Universidad Nacional Autónoma de Nicaragua, UNAN – León

Facultad de Ciencias y Tecnología

Ingeniería en Telemática

Título:

Análisis del uso que hacen los usuarios conectados a un punto de acceso inalámbrico, sin autenticación, con conexión a Internet, ubicado en el edificio CIDS de la Universidad Nacional Autónoma de Nicaragua (Unan-León), en el período comprendido entre el día 5 al día 23 del mes de octubre del año 2015.

Monografía para optar al título de Ingeniero en Telemática.

Autores:

Br. Roberto Francisco Duarte Martínez.

Br. Sherly Jessell Paredes Rios.

Tutor: M.Sc. Eduardo Santiago Molina.

León, Nicaragua

Septiembre de 2016.

Resumen

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras y dispositivos móviles con capacidad de conexión a internet mediante tecnología de red inalámbrica. Las redes inalámbricas facilitan la operación en los lugares en donde la computadora u otros dispositivos no pueden permanecer en un solo lugar como por ejemplo: en cafeterías, almacenes o incluso en oficinas que se encuentren en diferentes pisos de un edifico.

Anteriormente su uso era específicamente el laboral pero hoy en día a atrapado a gente de todas las edades principalmente jóvenes con el uso de la señal y el internet como medio de entretenimiento. Se puede observar su gran uso en los centros educativos como escuelas, colegios, universidades etc.

Vemos como las redes inalámbricas Wi-Fi han posibilitado la sustitución de los cables por ondas de radio. De este modo, se eliminan las ataduras y limitaciones de los dispositivos de conexión. Pero también permiten una mayor facilidad para que cualquiera tenga acceso a los datos que circulan por la red. Si con los cables un atacante debía obtener acceso físico a un punto de acceso para poder realizar alguna acción, con las redes inalámbricas esta tarea se vuelve trivial. Al eliminarse el componente físico que podía llegar a proteger los datos, éstos quedan mucho más expuestos.

Este trabajo monográfico trata sobre el uso que hacen los usuarios conectados a un punto de acceso inalámbrico sin autenticación con conexión a Internet ubicado en el edificio CIDS de la Universidad Nacional Autónoma de Nicaragua (Unan-León) en el período comprendido entre el día 5 al día 23 del mes de octubre del año 2015.

En él se abordan temas como son la gran importancia del tipo de información que se comparte en la red a través de APs desconocidos y como los usuarios se comportan ante estos, el tiempo que dedican y maneras de cómo mejorar el tráfico en dicho AP.

También se toman a bordo temas de gran importancia como son los las definiciones de trafico de red, los protocolos de red sus estándares etc. Así como los métodos que se utilizaron para el logro de este trabajo, las herramientas físicas y aplicaciones mediante las cuales es posible obtener información sobre el tráfico de red además de mostrar los resultados específicos obtenidos que se proponen en los objetivos de este trabajo monográfico.

Índice de Contenido.

Índice de Figuras.

Agradecimientos

El inmenso agradecimiento a ti divino Dios, pues nos dirigiste por el mejor camino de nuestras vidas, nos das salud y sabiduría para alcanzar nuestras metas. De igual manera a este prestigioso centro educativo que nos ha acogido y dado la oportunidad de superación. Nuestro agradecimiento y reconocimiento a los señores profesores que supieron impartir y compartir sus conocimientos, de manera especial al M.Sc Eduardo Santiago Molina por su colaboración en la dirección de este trabajo monográfico.

Los Autores

Dedicatoria

Primeramente a Dios por ser nuestra guía, a Jesús por ser nuestra inspiración, modelo y por ser el ejemplo más grande de amor en este mundo.

A nuestros padres que siempre nos dan su apoyo en todo momento para culminar con éxito este trabajo, ya que ellos siempre han estado presentes para apoyarnos moral, psicológica y económicamente, y por darnos el ejemplo de vida a seguir.

A nuestro profesor guía por darnos su apoyo y corrección con amor y desinterés para la el desarrollo de este trabajo y ofrecerles este trabajo a todos sin distinción de religión, raza, sexo, condición política y social. Respetamos la vida y fomentamos la oportunidad que tenemos de dar y aprender. Hacemos todo con las mejores intenciones, trabajando transparentemente con respeto y humildad, sin forzar a otros a creer en lo que creemos, ofreciéndolo de corazón.

Los Autores.

1. Introducción

Internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos, es decir información. Información que puede estar almacenada en las llamadas páginas o sitios web, que son accesibles a todas aquellas personas que tenga acceso a esta red de redes por cualquiera de los medios antes mencionados.

Los dispositivos routers se encargan de conectarse con algún servidor de acceso a Internet y distribuyen la señal para todos los ordenadores que estén conectados a la red local, por ejemplo: tu casa u oficina, ya sea por cable o Wireless (Wi-Fi, conexión inalámbrica).

La conexión a Internet a través de una red Wi-Fi, es hoy en día uno de los medios más utilizados para conectarse desde todo tipo de dispositivos, sustituyendo al clásico Ethernet debido a la ausencia de cables, algo que es ideal para acceder desde teléfonos móviles o portátiles, el inconveniente, es que al no necesitar cable, cualquiera que tenga la contraseña de una red Wi-Fi puede conectarse a la red local.

Otro inconveniente con la redes Wi-Fi es que al no estar presente un medio como el cable, que en cierto modo protege los datos, estos quedan un poco más expuestos ante la ausencia de este medio.

El monitorizar y analizar todo aquel tráfico de red que pase en alguna red, no podría ser tan sencillo sino se tienen los conocimientos necesarios y más aún si no se cuenta con las herramientas adecuadas que faciliten más aun el trabajo, con lo antes mencionado se podría conocer prácticamente cualquier cosa que ocurra en una red.

A continuación se presenta en la siguiente sección de este documento, algunos de los trabajo relacionados con la temática que se abordó para el desarrollo del presente trabajo; luego se presenta la problemática principal con la que se desarrolló este trabajo, así mismo se presentan los objetivos tanto general como específicos que se pretenden alcanzar al finalizar este trabajo monográfico, posteriormente se describen los conceptos teóricos necesario para tener un conocimiento más claro con respecto a los términos informáticos que se encuentran en el documento.

Luego se describen de forma detallada y explicativa el diseño y métodos utilizados para la realización de este trabajo así como los pasos a seguir para obtener los resultados a continuación mostrados. Como último se presentan los resultados obtenidos junto con las conclusiones y recomendaciones más convenientes para dicho trabajo monográfico.

2. Antecedentes

En esta sección se hace mención de los principales trabajos relacionados con el tema que se ha desarrollado en esta investigación.

