaxy A5	5.0.2	HTTP, SMTP, ARP, DNS,TLSV1,DHCP,TCP,UDP	ARP, HTTPS
Samsung Galaxy Ace	2.3.4	HTTP, SMTP, ARP, DNS,TLSV1,DHCP,TCP,UDP	ARP, HTTPS
Huawei y 550-l03	4.4.4	HTTP, SMTP, ARP, DNS,TLSV1,DHCP,TCP,UDP	ARP, HTTPS
Sony Ericsson Xperia Z3 D6603	6.0.1	HTTP, SMTP, ARP, DNS,TLSV1,DHCP,TCP,UDP	ARP, HTTPS

Tabla 3.5. Protocolos Visualizados en los diferentes dispositivos móviles con el Programa Wireshark y Cáin & Abel
Elaboración: Los Autores

Métrica 2.- Nivel de vulnerabilidad

Mediante la determinación de la visualización de los protocolos de seguridad que se muestran en la **Tabla 3.5** detallados de manera ordenada los protocolos visualizados con los programas Wireshark y Caín & Abel en los diferentes dispositivos móviles, se enlistan los niveles de seguridad de acceso con respecto a cada Programa utilizado. **Ver Tabla 3.6 y 3.7**

Programa

WIRESHARK

Nivel Osi	Protocolo	Nivel de Seguridad
Físico		
Enlace de Datos		
Red	ARP	Bajo al contar con un encriptado en la trama del paquete
Transporte	TCP	Bajo al contar con un encriptado en la trama del paquete
	UDP	Bajo al contar con un encriptado en la trama del paquete
Sesión		
Presentación		
Aplicación	HTTP	Bajo al contar con un encriptado en la trama del paquete
	DNS	Bajo al contar con un encriptado en la trama del paquete

Tabla 3.6. Protocolos del Modelo Osi Vulnerados Mediante Programas Wireshark

Elaboración: Los Autores

Caín & Abel

Nivel Osi	Protocolo	Nivel de Vulnerabilidad
Físico		
Enlace de Datos		
Red	ARP	Alto al visualizar las direcciones IP para su manipulación
Transporte		
Sesión		
Presentación		
Aplicación	HTTPS	Bajo al contar con un encriptado complejo y bloqueo de direcciones durante su ejecución

Tabla 3.7. Protocolos del Modelo Osi Vulnerados Mediante el Programa Caín & Abel

Elaboración: Los Autores

Con la implementación de nuevas medidas de seguridad a los protocolos de los dispositivos móvil específicamente a Android el nivel de encriptación se elevó, para que la trasmisión y recepción de mensajes sea segura en el móvil y el servidor, de acuerdo a la obtención de los datos alcanzados en la práctica con los programas Wireshark y Cain & Abel, los autores verificaron que la hipótesis de esta investigación no se cumple, ya que los protocolos de seguridad de redes sociales en las App de dispositivos móviles Android no son totalmente vulnerables y en ambos programas se obtuvo solamente la visualización de los protocolos pero no la información que transmite los paquetes de datos.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

Los autores en este capítulo detallan los resultados obtenidos en la evaluación de los protocolos de seguridad de las App de redes sociales en dispositivos móvil Android, enfocada en los niveles de la metodología GQM (Goal Questions Metric) y combinada con los métodos de investigación experimental y de medición, utilizando los programas Wireshark y Cain & Abel para la verificación de vulnerabilidad en cada uno de los protocolos.

DETERMINAR LOS PROTOCOLOS DE SEGURIDAD CON LOS QUE CUENTAN LAS APLICACIONES DE REDES SOCIALES EN DISPOSITIVOS MÓVILES

ANÁLISIS DEL NIVEL CONCEPTUAL – GOAL

Mediante la investigación y clasificación de los protocolos de seguridad en las aplicaciones móviles **(Anexo 2)**, se pudo obtener como resultado en forma general y de acuerdo al modelo OSI, los siete niveles de comunicación determinando algunas medidas de protección para cada una de las capas. A continuación se muestra la **Tabla 4.1.**

NIVEL OSI	CARACTERÍSTICAS	TIPOS DE PROTOCOLOS	MEDIDAS DE PROTECCIÓN
1. Físico	Aspectos mecánicos, eléctricos y ópticos. Todo lo relacionado a la estructura que hace posible la conexión y transferencia de bits entre dispositivos.	Interfaces físicas (y no todas las tarjetas de red serían de capa 2 pero incluyen componentes de capa 1), cableado, señales, etc...	• Evitar comprar móviles en tiendas no oficiales y verificar las credenciales del vendedor.
2. Enlace de	Controla el correcto flujo de información regulando	IEEE 802.3 más conocido como	• Conectarse a redes Wi-Fi

Datos	la velocidad y estableciendo conexiones. Proporciona parámetros de calidad del servicio Qos, detecta y corrige errores.	Ethernet (CSMA/CD), IEEE 802.5 (token passing), FDDI token passing, VLANs, ATM Adaptation Layer, ISDN, Frame Relay, PPP, SMDS, HDLC, LAP-A, 802.2 (etiquetado de tramas)	conocidas y seguras, así como verificar el apagado y encendido del Bluetooth sólo cuando se navega en la red.
3.Red	Enrruta y conmuta paquetes de software entre dos Host. Los cuales pueden o no estar ubicados geográficamente en el mismo sitio. Su función es la de asegurarse que los datos lleguen desde el origen hasta su destino.	IP, SLIP, ARP, OSPF, IGRP, GGP, EGP, BGP, RIP, ICMP, IPX, X.25,...	• Acceder al internet a través de contraseñas proporcionadas por el prestador de servicios, así como configurar el móvil para activar la protección en línea.
4.Transporte	Permite a los usuarios elegir entre distintas calidades de servicio para establecer la conexión de un extremo a otro.	TCP, UDP, SPX, NetBEUI..	
5. Sesión	Permite la sincronización de diálogos entre dos ETD para el intercambio de datos. Ya sea abriendo o cerrando las conexiones (sesiones).	LDAP, RPC, SCP, SQL,	

6. Presentación	Asigna una sintaxis a los datos para unir las palabras. Codifica los caracteres gráficos y sus funciones de control. Selecciona el tipo de terminal y el formato para representar la información. Sus principales funciones son el formateo, cifrado y compresión de datos.	LPP, XDR, NetBIOS, NCP, X.25 PAD,...	• Procurar usar un vocabulario sencillo y sin contenido o frases que puedan exponer la confidencialidad de sus usuarios.
7. Aplicación	Permite al usuario la interacción con programas para el intercambio y gestión de datos.	HTTPS, HTTP, FTP, Telnet, SMTP, DNS, SNMP, DHCP, BOOTP, NTP, TFTP, NDS...	• Usar programas multiplataforma oficiales, que sean conocidos y con garantías de ser seguros. Considerando la compatibilidad entre diferentes dispositivos móviles.

Tabla 4.1. Información general de los Protocolos de seguridad en el modelo OSI
Elaboración: Los Autores

La seguridad en protocolos de aplicaciones móviles es importante debido a que se maneja la integridad de información, por medio de transmisión y comunicación de datos, teniendo en cuenta que muchas veces estos protocolos pueden ser vulnerados por atacantes cibernéticos, enfocándose principalmente a las App's (redes sociales y mensajería instantánea).

Una vez obtenida la información acerca de los protocolos utilizados en las aplicaciones móviles y el formato de datos al momento de comunicarse en

función de las capas del modelo OSI, se obtuvo como resultado los diferentes servicios web con diferentes protocolos para la comunicación, definiéndose estos como reglas para cada servicio en las aplicaciones móviles de redes sociales, mostrados en el siguiente **Tabla 4.2.**

SERVICIO WEB	PROTOCOLOS UTILIZADOS (Regla)
World Wide Web (www)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Mensaje Instantáneo (Jubber; AIM)	XMPP (Extensible Messeging and Presence Protocol) OSCAR (Sistema abierto para la comunicación en tiempo real)
Telefonía IP	SIP (Session Intuition Protocol)

Tabla 4.2. Protocolos utilizados en los diferentes servicios web para la comunicación en aplicaciones móviles
Elaboración: Los Autores

En la siguiente **Tabla 4.3**., se muestran los resultados del formato de datos al momento de comunicarse en función de las capas del modelo OSI, observando que los datos en las diferentes capas se dan una manera ordenada y lógica.

CAPAS DEL MODELO OSI	FORMATO DE UNIDAD DE DATOS
Capa de Aplicación	APDU (Capa 7)
Capa de Presentación	PPDU (Capa 6)
Capa de Sesión	SPDU (Capa 5)
Capa de Transporte	TPDU (Capa 4)
Capa de Red	PAQUETE (capa 3)
Capa de Enlace	TRAMA (Capa 2)
Capa Física	BIT (Capa 1)

Tabla 4.3. Forma de datos de Comunicación en las diferentes capas del modelo OSI
Elaboración: Los Autores

IDENTIFICAR LAS VULNERABILIDADES MÁS COMUNES Y MÉTRICAS EN EL USO DE LOS PROTOCOLOS DE SEGURIDAD DE LAS APLICACIONES DE REDES SOCIALES DE DISPOSITIVOS MÓVILES ANDROID.

ANÁLISIS DEL NIVEL OPERACIONAL – QUESTION

En la identificación de las vulnerabilidades y métricas de los protocolos de seguridad a través de la conexión hombre en el medio y su implementación, se obtiene la demostración de las capturas de envío y recepción de los paquetes, tramas, bits por medio del uso de la herramientas Wireshark y Caín & Abel **(Anexo 3)**, que permitió obtener los paquetes que se están trasmitiendo por la red y a la vez se verifica que sí se realiza él envió por este tipo de App, debido a que la red detecta el paquete de dato trasmitido.

De acuerdo a los resultados obtenidos en la identificación de las vulnerabilidades de los protocolos de seguridad se consiguió determinar la métrica 1 de visibilidad y la métrica 2 de vulnerabilidad. Mediante su evaluación se pudo obtener lo siguiente: En la **Tabla 4.4** la métrica 1 nos muestra los protocolos visualizados mediante la utilización de los programas (Wireshark y Caín & Abel). Los protocolos que se visualizan son: el protocolo HTTPS que es el que permite una seguridad más confiable en la transferencias de datos, HTTP que sirve para la trasmisión de datos, SMTP encripta la información, ARP se encarga de la resolución de direcciones IP, DNS trabaja con sistemas de nombres de dominios, TLSV1 encargado de la transmisión de datos de mensajería instantánea y DHCP configura las direcciones IP. Una vez visualizados los protocolos, se verificó con la métrica 2 referente al nivel de vulnerabilidad, el nivel de transferencia y de seguridad de los mismos, obteniendo lo siguiente: HTTPS, SMTP, son los protocolos con Alto nivel de seguridad y Alto nivel de Transferencia de datos, es decir que el envío y recepción de datos es elevado y la encriptación de la información es difícil de manipular. Los protocolos DHCP, DNS en el envío y recepción de los datos tienen nivel Medio y el nivel de seguridad en la encriptación de la información es Alto, es decir que no es vulnerable. HTTP tiene Alto nivel de transferencia

de datos pero es un protocolo de Bajo nivel de seguridad; el protocolo TLSV1 está en el nivel de transferencia Alto con una seguridad Media en el protocolo. ARP tiene un nivel Medio en la transferencia de datos y Bajo nivel de seguridad, lo que permite determinar que los protocolos de seguridad de las Apps móviles, no son totalmente vulnerables para la manipulación de la información.

Tipo de software o programa	Métrica 1	Métrica 2	
	Protocolos visualizados	Nivel de transferencia	Nivel de Seguridad de protocolos
Cain & Abel	**HTTPS**	Alto	Alto
Wireshark	**HTTP**	Alto	Bajo
	SMTP	Alto	Alto
	ARP	Medio	Bajo
	DNS	Medio	Alto
	TLVS1	Alto	Medio
	DHCP	Medio	Alto

Tabla 4.4. Métrica 1 de visibilidad y Métrica 2 de Vulnerabilidad de los protocolos utilizados para la comunicación en las aplicaciones móviles
Elaboración: Los Autores

El siguiente cuadro **(Cuadro 4.1)** es un análisis del comportamiento de las tramas en el momento que se realizó el experimento de ataque en los dispositivos móviles Android con Wireshark y Caín & Abel, donde se obtiene como resultado que al momento del envío y recepción de datos, los paquetes tienen la misma estructura de trama en las diferentes versiones de este sistema operativo, es decir, no hubo ninguna variación al momento de la irrupción en el nivel de transferencia de datos de los dispositivos **(Anexo 4).**

MODELO DE SMARTPHONE	VERSIÓN DE ANDROID	ESTRUCTURA DE LA TRAMA	
		Wireshark	Caín y Abel
Alcatel Idol 3	5.0.2	No varía	No varía
Samsung Galaxy A5	5.0.2	No varía	No varía
Samsung Galaxy Ace	2.3.4	No varía	No varía
Huawei y 550-l03	4.4.4	No varía	No varía
Sony Ericsson Xperia Z3 D6603	6.0.1	No varía	No varía

Cuadro 4.1. Comparación del comportamiento de las tramas con el programa Wireshark y Caín & Abel
Elaboración: Los autores

RECOLECCIÓN DE LOS DATOS CORRESPONDIENTES A LOS PARÁMETROS DE PRUEBAS DE LOS PROTOCOLOS DE SEGURIDAD DE LOS DISPOSITIVOS MÓVILES ANDROID.

ANÁLISIS DEL NIVEL CUANTITATIVO – METRIC

En la **Tabla 4.5** se puede observar los resultados obtenidos en la evaluación de las métricas de los protocolos de seguridad, referente al nivel de visualización en las diferentes capas del modelo OSI se puede observar en la capa de red los protocolos (ARP y HTTPS), en la capa transporte los (TCP y UDP) y en la capa de aplicación se muestra el (HTPP y DNS).

Con la utilización de software **(Anexo 4)**, solo se detectó el tipo de protocolo que está interviniendo en el momento del envío, mostrándolo, pero no se logró visualizar su contenido por lo tanto los protocolos de las App móviles no son vulnerados, constando de esta manera que los protocolos de seguridad no se encapsulan en su totalidad la información de los paquetes de datos, provocando un ataque desprevenido en la transferencia de mensajes.

NIVEL OSI	PROTOCOLO	VISUALIZADO CON WIRESHARK	VISUALIZADO CON CAÍN & ABEL
Red	ARP	Si	Si
Transporte	TCP	Si	No
	UDP	Si	No
Aplicación	HTTPS	No	Si
	HTTP	Si	No
	DNS	Si	No

Tabla 4.5. Información general de la visualización de los Protocolos de seguridad en el modelo OSI
Elaboración: Los Autores

En la siguiente **Tabla 4.6** se muestra la Métrica 2 y los resultados obtenidos en cuanto a la vulnerabilidad de los protocolos de seguridad, utilizando los mismos programas para la Métrica 1.

NIVEL OSI	PROTOCOLO	NIVEL DE SEGURIDAD CON WIRESHARK	NIVEL DE VULNERABILIDAD CON CAÍN & ABEL
Red	ARP	Bajo al contar con un encriptado en la trama del paquete	Alto al visualizar las direcciones IP para su manipulación
Transporte	TCP	Bajo al contar con un encriptado en la trama del paquete	
	UDP	Bajo al contar con un encriptado en la trama del paquete	
Aplicación	HTTP	Bajo al contar con un encriptado en la trama del paquete	
	HTTPS		Bajo al contar con un encriptado complejo y bloqueo de direcciones durante su ejecución
	DNS	Bajo al contar con un encriptado en la trama del paquete	

Tabla 4.6. Información general de la vulnerabilidad de los Protocolos de seguridad en el modelo OSI
Elaboración: Los Autores

Los autores consideraron todos los problemas de las Apps que hay actualmente, utilizando programas como herramientas que permitieron detectar los protocolos de seguridad para evaluar las métricas y vulnerabilidades más

comunes en los dispositivos móviles, y con esto llevar un control y realización de las respectivas pruebas a los datos recogidos en el que se observaron los riesgos antes mencionados y su afectación respectiva, dejando así establecida que más de la mitad de todos los Smartphones Android presentan seguridad en los protocolos de las Apps y no presenta vulnerabilidad al momento de querer desencriptar o ver el contenido de las tramas (Bernad, 2012).

Una publicación hecha por Pascual, J. 2015, en el portal de MSN, refiere que independientemente de la red WiFi los paquetes de datos pueden estar encriptados o no, en función de que el usuario esté usando un servicio o web encriptado. Si la web empieza por HTTPS, entonces lo está.

Los autores de esta investigación de acuerdo a esta publicación pueden determinar que el protocolo con más seguridad y no es vulnerado tan fácilmente es HTTPS, ya que este protocolo encripta la información y no la visualiza al hacker o a la persona que intenta acceder a la información.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Fue imprescindible conocer los tipos de protocolos de las aplicaciones móviles para la evaluación y la medición del nivel de vulnerabilidad en el envío y recepción de los paquetes de datos **(Ver Tabla 4.4)**.

- Para el desarrollo de aplicaciones móviles seguras se debe tener claro el sistema operativo, las tecnologías y las redes de comunicación, además de implementar procesos de desarrollo de aplicaciones seguras, las buenas prácticas de desarrollo y los estándares o protocolos que ayudarán a minimizar errores, fallas y vulnerabilidades, con el objetivo principal de aplicar métricas que permitan minimizar la inseguridad de la información, porque no existen aplicaciones o sistemas de computación cien por ciento seguros.

- De acuerdo a los resultados de las pruebas realizadas con los programas WIRESHARK y CAIN & ABEL se concluye que el protocolo ARP es el más vulnerable debido a que su nivel de seguridad es Bajo y la información fácilmente puede ser manipulada, mientras que el protocolo HTPPS y SMTP son los que tienen un alto nivel de seguridad. **(Ver Tabla 4.6)**.

- Realizado el análisis en el envío y recepción de datos se concluye que con Wireshark se visualiza más el tráfico de datos que con Caín & Abel, pero en ambos programas no varía la estructura de la trama en los diferentes dispositivos móviles Android en diferentes versiones **(Ver Cuadro 4.1).**

5.2. RECOMENDACIONES

- Realizar varias prácticas y revisiones en el momento de envío y recepción de mensajes para asegurarse que los datos hayan llegado correctamente siguiendo todas las medidas de seguridad de información y así evitar los ataques de hackers.

- Actualizar las versiones de App de los dispositivos móviles teniendo en cuenta en qué tipo de red se va a conectar ya que los protocolos que son utilizados ayudan a minimizar la inseguridad de la información en cada uno de los procesos que se manejan en la transferencia de datos.

- Verificar en el momento de acceder a la conexión Wi-Fi, que el protocolo que se está utilizando sea HTPPS y SMT en las App móvil ya que con ellos el nivel de seguridad es Alto y no permite que la información sea vulnerada en el instante de que haya una comunicación en una red abierta o privada, permitiendo también llevar un control al instante del envío-recepción de datos y así poder determinar mejor la funcionabilidad de los mismos.

- Mantener constantes evaluaciones en los protocolos de seguridad al momento de envío y recepción de datos para confirmar que las estructuras de las tramas mantienen su mismo proceso.

BIBLIOGRAFÍA

Bolois, J. 2013. Los protocolos de cifrado. (En línea). ES. Consultado el 13 de dic. 2015. Formato HTML. Disponible en: http://es.slideshare.net/Bolois/protocolos-de-cifrado-28745802.

Branding, T. 2012. Tipos de Aplicaciones para dispositivos Móviles. (En Línea). US. Formato HTML. Disponible en: https://tommybranding.wordpress.com/?s=aplicaciones+nativas

Burgos, D. y Echeverry, H. 2012. Estado del arte del uso de aplicaciones en dispositivos móviles en el área de la Telemedicina. (En Línea) EU. Consultado el 9 de diciembre de 2013. Formato PDF. Disponible en: http://recursosbiblioteca.utp.edu.co/tesisd/textoyanexos/0053B957.pdf

González, S. 2013. Aplicaciones móviles (En Línea). Formato HTPP. Disponible en:http://www.estoespurpura.com/2013/12/que-son-lasaplica cionesmoviles/

Hütt, H. 2012. Las redes sociales: una herramienta para la difusión. Revista Reflexiones. Universidad de Costa Rica. San José, CR. Vol. 91. Núm. 2. Pág. 121-128.

JCGM (Comité Conjunto de Guía en Metrología). 2010. Evaluación de datos de medición. 3ra. Edición. Centro Español de Metrología. España. pág. 68.

Lara, P; Serradel, E y Maniega, E. 2014. App, movilidad de contenidos para la extensión de servicios de información. Textos Universitario biblioteconomía i documentación. Universidad de Barcelona. España. Vol. 1. Núm. 32. pág. 45.

LOES (Ley Orgánica Superior de Educación Superior). 2010. Constitución. Sistemas de educación. (En línea). EC. Consultado el 08 de jun. 2014. Formato PDF. Disponible en: http://www.ceaaces.gob.ec/sitio/wp-content/uploads/2013/10/loes1.pdf

Martínez, F. 2011. Aplicaciones para dispositivos móviles (En Línea). Consultado el 8 de diciembre de 2013. Formato PDF. Disponible en: http: //riunet. upv.es/bitstream/handle/10251/11538/Memoria.pdf?sequence= 1

Menéndez, R y Barzanallana, A. 2012. Historia del desarrollo de aplicaciones web. (En línea). AL. Consultado el 10 de ago. 2014. Formato HTML. Disponible en: http://www.um.es/docencia/barzana/DIVULGACION/INFORMATICA/Historia-desarrollo-aplicaciones-web.html

Novaley. 2014. Los Perfiles Falsos en las Redes Sociales (En Línea). Consultado el 13 de febrero 2014. Formato HTML. Disponible en: http://novaley.es/portada/los-perfiles-falsos-en-las-redes-sociales/

ONTSI (Observatorio Nacional de Telecomunicaciones y SI). 2011. Redes Sociales en Internet. (En línea). CO. Consultado el 02 de mar. 2014. Formato PDF. Disponible en: http://www.osimga.gal/export/sites/osimga/gl/documentos/d/20111201_ontsi_redes_sociais.pdf

Ortega, D. 2011. Privacidad y Seguridad en las Redes Sociales (En Línea). Consultado 12 de Enero 2013. Formato HTML. Disponible en: http://recursostic.educacion.es/observatorio/web/es/internet/recursos-online /1015-daniel-ortega-carrasco

Peñalva, M. 2014. Modelo de evaluación de la calidad de aplicaciones Web en e-government. (En línea) AR. Consultado el 13 de dic. 2015. Formato PDF. Disponible en: http://sedici.unlp.edu.ar/Documentocompleto.pdf?sequence=1

Pérez, C. 2010. Goal Question Metric. (En línea). ES. Consultado el 07 de sep. 2014. Formato HTLM. Disponible en: http://asprotech.blogspot.com/2010/09/goal-question-metric.html

_____. 2012. Modelos, normas, metodologías y técnicas para mejorar los procesos. (En Línea). ES. Consultado el 07 de sep. 2014. Formato HTML. Disponible en: http://asprotech. blogspot.com/2012/03/modelos-normas-metodologias-y tecnicas.html

Roca, M. 2014. Que son las redes Sociales (En Línea). Consultado 1 de enero de 2014. Formato HTML. Disponible en: http://www.informeticplus.com/que- son-las-redes-sociales

Ruiz, Y. 2014. E-Evaluación del aprendizaje: Aproximación conceptual. Revista Científica en Educación en Red Aula Magna 2.0. ISSN: 2386-6705. Universidad Nacional Experimental del Táchira (UNET). Venezuela. Vol 1. Núm. 1. pág. 32.

Sei, T. 2014. Alerta: Saber si una aplicación puede dañar mi cel. Consultado el 24 de Junio 2015. Formato HTML. Disponible en: http://www.androidjefe.com/como-saber-aplicacion-danar-celular/

Serrano, A; García, L; León, I; García, E; Gil, B y Ríos, L. 2010. Métodos de Investigación de enfoque experimental. (En línea). CO. Consultado el 3 de dic. 2014. Formato PDF. Disponible en: http://www.postgradoune.edu.pe/documentos/Experimental.pdf

Steffens, H. 2010. El uso de redes sociales y los riesgos de seguridad para las empresas (En Línea). Consultado 19 de febrero 2014. Formato HTML. Disponible en: http://pulsosocial.com/2010/11/11/el-uso-de-redes-sociales-y- los-riesgos-de-seguridad-para-las-empresas/

Van Dalen, B y Meyer, W. 2010. Estrategia de la Investigación Experimental. (En línea). ES. Consultado el 26 de mar. 2016. Formato PHP. Disponible en: http://noemagico.blogia.com/2006/092201-la-investigacion-experimental.php

Vizuete, M. 2012. Soluciones móviles y su influencia en los usuarios a escala mundial. (En Línea). MX. Consultado el 16 de dic. 2013. Formato PDF. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/4901/1/UPS-QT03467.pdf

ANEXOS

ANEXO 1: CERTIFICACIÓN DEL TRIBUNAL

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
"MANUEL FÉLIX LÓPEZ

EPÚBLICA DEL ECUADOR

CARRERA DE INFORMÁTICA

Calceta, 23 de julio 2015

Oficio ESPAM MFL Nº-07

Ing. Fernando Moreira Moreira
DOCENTE – TUTOR DE TESIS
Ciudad.-

De mi consideración:

Reciba un cordial saludo y deseándole el mayor de los éxitos en su labores diarias.