En la Universidad Nacional Autónoma de México (UNAM), (Sánchez, 2012) se realizó un proyecto sobre Herramientas de Monitorización y análisis de usuarios en redes sociales. En él se citan herramientas específicamente orientadas a localizar perfiles de individuos o entidades, en redes sociales, para medir la actividad que estos realizaban (es decir el uso activo en cuanto a la publicación de contenido), se trataba de una monitorización no ya de los websites sino de usuarios en línea.

La mayoría de las herramientas realizaban un análisis de la actividad de un usuario/entidad, midiendo la intensidad y frecuencia de su actividad en esa red (por ejemplo el número de mensajes publicados). También el análisis de su influencia o impacto en línea, que recogen datos, también de la visibilidad de su perfil en la red para otros usuarios (número de seguidores, fans…).

Algunas de las herramientas utilizadas de los cuales se hace mención es MentionMap (que es una aplicación para twitter que permite crear un especie de mapa con forma de árbol, para conocer, y si hace falta analizar, las conexiones recientes entre los usuarios por medio de las menciones que han hecho o los hashtags que han usado en los tweets por ejemplo en los perfiles), entre otras más herramientas.

Por otra parte en la Escuela Politécnica Nacional, Ecuador, (Ríos & Fermin, 2009) realizaron un estudio sobre la red local de la Facultad de Electrónica y Eléctrica de la universidad antes mencionada, con el propósito de medir, a nivel de las capas dos y tres del modelo OSI, la cantidad de tráfico, la tasa de transferencia y el porcentaje de utilización de la red.

Para ello, se empleó el software comercial denominado TracerPlus Ethernet para estudiar el flujo de información generado por los sistemas administrativos y académicos existentes en la Facultad de Electrónica y Eléctrica de la universidad antes mencionada. Después de las mediciones efectuadas, se determinó que la red universitaria, bajo la infraestructura de ese momento, tenía un comportamiento dentro de los estándares recomendados.

Finalmente, Talia Odete Ledesma Quiñones, Lucy Coya Rey y Luis Alberto Marchal Alcántara, todos ingenieros en Telecomunicaciones, realizaron un trabajo titulado como: Herramientas de monitorización y análisis de tráfico de red. El trabajo consistió en citar las mejores herramientas para realizar análisis y monitoreo de una red, y hacer pruebas con ellas. En el trabajo se citan herramientas tanto de distribución libre como de pago, entre las mencionadas tenemos: Tcpdump, Wireshark, NetworkMiner, CommView, Kismet, OmniPeek, InSSiDer, etc.

3. Planteamiento del problema

Internet es la red más grande de información que existe, la cual es usada por las personas para buscar y compartir información. Y el acceso a esta red es cada vez más fácil, ya que hoy en día podemos encontrar una gran variedad de maneras de conectarnos a ésta; una de ella es mediante las redes inalámbricas, específicamente las redes Wi-Fi, que son en muchas ocasiones las más preferidas, probablemente, esto debido a que una gran variedad de dispositivos pueden conectarse a ellas, por ejemplo, dispositivos móviles tales como teléfonos inteligentes (Smartphone), tabletas (Tablet), computadoras portátiles (laptops) y además de que estas redes podemos encontrarlas en muchos lugares, por ejemplo parques, instituciones públicas, plazas, y en muchos otros sitios públicos.

Pero las redes Wi-Fi son en el mayor de los casos, redes con restricciones, es decir, poseen un mecanismo de autenticación y una contraseña cifrada con algunos de los algoritmos existentes según protocolo de autenticación, por lo que solo los dueños y aquellas personas que conozcan la contraseña pueden acceder y hacer uso de estas para conectarse a Internet.

Sin embargo, aunque es poco común, es posible encontrarse con redes Wi-Fi sin ninguna restricción de acceso, por lo que representa una tentación el deseo de conectarse para los potenciales usuarios. Si éstos llegaran a conectarse, sería interesante saber qué uso harían de la red con conexión a Internet. Por tal razón surgen las siguientes interrogantes:

- ¿Cuál es la respuesta de los usuarios al encontrarse con una red Wi-Fi sin autenticación y con acceso a internet?
- ¿Cuál es el uso que los usuarios hacen de este tipo de red?

4. Justificación

Este trabajo monográfico está enfocado sobre el análisis del tráfico capturado en un Punto de Acceso Inalámbrico (Access Point, AP), ejemplo de ello: ¿Cuáles son los dispositivos y sistemas operativos más empleados, así como las páginas web más visitadas por los usuarios de este AP?

Para lograr los objetivos planteados fue únicamente necesario instalar un AP de bajo costo y de fácil configuración, es decir, que en términos económicos este trabajo fue viable

Se puede decir que ha sido un trabajo innovador tomando en cuenta que el trabajo se realizó dentro de una red privada de una institución y la conexión a Internet que se brindó fue sin costo alguno para todos los usuarios; por tal razón no se le resta interés a este trabajo al querer tener conocimiento de la manera en que las personas utilizan las redes que les provea de Internet, además conociendo su respuesta al encontrarse con redes Wi-Fi desconocidas, y más aún si estas no poseen contraseña para su acceso, es decir, ¿Son capaces de conectarse o poner información delicada en riego de ser obtenida por otros?. Algo muy interesante, es que se puede tener conocimiento de cuáles fueron las páginas web a los que estos acceden, o bien la manera en para que usarían el Internet, hay muchas maneras de darle uso, por ejemplo el de descargar aplicaciones a través de un Smartphone o acceder a las tan usadas redes sociales.

También el Departamento de Computación, por medio de los resultados de este trabajo podría estimar qué número de estudiantes poseen computadoras portátiles o dispositivos móviles, de esa manera, sabría si es necesario reducir inventario de computo en los laboratorios, también si es necesario actualizar los equipos, debido a que no tiene sentido tener los equipos de cómputos si los estudiantes no hacen uso de ellos por el motivo de que estos poseen sus propios equipo.

Además, si se conoce el tiempo de ocio de los estudiantes que también poseen los equipos de cómputo, podría utilizarse la red de la institución para implementar computación grid (Grid Computing); así se podrían utilizar en tiempo ocioso de dichos recursos de cómputo para algún tipo de trabajo (como por ejemplo compartir recursos de los equipos para ayudar a encontrar la vacuna contra alguna enfermedad).

5. Objetivos

A continuación se presentan tanto el objetivo general de esta investigación, así como los objetivos específicos.