Toda vez que se recibió el oficio s/n de fecha 16 de julio de 2015, suscrito por el Ing. Fernando Moreira tutor de la tesis "Evaluación de protocolos de seguridad de las APP de redes sociales en dispositivos móviles android ", de los autores Teresa García y Jorge Alberto, donde expone que la tesis de los postulantes se encuentra en la fase final, pero no se ha podido culminar en los lapsos establecidos en el cronograma que platearon los autores, debido a que uno de los autores tiene su hijo con diagnostico parálisis cerebral infantil. Los integrantes del tribunal de software resuelven que:

1. *De acuerdo a los estipulado en el manual de investigación Art. 37, el cual manifiesta que los "postulante(s) queda obligado a repetir, por única vez, toda la etapa del desarrollo de tesis, acatando lo dispuesto en los capítulos VI y VII de este reglamento. De reincidir en la no aprobación de la tesis, el postulante(s) debe asistir a las clases del curso Proyecto de Tesis del noveno semestre, para iniciar notificación de un nuevo tema", por lo tanto este tribunal se acoja a este Art. Para que los postulantes concluya con el trabajo investigativo.*

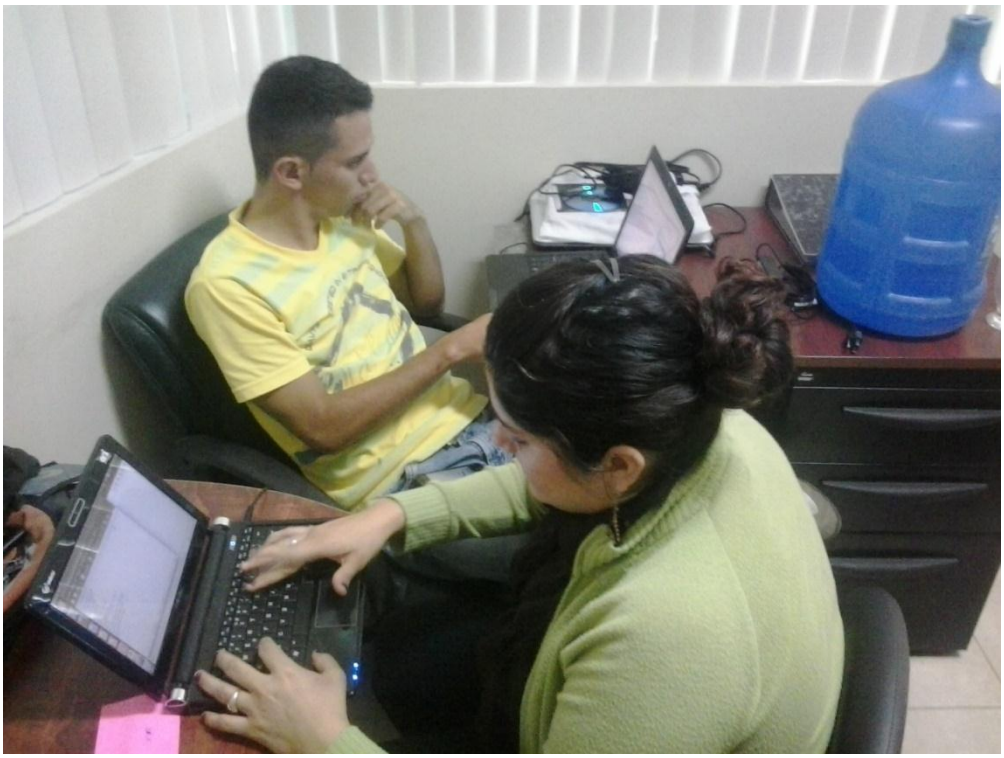
Particular que comunico a usted para los fines legales pertinentes.

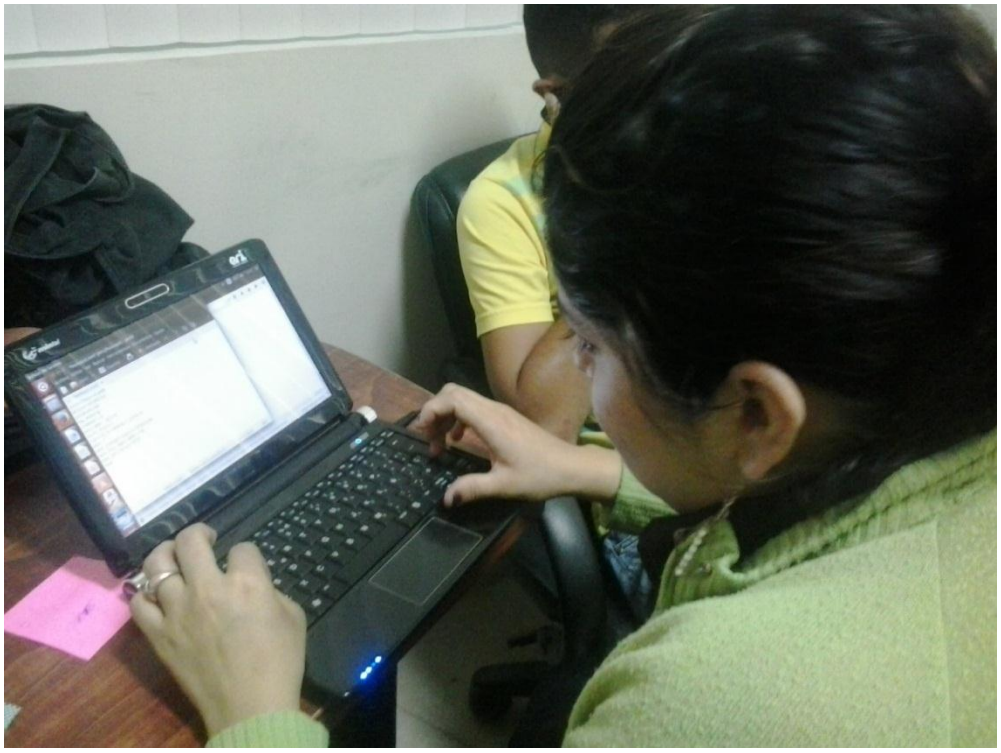
Lic. Guillermo Intriago C
PRESIDENTE DEL TRIBUNAL

Recibido 23/07/15

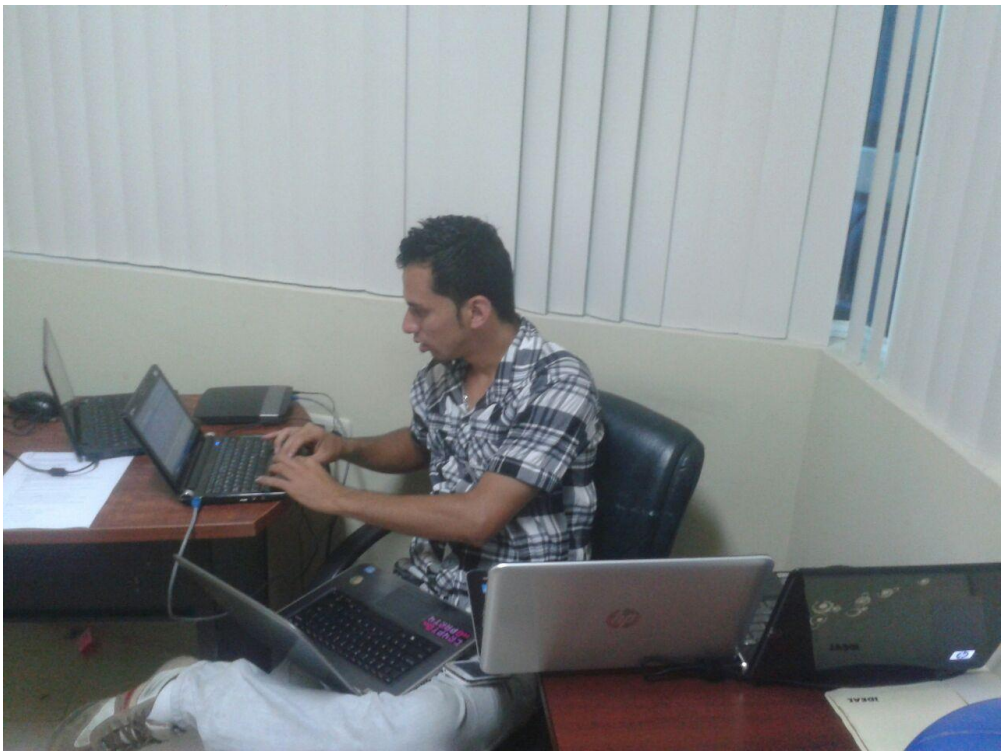
Dirección: Campus Politécnico Sitio "El Limón". **Teléfono: (05)3029021**
Email: informatica@espam.edu.ec
CALCETA - ECUADOR

ANEXO 2: ANÁLISIS DE REGIMIENTOS DE LOS PROTOCOLOS MÁS COMUNES DE APP'S MÓVILES

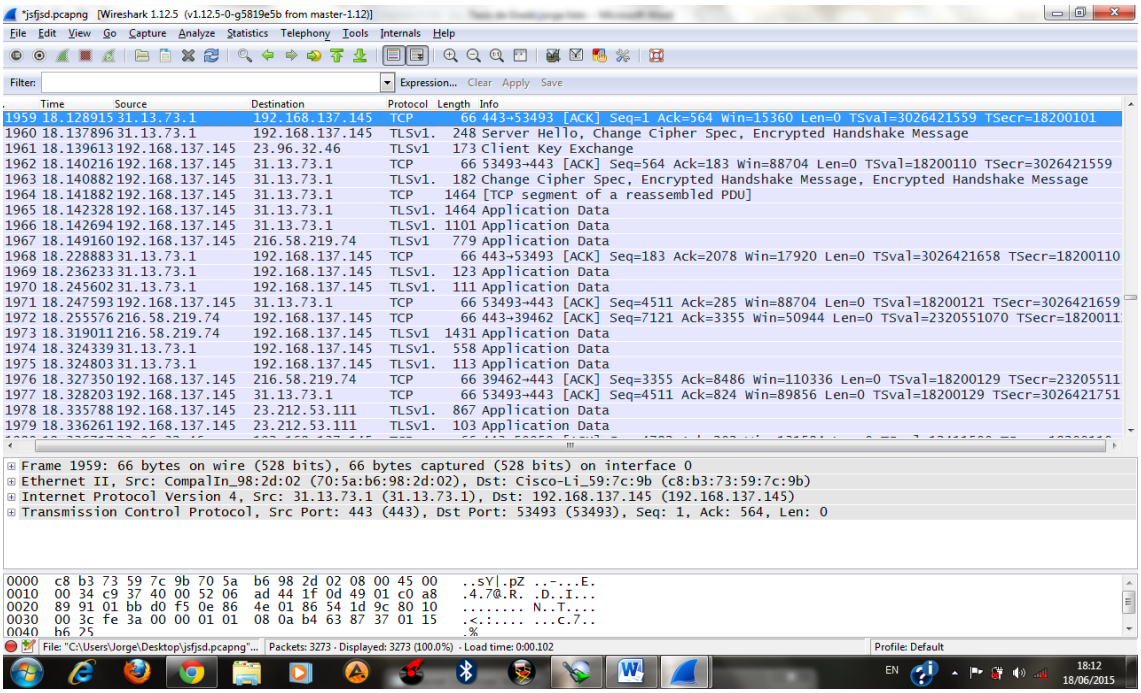




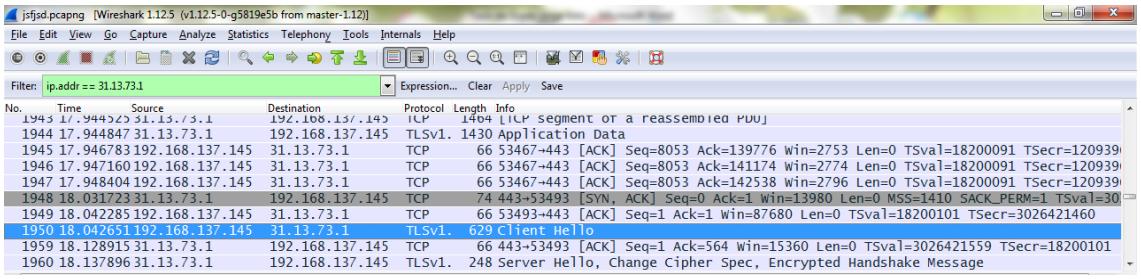
ANEXO 3: PRUEBAS DE WIRESHARK PARA EL ANÁLISIS DE PROTOCOLOS DE REDES SOCIALES Y MENSAJERÍA INSTANTÁNEA EN DISPOSITIVOS MÓVILES