5.1. Objetivo General

- Analizar el tráfico de red generado, por todos aquellos dispositivos conectados a un punto de acceso inalámbrico (AP) sin autenticación, que provea acceso a Internet, para conocer qué uso dan de dicha Red.

5.2. Objetivos específicos

- Utilizar aplicaciones para el análisis del tráfico de red generado por los usuarios conectados al punto de acceso inalámbrico con servicio de Internet.
- Identificar los sitios web y aplicaciones web a los que comúnmente se dirigen y usan los usuarios conectados al AP.
- Identificar si los usuarios utilizan dispositivos móviles o computadoras portátiles al momento de conectarse al AP.
- Determinar el sistema operativo de los dispositivos móviles y de las computadoras portátiles usados por los usuarios al momento de conectarse al AP.
- Estimar el tiempo promedio en el que los usuarios generaron tráfico web durante su conexión con el AP.

6. Marco Teórico

Esta sección describe los fundamentos y conceptos teóricos para brindar un contexto referencial que ayude a comprender sin ambigüedad el trabajo que se ha realizado.

6.1. Tráfico de red

Tráfico es un concepto que tiene su origen en un vocablo italiano que se refiere al tránsito o desplazamiento de medios de transporte por algún tipo de camino o vía. El concepto de tráfico puede hacer mención tanto a la acción del movimiento como a las consecuencias de dicha circulación. (Porto & Merino, 2014).

Por tanto el tráfico de red se puede definir como la cantidad de información o datos enviados y recibidos por todas aquellos equipos de una red computadoras.

6.2. Tráfico web

En internet, el tráfico hace referencia a la cantidad de visitantes, visitantes únicos, hits, megabytes transferidos o cualquier otra forma de medida, que se produce en un servidor web o en sitios webs específicos en un determinado período de tiempo.

Existen múltiples formas de cuantificar (de cantidad) o cualificar (de calidad) el tráfico de un sitio web. Para cuantificar el tráfico se utilizan contadores, en donde el tráfico puede diferenciarse entre visitantes únicos, páginas vistas por cada usuario, hits, etc.

En tanto, la calidad del tráfico web puede estimarse con la información del contador, más estadísticas: procedencia del usuario, nivel adquisitivo, nivel de conocimientos, intereses de los visitantes, etc. (Alegsa, 2010).

El tráfico web es la cantidad de datos enviados y recibidos por los visitantes de un sitio web. Esta es una gran proporción del tráfico de Internet. El tráfico web es determinado por el número de visitantes y de páginas que visitan.

6.3. Definición de red de computadoras

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos (computadoras y/o dispositivos) conectados por algún medio de transporte de datos (cables, ondas, señales), que comparten información, recursos, y servicios (Internet). (Mansilla, 2016). Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos.

Normalmente se trata de transmitir datos, audio y video a través de diversos medios de transmisión.

6.3.1. Protocolo de red

El concepto de protocolo (Porto & Gardey, Definicion.de, 2013) de red se utiliza en el contexto de la informática para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos.

También conocido como protocolo de comunicación, el protocolo de red establece la semántica y la sintaxis del intercambio de información, algo que constituye un estándar. Las computadoras en red, de este modo, tienen que actuar de acuerdo a los parámetros y los criterios establecidos por el protocolo en cuestión para lograr comunicarse entre sí y para recuperar datos que, por algún motivo, no hayan llegado a destino.

En el protocolo de red se incluyen diversas informaciones que son imprescindibles para la conexión. El protocolo indica cómo se concreta la conexión física, establece la manera en que debe comenzar y terminar la comunicación, determina cómo actuar ante datos corrompidos, protege la información ante el ataque de intrusos, señala el eventual cierre de la transmisión, etc.

Existen protocolos de red en cada capa o nivel de la conexión. La capa inferior refiere a la conectividad física que permite el desarrollo de la red (con cables UTP, ondas de radio, etc.), mientras que la capa más avanzada está vinculada a las aplicaciones que utiliza el usuario de la computadora (con protocolos como HTTP, FTP, SMTP, POP y otros).

6.3.2. Estándares de redes

- IEEE 802.3, estándar para Ethernet.
- IEEE 802.5, estándar para Token Ring.
- IEEE 802.11, estándar para Wi-Fi.
- IEEE 802.15, estándar para Bluetooth.

6.4. Internet

Internet (Ramirez, 2016) es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominados TCP/IP, que ofrece diversos servicios a sus usuarios como pueden ser el correo electrónico, chat o la web. Todos los servicios que ofrece Internet son llevados a cabo por miles de ordenadores que están permanentemente encendidos y conectados a Internet, esperando que los usuarios les soliciten los servicios y sirviéndolos una vez son solicitados. Como decimos, hay servidores para todo, los hay que ofrecen correo electrónico, otros hacen posible nuestras conversaciones por chat, otros la transferencia de ficheros o la visita a las páginas web y así hasta completar la lista de servicios de Internet.

A menudo, un mismo servidor de Internet ofrece varios servicios distintos, es decir, un único ordenador puede ofrecer servicio de correo electrónico, transferencia de ficheros y servidor web.

6.5. ¿Qué es un Router?

Un router (Kioskena.net, 2015) es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes. Este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento. Es un dispositivo que opera en la capa 3 del modelo OSI y no debe ser confundido con un conmutador (capa 2). Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.

Los dispositivos Router se encargan de conectarse con el servidor de acceso a Internet y distribuye la señal para todos los ordenadores que estén conectados a la red local de tu casa u oficina, ya sea por cable o Wireless (Wi-Fi, conexión inalámbrica).

6.6. Redes Wi-Fi (802.11)

Wi-Fi (Falcón, WI-FI, Lo que se necesita conocer, 2010) es una comunicación inalámbrica porque se lleva a cabo sin el uso de cables de interconexión entre los participantes, por ejemplo, una comunicación con teléfono móvil es inalámbrico. No cabe duda de que la tecnología inalámbrica está ocupando rápidamente las preferencias de todo tipo de usuarios.

Desde hace pocos años, los ordenadores están también liberándose de sus ataduras. Cada vez son más los hogares, los cafés, las pequeñas empresas, los aeropuertos o las grandes compañías en los que se dispone de redes inalámbricas Wi-Fi.

Wi-Fi es una tecnología que permite que una gran variedad de equipos informáticos pueda interconectarse sin necesidad de utilizar cables.

Lo que hace que funcione Wi-Fi además de las configuraciones que permite es un equipo conocido como punto de acceso. En las redes pequeñas, el punto de acceso suele estar conectado junto al equipo de acceso a internet. Si la red es grande lo normal es que se encuentren en las partes altas de las paredes de las oficinas, en los salones de los hoteles, de las cafeterías, estaciones de autobús, tren o aeropuertos, etc.

Una de las principales ventajas de Wi-Fi es que utiliza el mismo protocolo que internet (protocolo TCP/IP). Este protocolo lo usan también las redes locales de cable, por lo que interconectar una red Wi-Fi con una red cableada es bastante simple.

Para que un equipo informático pueda comunicarse de forma inalámbrica, necesita disponer de un dispositivo que se conoce como adaptador de red, un adaptador de red es un equipo de radio con transmisor, receptor y antena. Wi-Fi es una tecnología asentada, lo que hace que disponga de una oferta amplia y a bajo precio.

Una red Wi-Fi cuenta con unos o más puntos de acceso a los que se conectan los terminales de la red gracias a que disponen del hardware (adaptador de red) y software (protocolo necesario). De forma general a los equipos que forman parte de una red

inalámbrica se les conoce como terminales, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de puntos de acceso.

Tanto a los terminales como punto de acceso se les conoce por el nombre general de estación.

Las estaciones se comunican entre sí gracias a que usan la misma tecnología de comunicación ósea usan la misma banda de frecuencias y tienen instalados el mismo conjunto de protocolos. Estos protocolos se componen de dos grupos: uno se ocupa de garantizar la comunicación inalámbrica entre las estaciones, mientras que el otro se ocupa del intercambio de información entre los terminales de esto se ocupan los protocolos TCP/IP.

Wi-Fi, Bluetooth y 3G son tecnologías completamente diferentes que no tienen nada que ver entre sí. Por ejemplo, un teléfono móvil puede utilizar Bluetooth para conectarse al manos libre del coche, utilizar Wi-Fi para conectarse a internet a través del ADSL de casa, y utilizar 3G para conectarse a internet cuando esta fuera del hogar.

La tecnología Bluetooth está pensada para conexiones de corta distancia (menos de 10 metros) Wi-Fi lo está para conexiones de carácter local (algunos cientos de metros) y las redes móviles para disponer de una cobertura global.

Las comunicaciones de Bluetooth se desarrollaron mediante el modelo maestro/esclavo. Un terminal maestro puede comunicarse hasta con 256 esclavos, aunque solo siete de estas comunicaciones pueden ser simultaneas.

Habitualmente, la tecnología Bluetooth la incorporan los terminales de los teléfonos móviles para comunicarse con las manos libres del coche, intercambiar información con otros terminales o comunicarse con el ordenador de casa.

En cuanto al 3G, se trata de una tecnología que les ofrece a los terminales móviles la posibilidad de transmitir datos a alta velocidad. Mientras que con los móviles tradicionales no se superan los 100 Kbps reales, (384 Kbps teóricos), con los terminales 3G se pretende alcanzar varios Mbps. Independientemente de que la realidad se aparte

mucho de la teoría, lo cierto es que se está trabajando para conseguir una red de cobertura global que permita ofrecer un servicio de acceso a internet a velocidades del orden de 100 Mbps para esto se habla del 4G.

Recientemente ha aparecido una nueva tecnología conocida como HSDPA (*High Speed Downlink Packet Access*, Accesos a paquetes de alta velocidad) que permite ofrecer unos anchos de banda en las redes 3G de hasta 14,4 Mbps (corresponde con 7,2 Mbps reales).

El usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden interconectarse sin problemas. Wi-Fi es un estándar de comunicación inalámbrica. Si un fabricante desea construir un dispositivo Wi-Fi, solo tendrá que seguir el estándar y listo.

Los estándares son regulados por los organismos de normalización. Aunque existen muchos organismos en el mundo, el más relevante en el caso de Wi-Fi es el IEEE (Instituto de ingenieros eléctricos y electrónicos).

6.7. Normas IEEE del estándar Wi-Fi

El estándar Wi-Fi (Falcón, WI-FI, lo que se necesita saber, 2010) está recogido en la norma IEEE 802.11b. Esta norma describe los detalles técnicos para establecer comunicaciones de datos de forma inalámbrica a una velocidad máxima de 11 Mbps. Por tanto, el estándar original de Wi-Fi solo permite transmitir datos a una velocidad máxima de 11 Mbps.

Por otro lado, la tecnología de comunicaciones inalámbrica ha seguido desarrollándose, lo que ha permitido que posteriormente apareciesen soluciones que permiten transmitir datos a velocidades superiores a 11 Mbps. Incluso se ha llegado a hablar de soluciones teóricas que alcanzan los 540 Mbps. Muchas de estas nuevas soluciones llegan a tener su propia norma IEEE. Las más interesantes son las siguientes:

- IEEE 802.11b (año 1999). Es la norma original que permite velocidades de transmisión de hasta 11 Mbps utilizando la banda de frecuencias de 2,4 GHz, a esta norma se le conoció también como 802.11 HR.

- IEEE 802.11ª (año 1999). Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de los 2,4 GHz, sino la de los 5 GHz.

- IEEE 802.11g (año 2003). Esta norma surgió con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2,4 GHz. Esta norma permite transmitir datos a 54 Mbps.

- IEEE 802.11n (año 2009). Se trata de un nuevo paso en el objetivo de conseguir velocidades cada vez mayores. Con esta norma se habla de velocidades de 300 Mbps y alcances mucho mayor que con las normas anteriores. Otras de las ventajas de 802.11n es que resulta ser compatible con todos los estándares anteriores (a, b y g).

La característica externa más destacable de 802.11n es que incorpora varias antenas para poder utilizar varios canales simultáneamente. Si dispone de un punto de acceso compatible con 802.11g y desea establecer una comunicación a 54 Mbps, asegúrese de que el resto de terminales de su red son también compatibles con 802.11g y no se limite a fijarse en la velocidad.

La tecnología Wi-Fi define una forma de intercambiar datos entre dos equipos utilizando ondas de radio. Esto es lo que se conoce como utilización del medio radioeléctrico. La tecnología básica en la que se fundamenta el funcionamiento de estos sistemas inalámbricos es el sistema conocido como espectro expandido.

Este sistema tiene la particularidad de ser muy resistente a las interferencias de otras fuentes de radio y a los efectos del eco, lo que le permite coexistir con otros sistemas de radiofrecuencia sin verse afectado fuertemente. Estas ventajas hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia en las que funciona Wi-Fi.

6.7.1. ¿Por qué instalar una red Wi-Fi?