ANÁLISIS DE PROTOCOLOS MEDIANTE EL PROGRAMA WIRESHARK

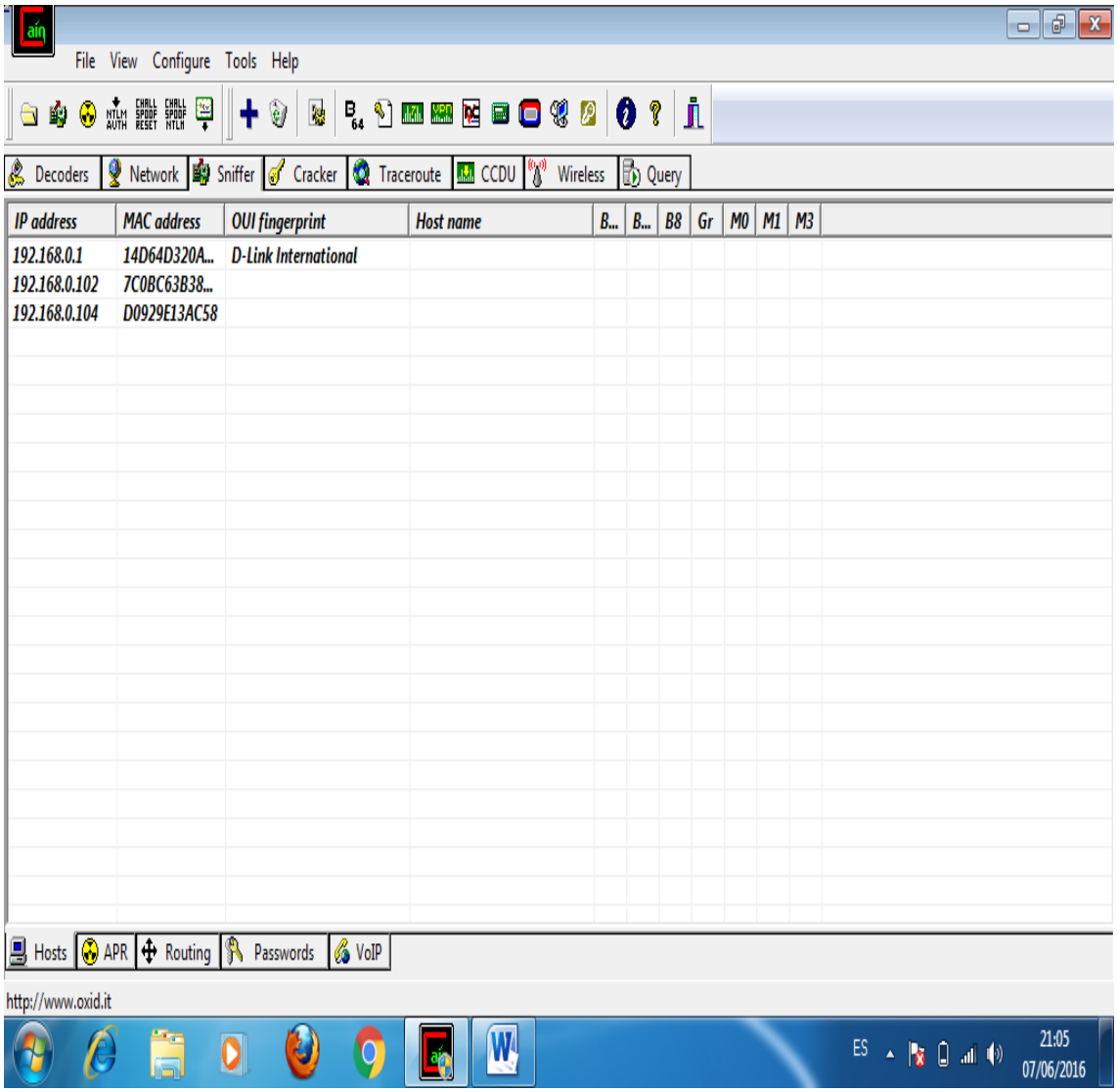


PROTOCOLO VULNERADO ARP MEDIANTE EL PROGRAMA WIRESHARK

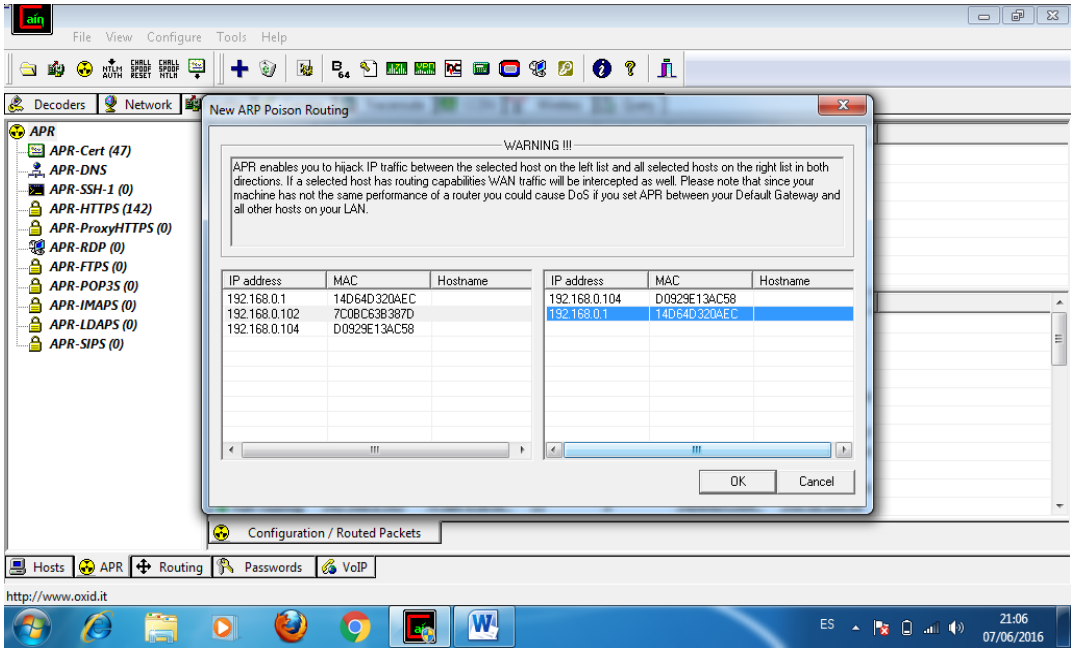


ANEXO 4. EXPERIMENTO DE ATAQUE CON LOS PROGRAMAS WIRESHARK Y CAÍN & ABEL A LOS DIFERENTES DISPOSITIVOS MÓVILES ANDROID CON DIFERENTES VERSIONES

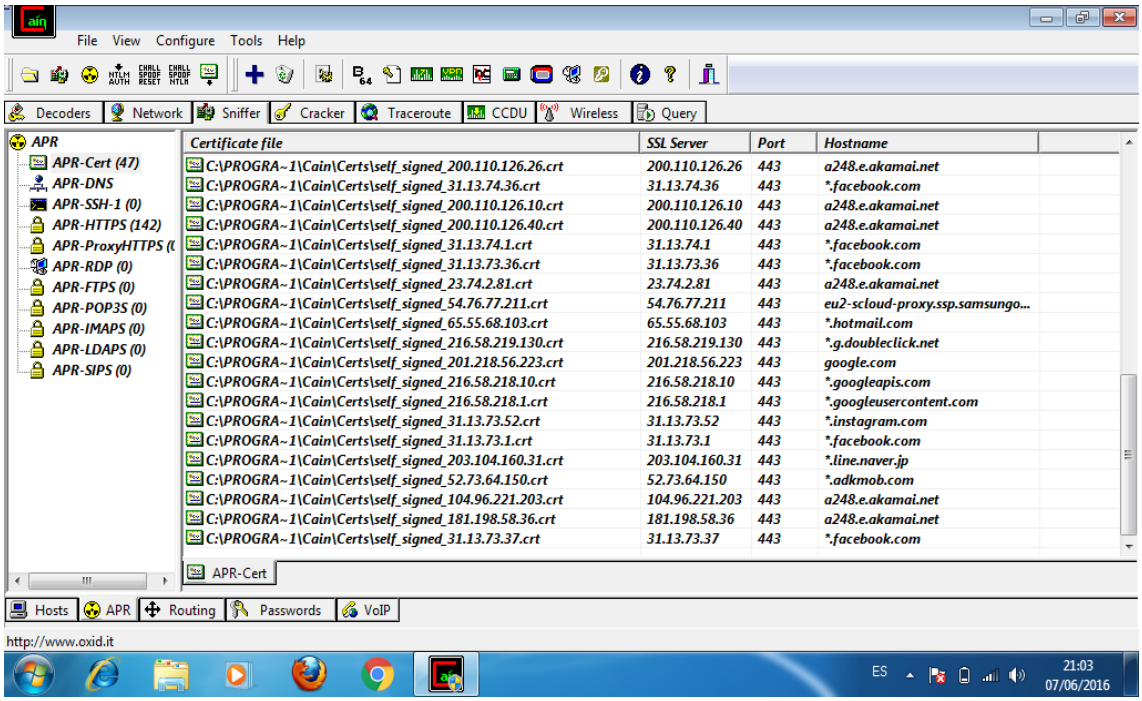
ANEXO 4.1. ESCANEO DE LA RED PARA HACER EL ATAQUE EN EL DISPOSITIVO MOVIL SAMSUNG A5



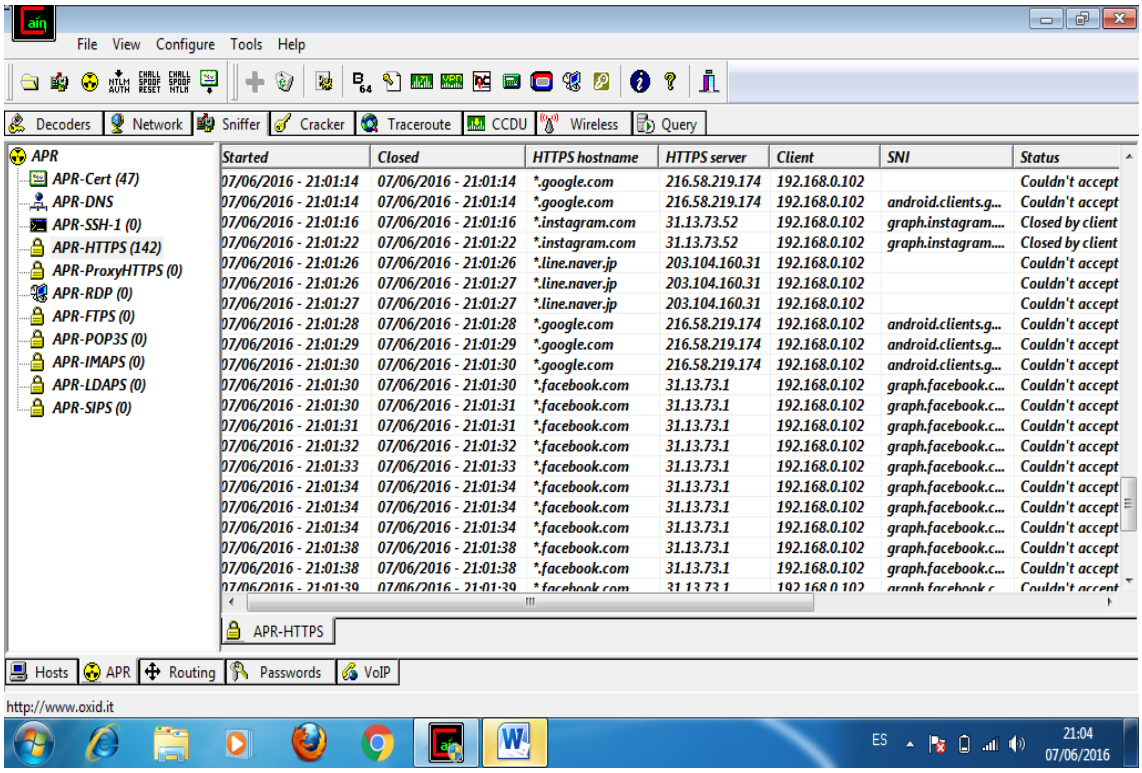
ANEXO 4.1.1. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ESCANEO DE LA RED EN BÚSQUEDA DE DIRECCIONES Y SELECCIÓN DEL HOST AL QUE SE VA ATACAR.