(Falcón, WI-FI, lo que se necesita saber, 2010) Se habla de red de ordenadores o equipos informáticos, cuando varios de estos equipos están interconectados entre sí. Las grandes ventajas de poder contar con equipos interconectado son:

- Permite compartir los servicios de comunicaciones, fundamentalmente el acceso a internet (mediante ADSL, modem cable, RDSI, etc.).
- Permite compartir periféricos: impresoras, escáneres, discos duros en red, cámaras, etc.
- Permite compartir la información contenida en cada ordenador.
- Permite compartir aplicaciones.

Se habla de distintos tipos de redes dependiendo de la extensión de la misma. Las redes locales son las que cubren el entorno de un edificio, mientras que las redes metropolitanas, redes de área extensa o global, cubren un entorno mayor: una ciudad, un país o un entorno multinacional.

La tecnología Wi-Fi puede utilizarse realmente para cualquier tipo de red, se trata de poner simplemente más o menos puntos de acceso; no obstante, suele utilizarse principalmente para las redes de tipo local.

En el mercado existen dos tipos de redes locales: la que se forma con el uso de cables y la de tipo inalámbrico o redes WI-Fi. Tanto las redes cableadas como las inalámbricas hacen exactamente el mismo trabajo: interconectan ordenadores y otros dispositivos informáticos (impresoras, modem, etc.) para permitirles compartir recursos.

Principales ventajas que ofrecen las redes Wi-Fi frente a las redes cableadas:

- Movilidad: la libertad de movimientos es uno de los beneficios más evidentes de las redes Wi-Fi. Un ordenador o cualquier otro dispositivo, puede situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio.

- Desplazamiento: con un ordenador portátil o PDA no solo se puede acceder a internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación.

- Flexibilidad: las redes Wi-Fi también nos permiten colocar un ordenador de sobre mesa en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. El nivel de seguridad de las redes Wi-Fi es similar al de las redes cableadas.

- Ahorro de costes: Diseñar e instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias, la instalación de una red Wi-Fi permite ahorrar coste al permitir compartir recursos.

- Escalabilidad: se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar un nuevo ordenador cuando se dispone de una red Wi-Fi es algo tan sencillo como hacer un par de clics.

6.8. Sistema Operativo

(Masadelante.com, 2016) Un sistema operativo es el programa (o software) más importante de un ordenador. Para que funcionen los programas, cada ordenador de uso general debe tener un sistema operativo. Los sistemas operativos realizan tareas básicas, tales como reconocimiento de la conexión del teclado, enviar la información a la pantalla, no perder de vista archivos y directorios en el disco, y controlar los dispositivos periféricos tales como impresoras, escáner, etc.

6.8.1. Sistemas Linux

(Debian.org, 2015) Linux está modelado como un sistema operativo tipo Unix. Desde sus comienzos, linux se diseñó para que fuera un sistema multi-tarea y multi-usuario. Estos hechos son suficientes para diferenciar a Linux de otros sistemas operativos más conocidos. Sin embargo, Linux es más diferente de lo que pueda imaginar. Nadie es dueño de Linux, a diferencia de otros sistemas operativos. Gran parte de su desarrollo lo realizan voluntarios de forma altruista. En un sistema GNU/Linux, Linux es el núcleo. El resto del sistema consiste en otros programas, muchos de los cuales fueron escritos por o para el proyecto GNU. Dado que el núcleo de Linux en sí mismo no forma un sistema operativo funcional, preferimos utilizar el término “GNU/Linux” para referirnos a los sistemas que la mayor parte de las personas llaman de manera informal “Linux”.

Entre sistemas operativos basados en Linux más usados y conocidos tenemos: Ubuntu, CentOs, Debian, Fedora, OpenSUSE, etc. Y para dispositivos móviles (Smartphone) Android.

6.8.2. Sistemas Windows

Windows es una familia de sistemas operativos producidos por Microsoft, es decir que es un sistema de pago. El núcleo del sistema se encuentra entre HAL y el Executive y proporciona sincronización multiprocesador, hilos y envió y planificación de interrupciones y envió de excepciones, también es el responsable de la inicialización de controladores de dispositivos que son necesarios en el arranque.

La familia de sistemas operativos Windows NT está construida para versiones como Windows 10, 8.x, 7, Vista, XP, 2000, Windows Server 2003 y NT (todos tienen multitarea apropiativa y pueden trabajar en ordenadores de un solo procesador). (Porto & Merino, Definicion.de, 2010).

Versiones de Windows y su NT versión.

Windows NT 3.1	Workstation, Advanced Server
Windows NT 3.5	Workstation, Server
Windows NT 3.51	Workstation, Server
Windows NT 4.0	Workstation, Server Enterprise Edition
Windows NT 5.0	Windows 2000
Windows NT 5.1	Windows XP.
Windows NT 5.2	Windows Sever 2003
Windows NT 6.0	Windows Vista y server 2008.
Windows NT 6.1	Windows 7 (y sus versiones)
Windows NT 6.2	Windows 8, Pro, RT, Windows Phone 8
Windows NT 6.3	Windows 8.1, Pro, RT, Windows Phone 8.1
Windows NT 10	Windows 10 (y sus versiones)

6.9. Usert-Agent

(Wikipedia, 2015) Un Usert-Agent ó agente de usuario es una aplicación informática que funciona como cliente en un protocolo de red; el nombre se aplica generalmente para referirse a aquellas aplicaciones que acceden a la World Wide Web. Los agentes de usuario que se conectan a la Web pueden ser desde navegadores web hasta los web crawler de los buscadores, pasando por teléfonos móviles, lectores de pantalla y navegadores en Braille usados por personas con discapacidades.

Cuando un usuario accede a una página web, la aplicación generalmente envía una cadena de texto que identifica al agente de usuario ante el servidor. Este texto forma parte del pedido a través de HTTP, llevando como prefijo User-agent: o User-Agent: y generalmente incluye información como el nombre de la aplicación, la versión, el sistema operativo, y el idioma. Los bots, como los web crawlers, a veces incluyen también una URL o una dirección de correo electrónico para que el administrador del sitio web pueda contactarse con el operador del mismo.

6.10. DD-WRT

(dd-wrt.com, 2010) DD-WRT es un firmware no-oficial para dispositivos Linksys WRT54g/GS/GL y muchos otros dispositivos router 802.11g basados en un diseño de referencia similar o igual al Broadcom. Ejecuta un reducido sistema operativo basado en Linux; todos los routers con los que se tiene compatibilidad se puede ver en la página oficial.

Todos estos routers soportados están diseñados para utilizar Linux firmware oficial y su código fuente está disponible bajo licencia GPL.

El firmware lo desarrolla BrainSlayer y su página oficial es dd-wrt.com. Las primeras versiones de DD-WRT se basaron en el firmware “Alchemy” de Sveasoft Inc, que a su vez se basa en el firmware original GPL de Linksys y en otros proyectos. DD-WRT se creó debido a que Sveasoft comenzó a cobrar por descargar su software.