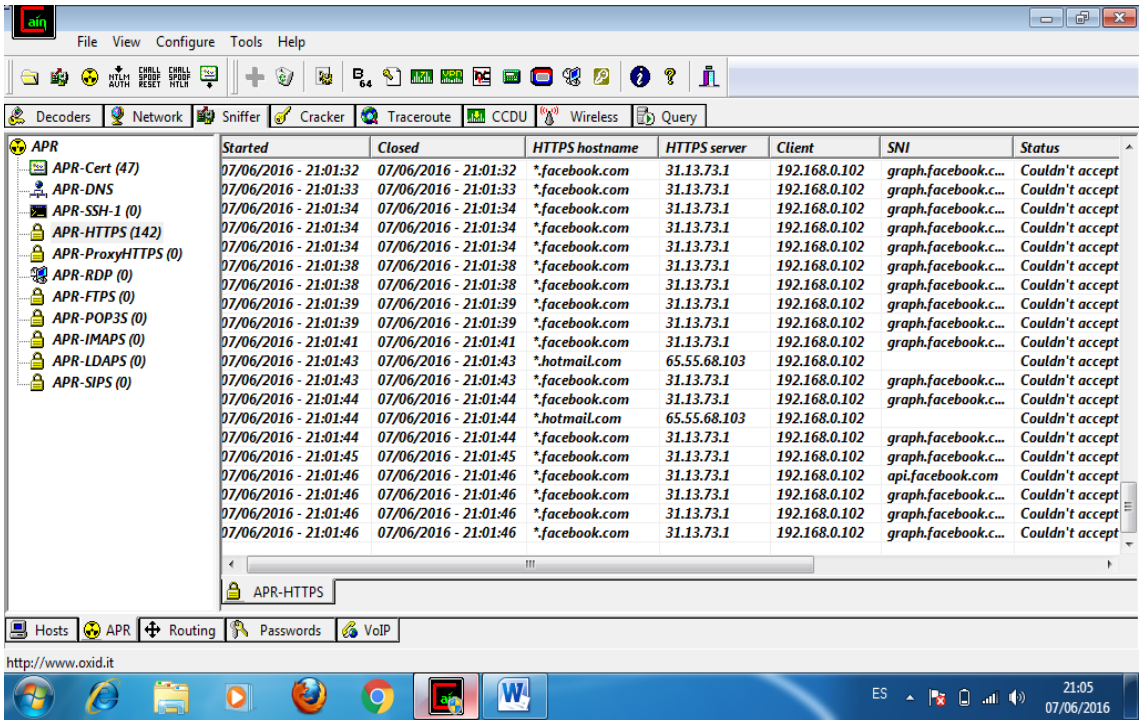


ANEXO 4.1.2. ASIGNACIÓN DE CERTIFICADOS POR PARTE DE CAÍN & ABEL

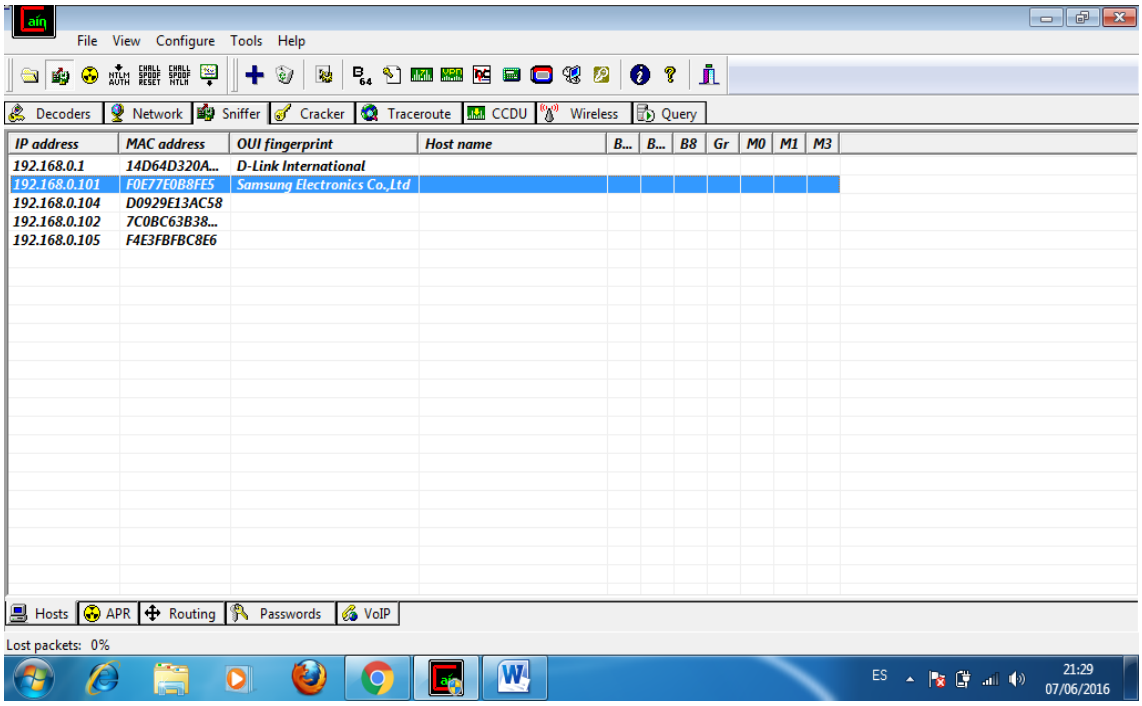


ANEXO 4.1.3. VISUALIZACIÓN DEL PROCOLO HTTPS

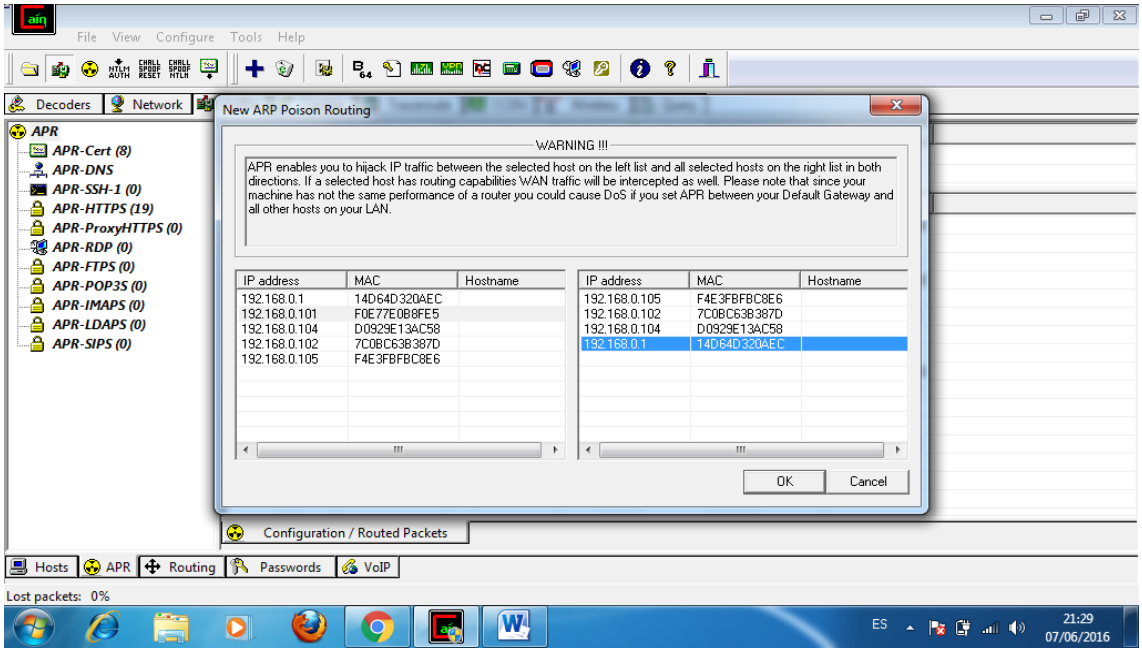




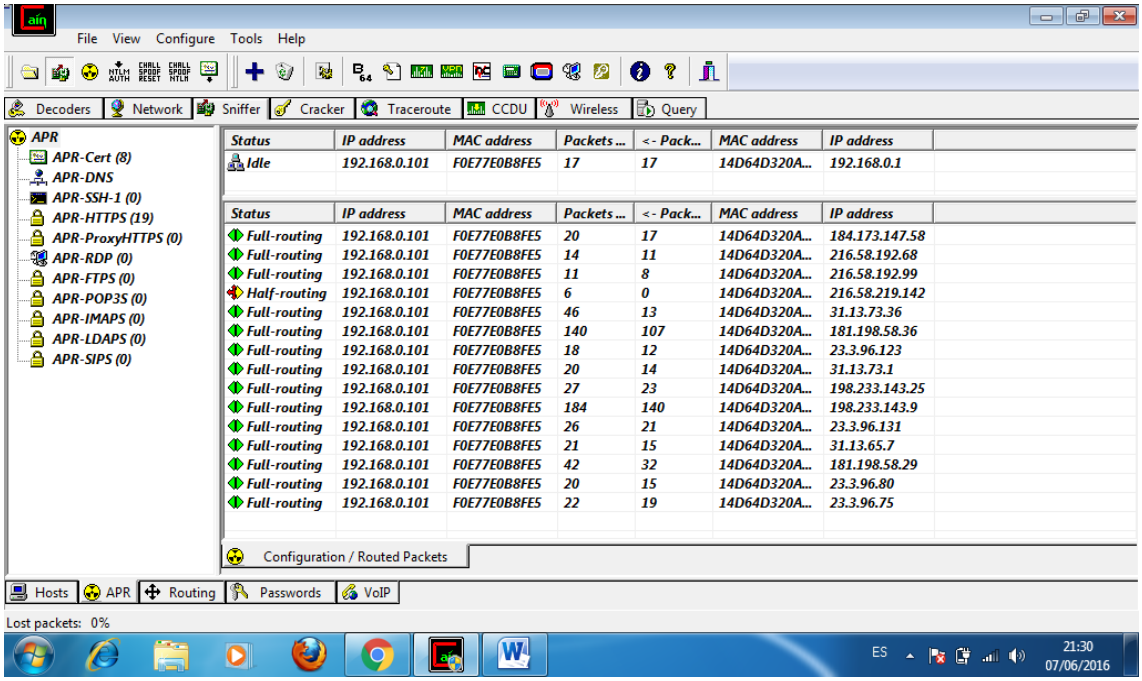
ANEXO 4.2. ESCANEO DE LA RED PARA HACER EL ATAQUE EN EL DISPOSITIVO MOVIL SAMSUNG ACE



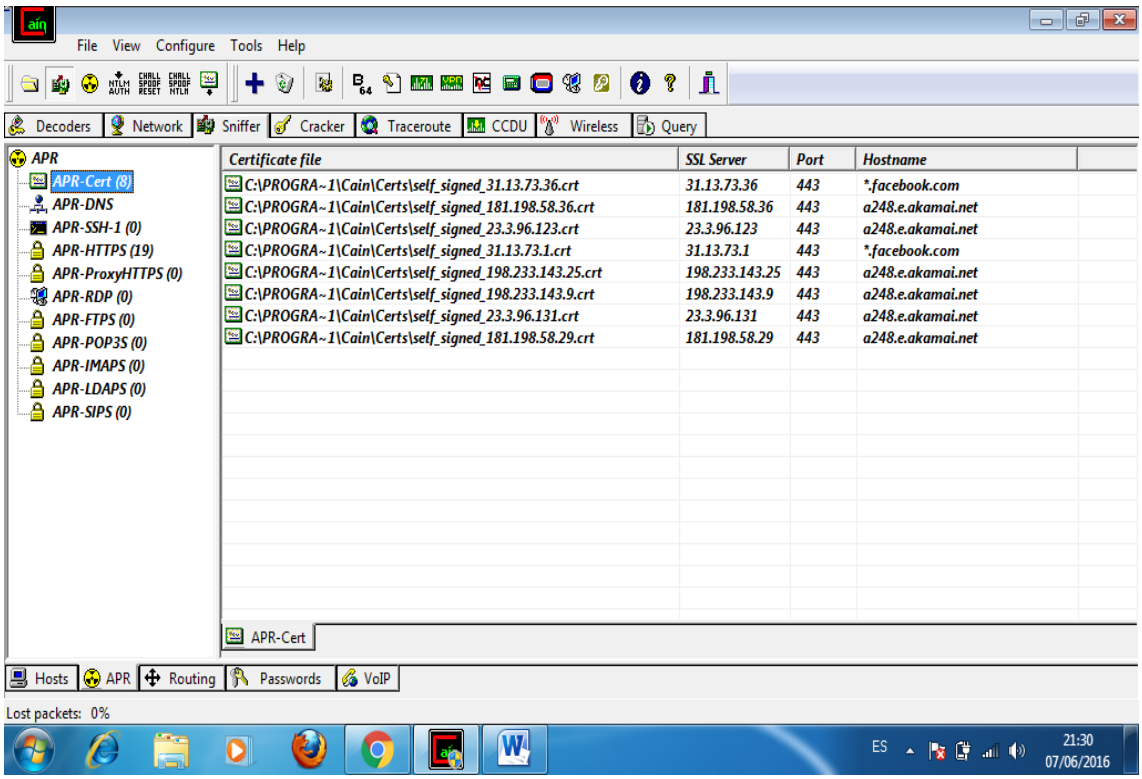
ANEXO 4.2.1. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ESCANEO DE LA RED EN BÚSQUEDA DE DIRECCIONES Y SELECCIÓN DEL HOST AL QUE SE VA ATACAR.



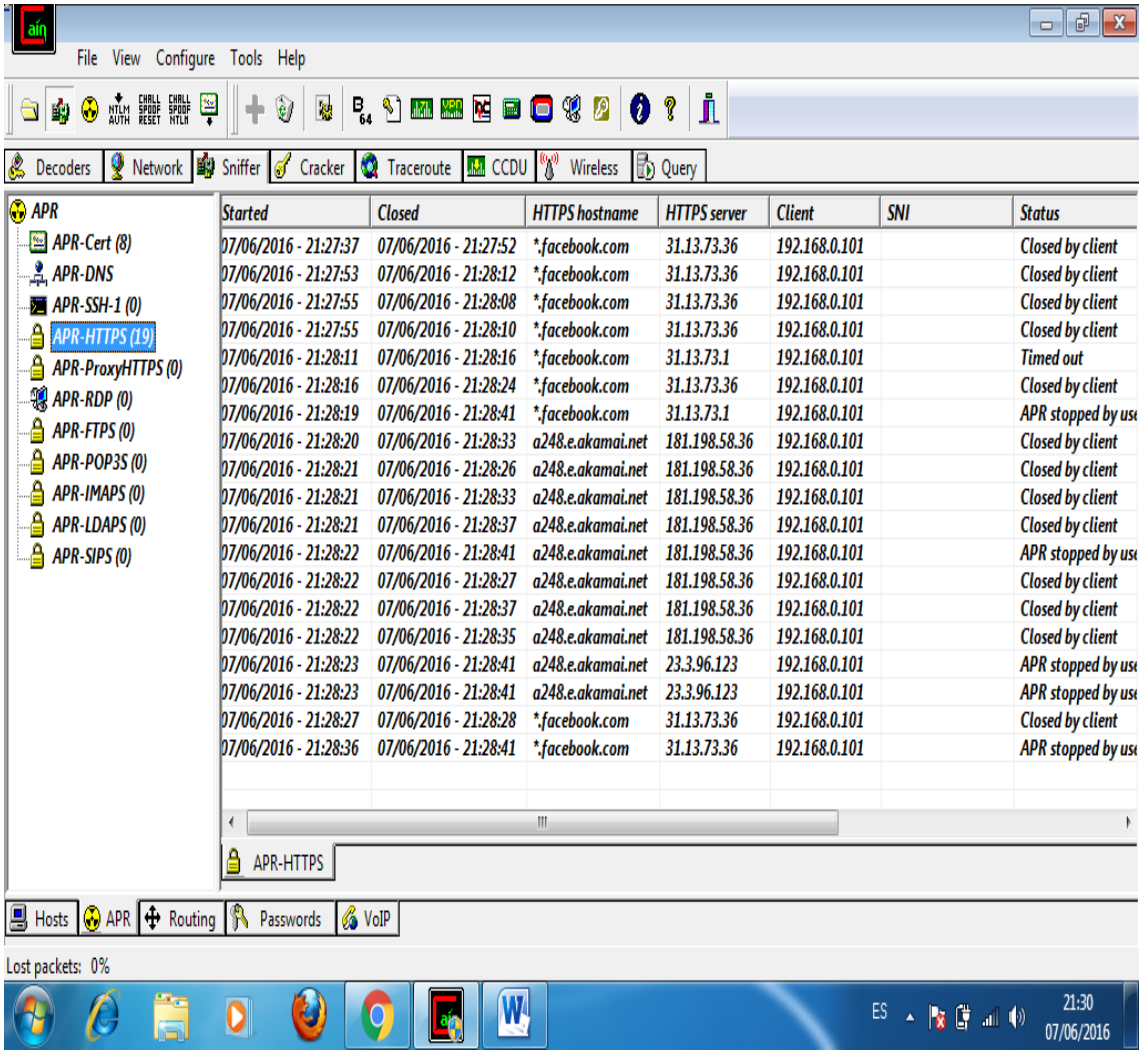
ANEXO 4.2.2. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ENVENENAMIENTO DE LA RED.



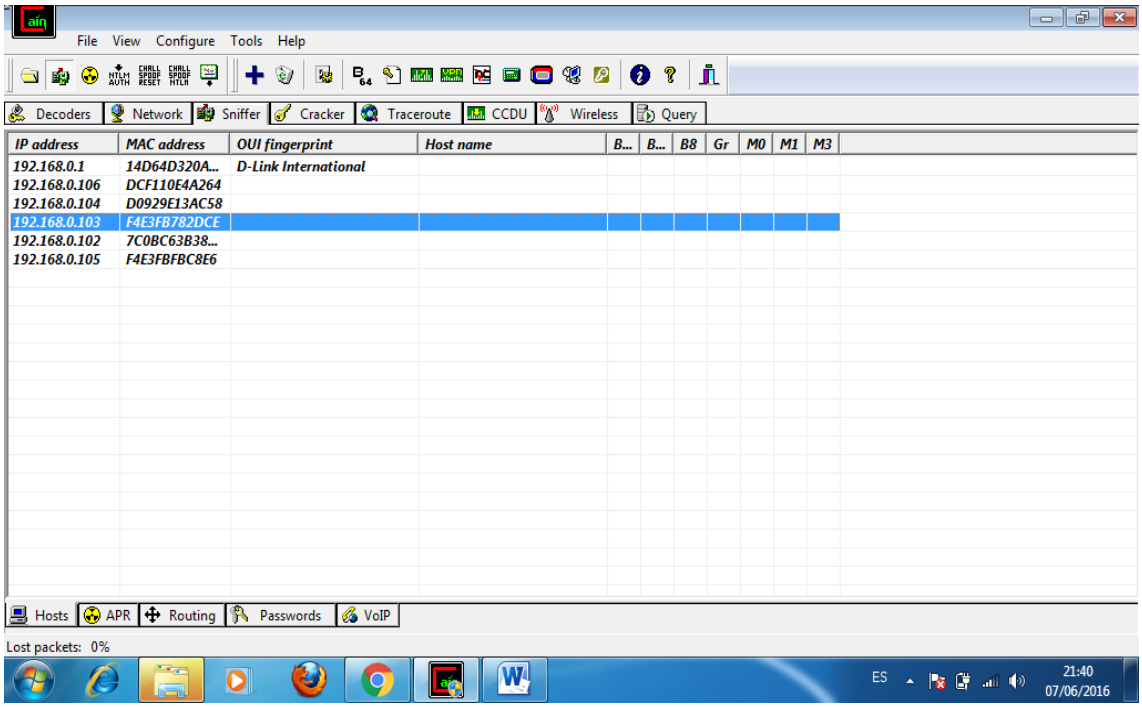
ANEXO 4.2.3. ASIGNACIÓN DE CERTIFICADOS POR PARTE DE CAÍN & ABEL



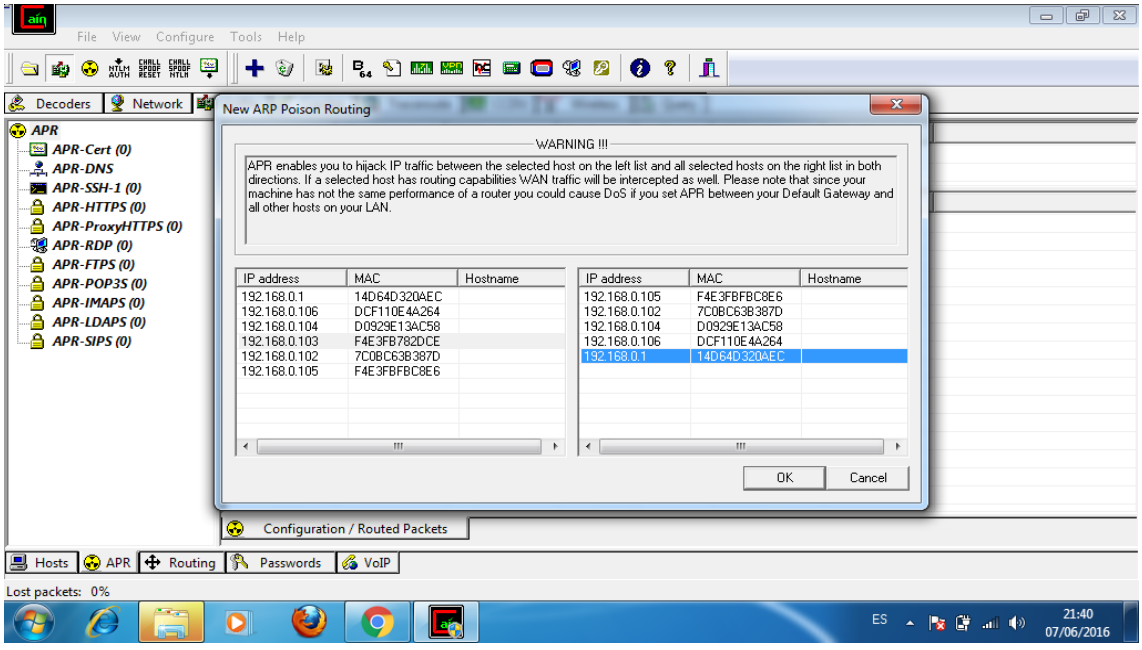
ANEXO 4.2.4. VISUALIZACIÓN DEL PROCOLO HTTPS



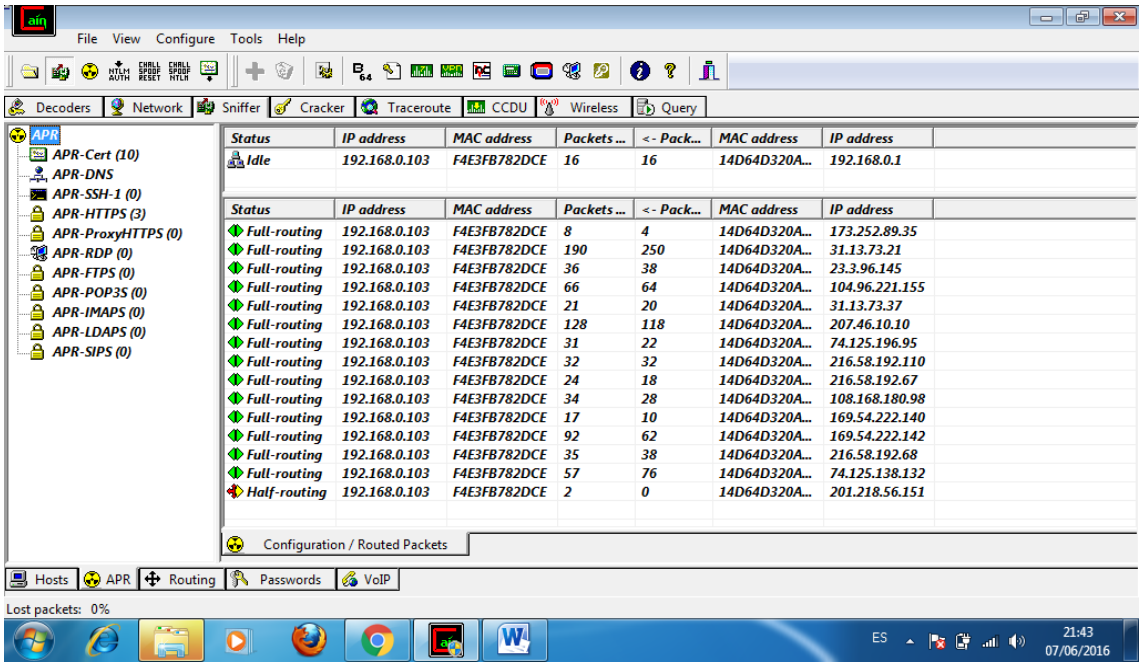
ANEXO 4.3. ESCANEO DE LA RED PARA HACER EL ATAQUE EN EL DISPOSITIVO MOVIL HUAWEI



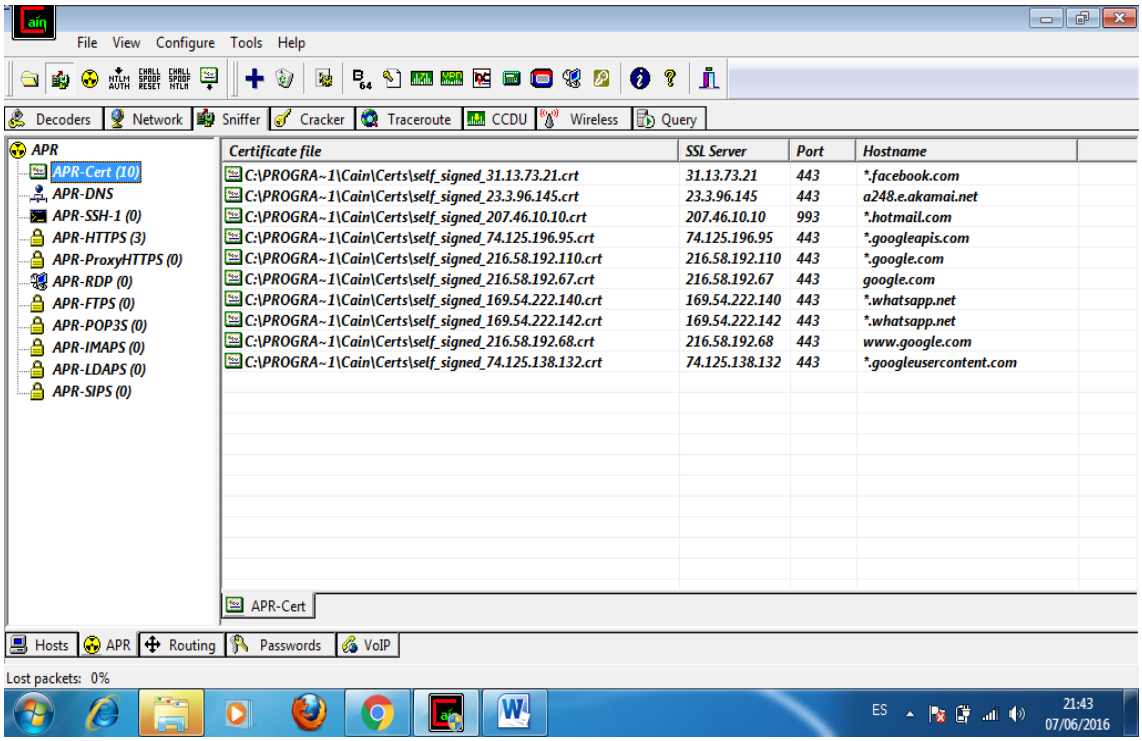
ANEXO 4.3.1. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ESCANEO DE LA RED EN BÚSQUEDA DE DIRECCIONES Y SELECCIÓN DEL HOST AL QUE SE VA ATACAR.