6.10.1. Características de DD-WRT

- Está disponible en 13 idiomas.
- 802.11x (Encapsulación sobre LANs)
- Restricción de acceso.
- Modo Adhoc.
- Modo aislamiento de cliente.
- Modo cliente WPA.
- Servidor DHCP, DNS forwarder.
- Zona desmilitarizada (DMZ).
- Portal Hotspot.
- Etc.

6.11. Sniffer

(Untiveros, 2010) Un "Sniffer" (Sniff: olfatear, rastrear) o "analizador de paquetes". Un Sniffer es un software que se encarga de capturar paquetes en tránsito (entrada y salida) en una cierta red y analizarlos. En otras palabras, es un programa que puede mirar la información en tránsito en una red y obtener información de esta. Está hecho para recibir información que no está destinada para él, lo que es muy útil, pero a la vez un gran peligro.

Están disponibles para varias plataformas, tanto en las variaciones comerciales como en código abierto. Algunos de los paquetes más simples son muy fáciles de implementar en C o Perl, utilizando una interfaz de línea de comandos y descargando los datos capturados a la pantalla.

Los proyectos más complejos utilizan una interfaz gráfica de usuario. Las estadísticas de tráfico de gráficos, realizan un seguimiento de varias sesiones y ofrecen varias opciones de configuración.

Los sniffers de red son también los motores para otros programas. Los llamados "Sistemas de Detección de Intrusos" (IDS) utilizan sniffers para localizar paquetes que coincidan con las reglas designadas para marcar algo como malicioso o extraño. La utilización de la red y los programas de vigilancia a menudo los utilizan para recoger los datos necesarios para mediciones y análisis. Las fuerzas de seguridad que necesitan controlar los correos electrónicos durante sus investigaciones, probablemente emplean un sniffer diseñado para capturar tráficos muy específicos. Sabiendo ya que los sniffers simplemente se apoderan de datos de la red, veremos a continuación cómo funcionan.

6.11.1. Funcionamiento de un sniffer.

(Untiveros, 2010) Estos tipos de programas (sniffer) le ordena al computador, específicamente a su tarjeta de red, que deje de ignorar a todo el tráfico dirigido a otros equipos y preste atención a ellos. Para esto, la tarjeta de red se coloca en un estado conocido como "modo promiscuo", el cual no descarta los paquetes que no son para su dirección MAC, sino que los almacena y lee.

Una vez que esto sucede, una máquina puede ver todos los datos transmitidos en ese segmento de red. El programa entonces comienza una lectura constante de toda la información que entra en el PC, a través de la tarjeta de red.

Los datos que viajan por la red se presentan como paquetes o ráfagas de bits con formato para protocolos específicos. Debido a este formato estricto, un sniffer puede filtrar las capas de encapsulación y decodificar la información pertinente almacenada en el equipo de origen, equipo de destino, número previsto de puerto, capacidad de carga y, en pocas palabras, en cada pieza de información que se intercambia entre dos equipos.

6.12. Tcpdump

(Tcpdump.org, 2015) Tcpdump es una herramienta de línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

6.12.1. Descripción de uso tcpdump

Este imprime los contenidos de los paquetes que pasan a través de una interfaz de red que coincide con su expresión booleana; la descripción de los paquetes está precedida por un cierto tiempo, impreso, por defecto, como horas, minutos, segundos.

También se puede ejecutar con la opción –w como bandera, esto para guardar los datos de paquetes en un archivo para su posterior análisis. Entre las plataformas que soportan la señal SIGINFO, como la mayoría BSD (incluyendo Mac OS X) y Digital/True64 UNIX.

6.12.2. Algunas de las opciones para usar tcpdump

-LA: Imprimir cada paquete (menos su cabecera del nivel de enlace) en ASCII. Útil para capturar páginas web.
-b: Imprime el número AS en paquetes BGP en ASDOT notación en lugar de la notación asplain.
-c count: este para salir después de recibir cierto número de paquetes.
-d: Volcar el código de paquete de coincidencia compilado en una forma legible por humanos en la salida estándar y la parada.
-dd: Volcado de código de paquete de coincidencia como C fragmento de programa.
-DDD: Volcado de código de paquete de coincidencia como números decimales (precedido con un recuento).

-D: Imprimir la lista de las interfaces de red disponibles en el sistema y en la que tcpdump puede capturar paquetes.
-e: Imprimir la cabecera a nivel de enlace en cada línea de descarga. Esto se puede utilizar, por ejemplo, para imprimir direcciones de capa MAC para protocolos como Ethernet y IEEE 802.11.
-F Archivo: utiliza el archivo como entrada para la expresión de filtro. Una expresión adicional dada en la línea de comando se ignora.
-H: Intentar detectar encabezados proyecto malla 802.11s.
-i interfaz: se le indica la interfaz de nuestro ordenador, por el cual se desea capturar los paquetes.
-m módulo: Cargar definiciones del módulo MIB SMI del archivo de módulo. Esta opción se puede usar varias veces para cargar varios módulos MIB en tcpdump.

6.13. Wireshark

(Seguridad y Redes, 2008) Anteriormente conocido como Ethereal, es uno de los analizadores de protocolos más empleado. Captura los paquetes que circulan por la red y muestra el contenido de cada campo con el mayor nivel de detalle posible. Puede capturar paquetes en redes con diferentes tipos de medios físicos, incluyendo las WLAN. Funciona tanto en modo consola como mediante una interfaz gráfica y contiene muchas opciones de organización y filtrado de información. Permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con otros protocolos de la capa de enlace) estableciendo la configuración en modo promiscuo.

Sus estadísticas y funciones gráficas son muy útiles, pues identifica los paquetes mediante el uso de colores. Además, examina datos de una red “en caliente” o de un archivo de captura salvado en disco. Incluye un lenguaje completo para la elaboración de filtros, la capacidad de mostrar el flujo reconstruido de una sesión de TCP y la reproducción de conversaciones VoIP.

Wireshark se desarrolla bajo licencia pública general (GNU General Public License) y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac Os X, así como en Microsoft Windows. Hace uso tanto de la librería Libpcap como de Winpcap para Linux y Windows respectivamente, siendo provistas junto con el instalador.

Carga datos almacenados en un archivo .pcap de una captura previa o de otros tipos de capturas entre las que se destacan los formatos: .cap, .pcapng y .ncf de otras herramientas como Commview.