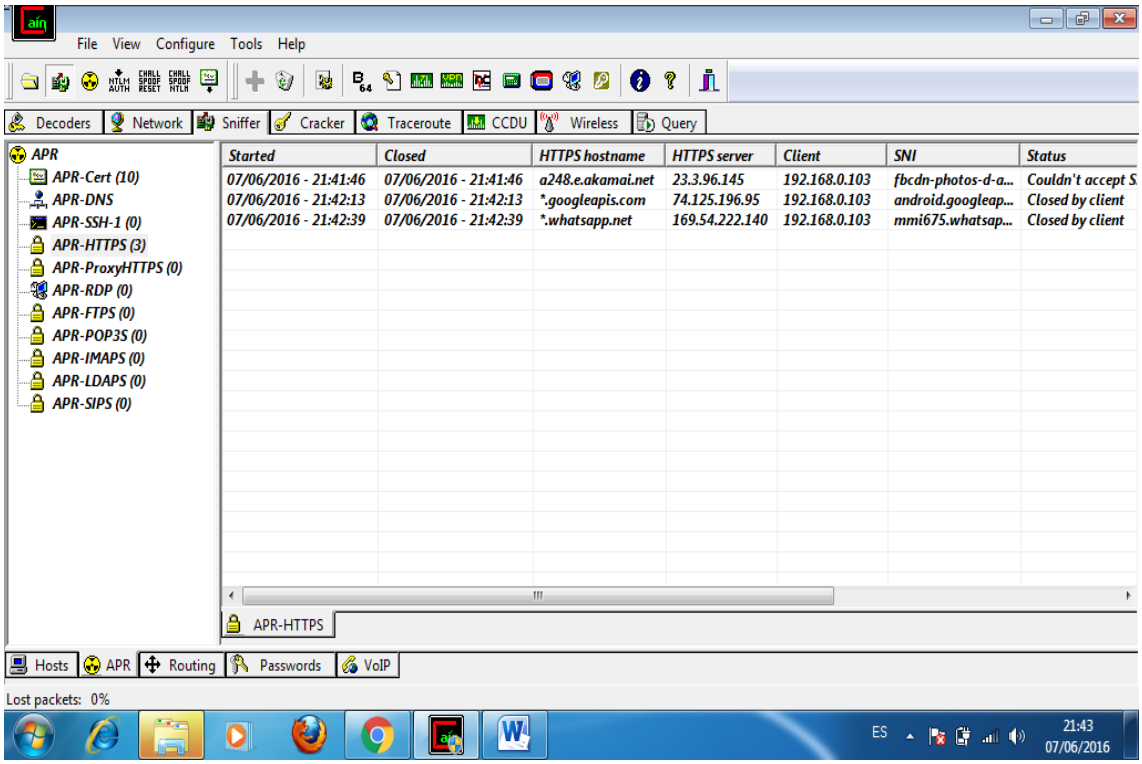
ANEXO 4.3.2. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ENVENENAMIENTO DE LA RED.



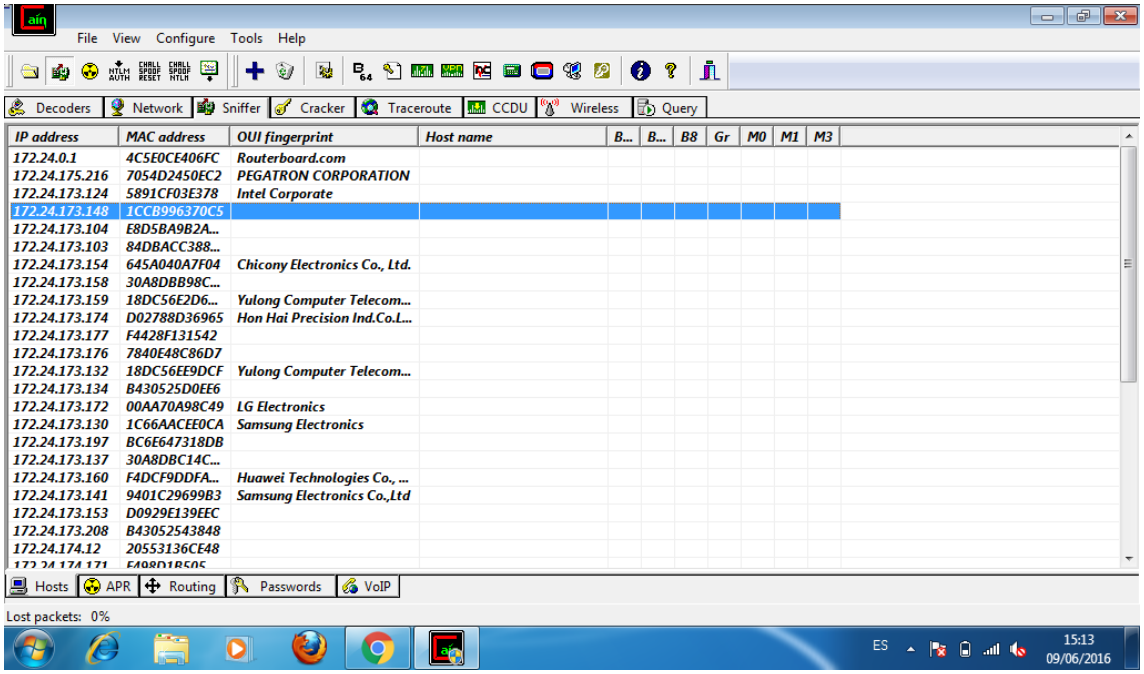
ANEXO 4.3.3. ASIGNACIÓN DE CERTIFICADOS POR PARTE DE CAÍN & ABEL



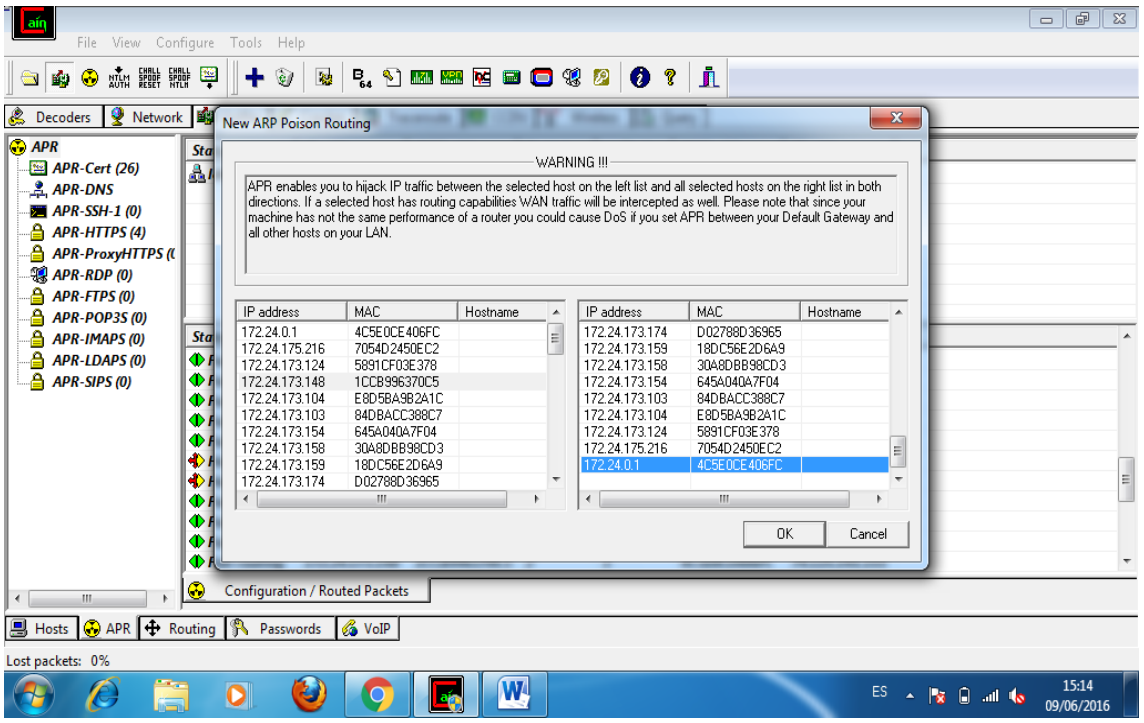
ANEXO 4.3.4. VISUALIZACIÓN DEL PROCOLO HTTPS



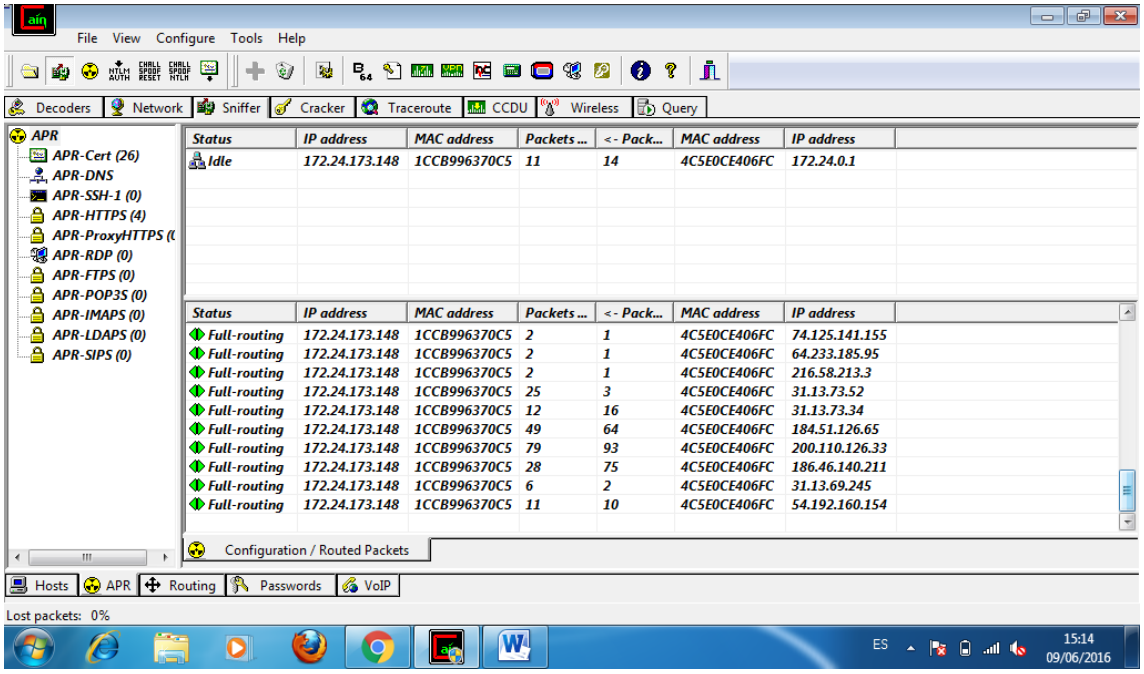
ANEXO 4.4. ESCANEO DE LA RED PARA HACER EL ATAQUE EN EL DISPOSITIVO MOVIL ALCATEL ONETOUCH IDOL 3



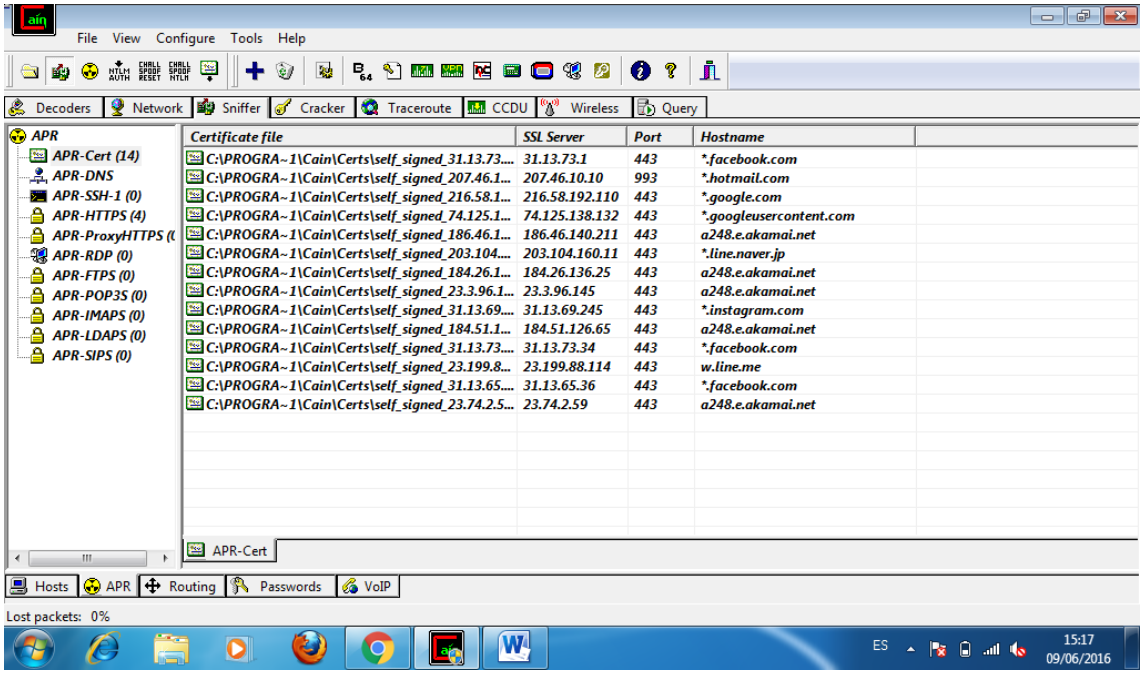
ANEXO 4.4.1. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ESCANEO DE LA RED EN BÚSQUEDA DE DIRECCIONES Y SELECCIÓN DEL HOST AL QUE SE VA ATACAR.