Para la opción de reconstrucción de sesiones, Wireshark realiza el filtrado automático de aquellos paquetes pertenecientes a la sesión en cuestión, mediante la opción Follow TCP Stream. El programa brinda la posibilidad de guardar la información reconstruida en diferentes formatos (ASCII, EBCDIC, HexDump, C Arrays y Raw). Este procedimiento para la reconstrucción de sesiones es más trabajoso en comparación con otras herramientas como el NetworkMiner, pues requiere mayores conocimientos por parte de los usuarios.

6.14. NetworkMiner

(Yashiroevil's Blog, 2010) Es una herramienta que entra en la categoría de análisis forense de redes y que corre en plataformas Windows, aunque con el empleo de Mono, puede igualmente hacerlo en distribuciones de Linux. Su propósito es recopilar información sobre los hosts en lugar de recoger información concerniente al tráfico de la red.

Utilizada tanto en redes cableadas como en inalámbricas, permite ser usada como sniffer pasivo y analizar capturas en formato pcap. Emplea la biblioteca de captura de paquetes estándar Winpcap, que debe estar instalada en la computadora para su funcionamiento. La vista de la interfaz de usuario principal está centrada en el host (ver Figura 4 anexo 3).

Hosts es la principal pestaña de la interfaz gráfica. En ella, NetworkMiner muestra los equipos detectados usando un árbol jerárquico desplegable, observándose todas las direcciones IP involucradas con la red de comunicaciones, al mismo tiempo que muchos otros detalles: dirección MAC, nombre del host, sistema operativo, TTL (time to live), y cuánto tráfico ha sido enviado hacia y desde la dirección. La identificación del sistema operativo puede realizarse apoyándose en las bases de datos Satori, p0f y Ettercap.

Se ofrecen muchos otros detalles como información de las sesiones de comunicación y del tráfico de DNS (Domain Name Service).

Además, la pestaña Cleartext muestra las cadenas de texto plano encontradas en la carga útil de cualquier paquete TCP o UDP (User Datagram Protocol). La pestaña de Credentials puede capturar los detalles de registro de entrada, por ejemplo vía cookies HTTP (Hypertext Transfer Protocol) y las credenciales de usuario (nombres de usuario y contraseñas).

En la pestaña Images se muestran las imágenes en miniatura que han sido extraídas del tráfico de la red. La pestaña Files permite reconstruir archivos tanto descargados como subidos a sitios web a través de los protocolos de extracción de archivos: FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), HTTP y SMB (Server Message Block).

7. Diseño Metodológico

La propuesta metodológica del presente trabajo, se basa en el estudio del comportamiento que presenta un determinado grupo de personas ante la utilización de un AP que les provea acceso a Internet sin límite de tiempo, sin la necesidad de autenticarse ante el AP, al mismo tiempo en que se provee este servicio, utilizar herramientas de monitoreo de redes que hará más fácil el manejo de la información relevante que se obtuvo y conocer el nivel de confianza que presentan las personas ante este punto de acceso y el ¿Para qué es utilizado?

El tipo de investigación que se realizó en este trabajo monográfico fue de campo o de terreno ya que se interactúo directamente con la información recolectada en el lugar en que se colocó el punto de acceso a medida que se realizó una observación detenida y minuciosa de los datos recolectados, también presenta un enfoque descriptivo ya que los resultados se estudiaron tal y como se obtuvieron en el presente al momento de realizarse el estudio.

Se tomó como población a los estudiantes y/o personas de dicha institución que se conectaron con el AP que se instaló en el Departamento de Computación de la Facultad de Ciencias y Tecnología de la UNAN-León; se tomó una muestra selectiva de la población ya que los usuarios fueron seleccionados, de manera que una vez conociendo el tamaño de la población, fue necesario emplear la ecuación:

$$\mathbf{h = N / [P^2(N-1)+1]}$$

Donde:

h= Es la muestra.

N= Es el número de sujetos que constituyen la población.

P= Es la probabilidad de error de la muestra que fija el investigador (0.05 es lo ideal).

Ya que ante la utilización de herramientas de monitoreo de red se obtuvo información sobre el fenómeno a investigar, se llevó a cabo la utilización de un método de análisis o analítico que nos permitió distinguir cada uno de los elementos de un fenómeno producido y observarlos de manera separada y ordenadamente al momento de entrar en contacto directamente con la información obtenida.

La utilización de técnicas de investigación juega un papel muy importante en el proceso de investigación ya que el propósito de estas es:

1) Ordenar las etapas de la investigación.
2) Aportar instrumentos para manejar la información.
3) Llevar un control de los datos.
4) Orientar la obtención de conocimientos.

Los instrumentos que se utilizaron en el proceso de investigación para recolectar la información, la muestra seleccionada y poder resolver el problema de la investigación están definidos de la siguiente, manera:

Se utilizó un dispositivo (Router) marca Linksys modelo wrt610n V1 (ver Figura 2 anexo 2) para configurar el AP.

Para recolectar la información requerida y especificada se utilizó un firmware basado en Linux, de los cuales se podía escoger entre dos opciones (OpenWRT & DD-WRT), en ese caso se optó por el segundo (DD-WRT, ver Figura 3 en anexo 2).

El firmware se configuró debidamente en la interfaz gráfica que este muestra según el propósito de uso, en este caso el cual es la recolección de datos, esto lo hizo por medio de un archivo script (ver a continuación).

```
#!/bin/sh
killall tcpdump
cd /mnt/disc0_part4/
var1=$(date +%H-%M)
mkdir $var1
cd $var1
tcpdump -i any "net 192.168.158.0/24" -w captura
```

Script.sh

Este archivo script realiza lo siguiente:

- El script termina con cualquier proceso Tcpdump que este en ejecución, esto para evitar que se sobrescriba información en un mismo archivo.
- El proceso implicaba moverse al directorio donde se encontraba montado el dispositivo USB.
- El script creaba una carpeta con la hora que marcaba el router al momento de crearse la carpeta y se movía a esa carpeta.
- Una vez estando dentro de la carpeta creada se ejecutaba un proceso Tcpdump, capturando la información de tráfico de red que circulaba en ese momento en todas las interfaces del dispositivo router, generada por los hosts pertenecientes a la dirección IP de la red 192.168.158.0/24 y se guardaba en un archivo llamado captura.

Este proceso que realizaba el archivo script se repetía cada 15 minutos, tiempo que fue configurado en el cron del router, esto para evitar capturas muy pesadas, ya que al ser las capturas de gran tamaño se dificultaba al momento de cargarlas en las aplicaciones (posteriormente a mencionar) a utilizarse para su análisis. Este procedimiento no elimino ninguna captura guardada antes de volverse a repetir su ejecución.