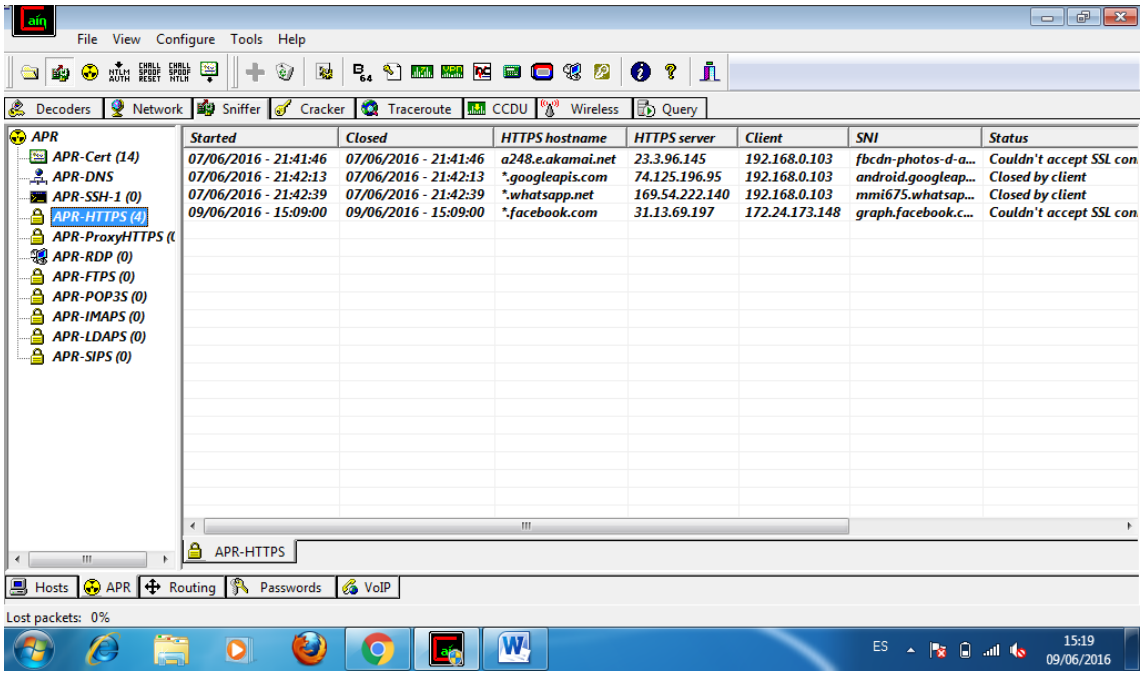
ANEXO 4.4.2. INICIACIÓN DE CAÍN & ABEL PARA REALIZAR EL ENVENENAMIENTO DE LA RED.



ANEXO 4.4.3. ASIGNACIÓN DE CERTIFICADOS POR PARTE DE CAÍN & ABEL



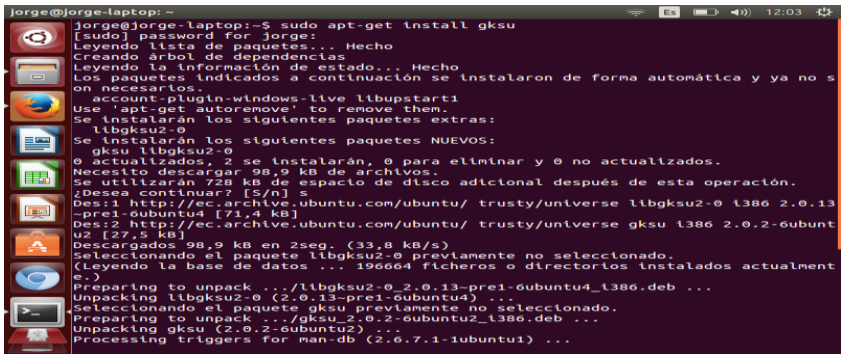
ANEXO 4.4.4. VISUALIZACIÓN DEL PROCOLO HTTPS



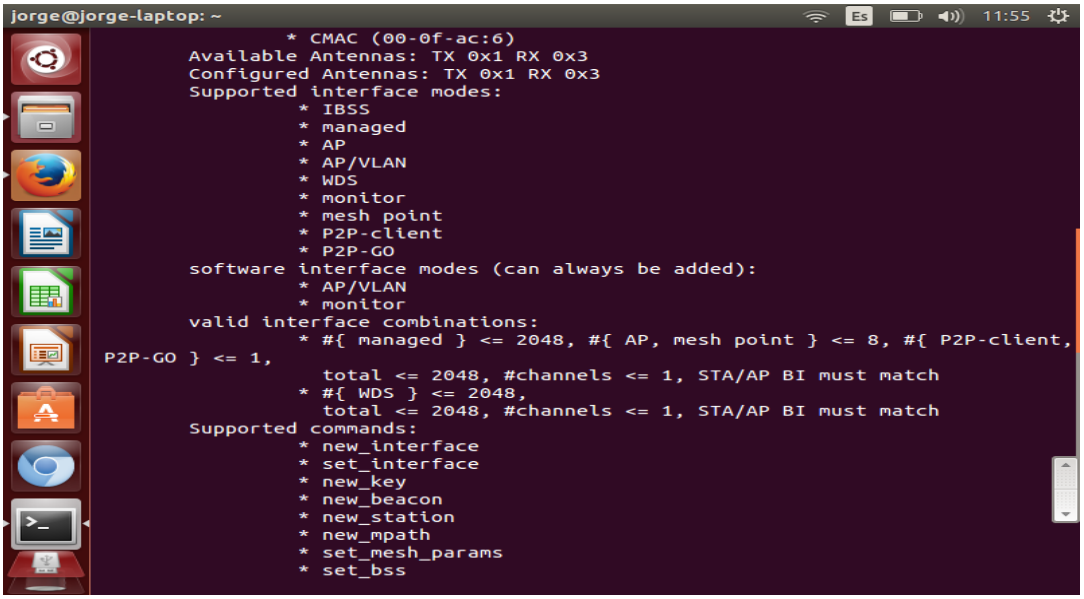
ANEXO 5. CONFIGURACIÓN DEL ACCES POINT EN UBUNTU

En el sistema operativo Ubuntu se realizó un punto de acceso inalámbrico es imprescindible contar con la instalación y configuración del hostapd el que permite tener un control total del acceso WLAN que mejoro la seguridad y el DNSMAQ que funciono como un mini servidor DHCP.

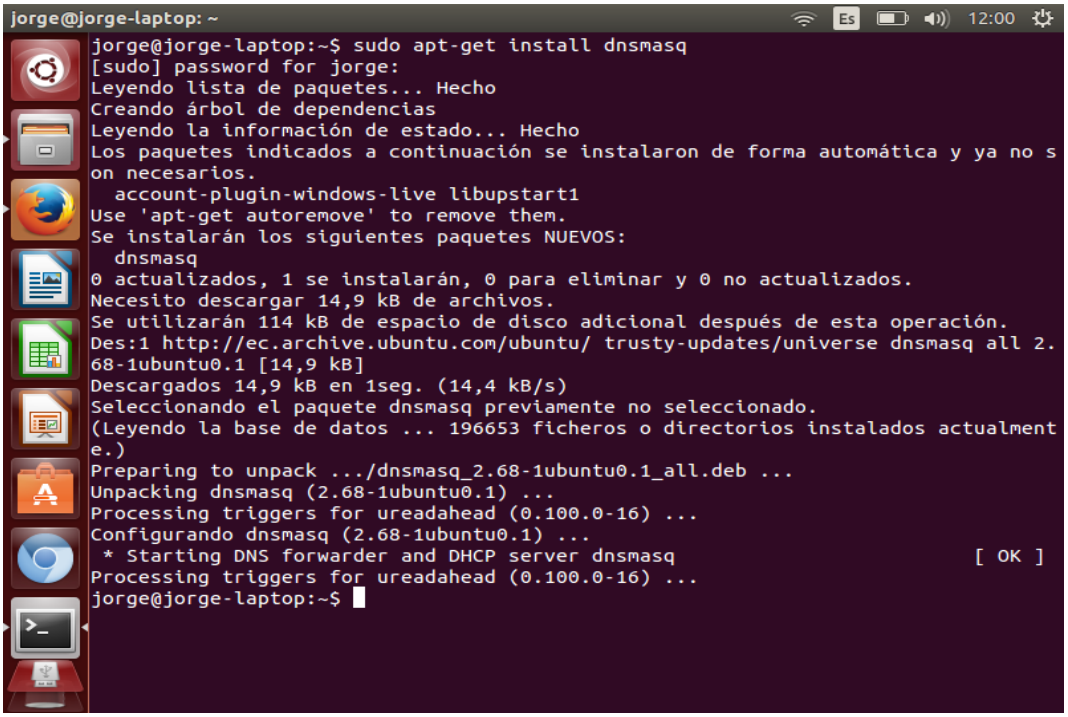
Instalación de archivos para la configuración del acces point



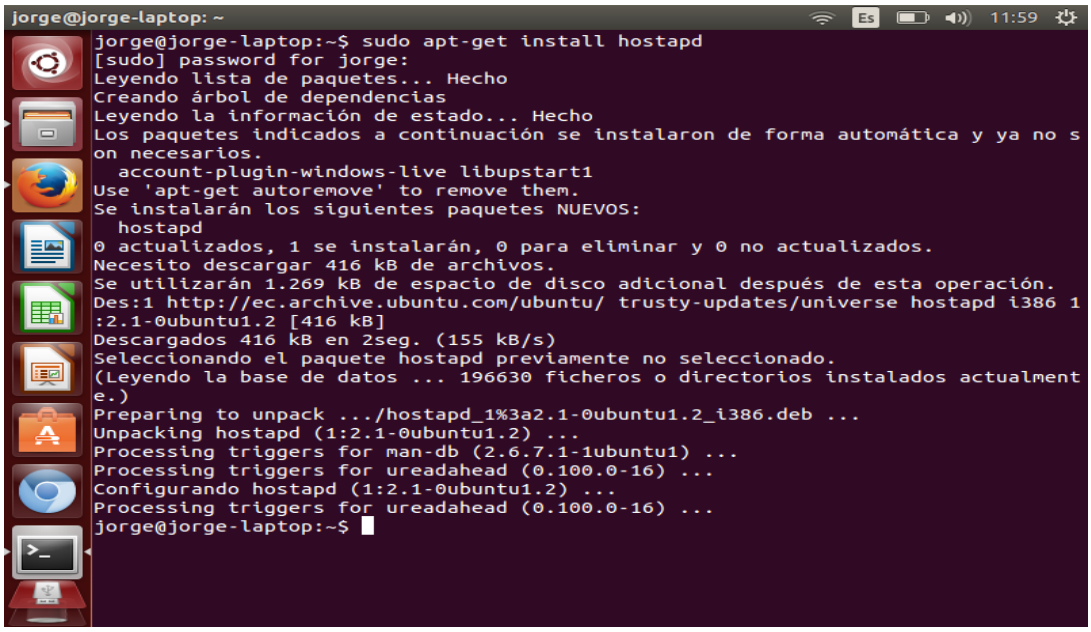
Instalacion del gksu



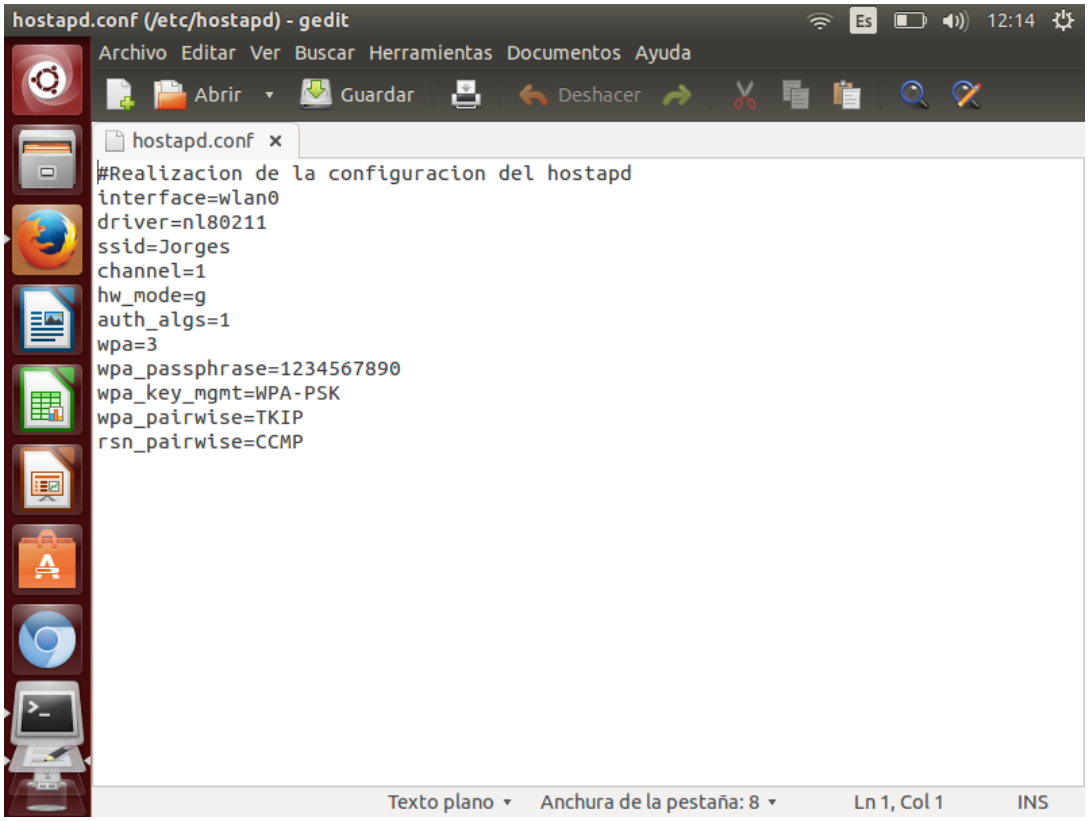
Comprobación si la interfaz soporta la creación de una AP



Instalación del dnsmasq mediante consola



Instalación del hostapd



Configuración del hostapd