Para realizar la conexión del dispositivo (Router) hasta la red principal que proporcionó el Internet fue necesaria la utilización de un cable de red que estuvo conectado a un puerto Ethernet suministrado por la división de informática ubicado en el laboratorio de Hardware del edificio CIDS.

Se utilizó una fuente de poder (cable conector) para alimentar de energía al dispositivo que servirá de AP.

Para el análisis de los datos capturados se utilizó la herramienta de análisis Wireshark y la herramienta de aplicación NetworkMiner, el primero una herramienta muy conocida para el análisis de tráfico, el segundo una herramienta desarrollada para plataformas Windows que también puede ser emulada en otras plataformas, esta es una herramienta para realizar un análisis forense de datos tanto de manera activa como pasiva.

También se utilizó una memoria USB que estuvo conectada al dispositivo (Router) para guardar los datos que sean capturados en ella.

La recolección de datos se realizó en días comprendido entre las fechas del 5 al 23 de octubre del año 2015, específicamente de lunes a viernes, a partir de las 8:00 am a 2:00 pm. Además, el nombre de la red Wi-Fi proporcionada, era modificado continuamente, específicamente los días lunes y miércoles de cada semana; esto para poder descubrir si las personas se conectaba a las nuevas redes.

Los datos numéricos obtenidos serán presentados a través de gráficos de manera que sea fácil de entender.

7.1. Obteniendo la cantidad de usuarios conectados

Para obtener la cantidad de usuarios conectados, fue necesario utilizar la herramienta Wireshark, debido a que esta aplicación permite el análisis pasivo de capturas salvadas en disco. Fue necesario cargar los archivos de capturas de tráfico de red en la aplicación y al finalizar las cargas de los archivos, la aplicación muestra información de tráfico de red y a continuación se inició el proceso de identificar a los usuarios que se conectaron con el AP, esto a través de la dirección IP asignada al dispositivo utilizado y su dirección MAC, pero por defecto la aplicación Wireshark no muestra información correspondiente a la direcciones MAC, por lo que se modificó la información desplegada por la aplicación, esto, agregándole una nueva columna de información para que en esta nueva columna de se muestren las direcciones MAC de origen involucradas en el tráfico de red.

Al finalizar el proceso explicado anteriormente y obtenido la información deseada, se exportaron esos datos que nos muestra la aplicación Wireshark en un archivo con extensión ".csv", esto para poder cargar esa información en una hoja de cálculo de Excel y utilizar las características de manejo y observación de datos de esta aplicación, para obtener la cantidad de usuarios conectados. Ver Figura 8 en anexo 5 y Figura 12 en anexo 6.

7.2. Obteniendo el Sistema Operativo y los tipos de dispositivos usados

Para saber cuáles fueron los sistemas operativos que ejecutan los dispositivos de los usuarios, se utilizó la herramienta NetworkMiner. En la aplicación son cargados los archivos con la información de tráfico de red y al finalizar las cargas de estos archivos, la aplicación despliega en su interfaz, información con la direcciones IP de todos los hosts involucrados en el tráfico de red, se identificó a los hosts de los usuarios por medio de su dirección IP, y una vez identificados se observó la información detallada de cada host la cual es capaz de mostrar la aplicación.

Entre los datos capaces de mostrar la aplicación se encuentra el User-Agent o agente de usuario de los navegadores que fueron usados para navegar en Internet.

Cada modelo de navegador posee una serie de caracteres que indican varias características técnicas suyas y del equipo donde funciona y al realizar la petición de una página web, envía dicho agente de usuario para asegurarse que el servidor entregue la página en el formato adecuado. Y entre las características que envían los User-Agent está el sistema operativo del equipo, así como el tipo del dispositivo, por lo que al interpretar correctamente un User-Agent, es posible obtener toda esa información.

Ejemplo 1: En el siguiente User-Agent se identifica a un ordenador que ejecuta un S.O Windows 10, que usa un navegador Chrome versión 47.0.0.11536. Ver Figura 5 en anexo 3.

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,like Gecko)
Chrome/47.0.0.11536 Safari/537.36
```

Ejemplo 2: En el siguiente User-Agent se identifica a un dispositivo móvil que corre un S.O Android 4.2.1, que uso un navegador ucbrowser versión 10.7.6.805. Ver Figura 6 en anexo 3.

```
Mozilla/5.0 (Linux; U; Android 4.2.1; es-LA; HUAWEI_G610-U15 Build/HuaweiG610-U15)
AppleWebKit/528.5+ (KHTML, like Gecko) Version/3.1.2 Mobile Safari/525.20.1
UCBrowser/10.7.6.805 Mobile
```

7.3. Obteniendo la cantidad de tiempo que los usuarios generaron tráfico web.

Este proceso se realizó en conjunto con el apartado 7.1 en el que se explica cómo obtener la cantidad de usuarios conectados con el AP, ya que se utilizó igualmente la aplicación Wireshark, en esta aplicación se ejecutó el filtro "http || tcp.port==443". Lo anterior hace que Wireshark muestre los paquetes con información sobre las peticiones de acceso a sitios webs seguros (indicados con tcp.port==443) y sitios webs no seguros (indicado con http), esta información al igual que en el apartado 7.1 fueron exportados en un archivo con extensión ".csv" para posterior análisis la información con Excel.

Entre la información que muestra Wireshark está:

1) En número de paquetes mostrados.
2) Tiempo en que se generó un paquete.
3) La dirección IP origen.
4) Dirección Mac Origen, agregada manualmente en la sección 7.1.
5) Información sobre el paquete mostrado.

Luego de ejecutar el filtro en la aplicación y haberlo exportado, se realizó con Excel el proceso para calcular cuánto tiempo un usuario generó trafico web, esto al hacer una diferencia entre el tiempo en el que se generó el primer y último paquete. Ver Figura 9 en anexo 5.

7.4. Obteniendo la información del tráfico web

Para obtener información sobre cuáles fueron los sitios web a los que los usuarios se dirigían, fue necesario utilizar principalmente la aplicación Wireshark, para lograr obtener los sitios fue necesario emplear el filtro DNS luego de cargar los datos (Wireshark), este muestra la información correspondiente a las resoluciones DNS que realizaron los usuarios al hacer una petición a un sitio web.

Al igual que en la sección 7.1 y 7.3 se empleó el mismo proceso de análisis, al exportar la información en archivos con extensión ".csv" para poder cargarlas con Excel y con esta misma obtener los datos estadísticos. Ver Figura 10 y Figura 11 en anexo 5.

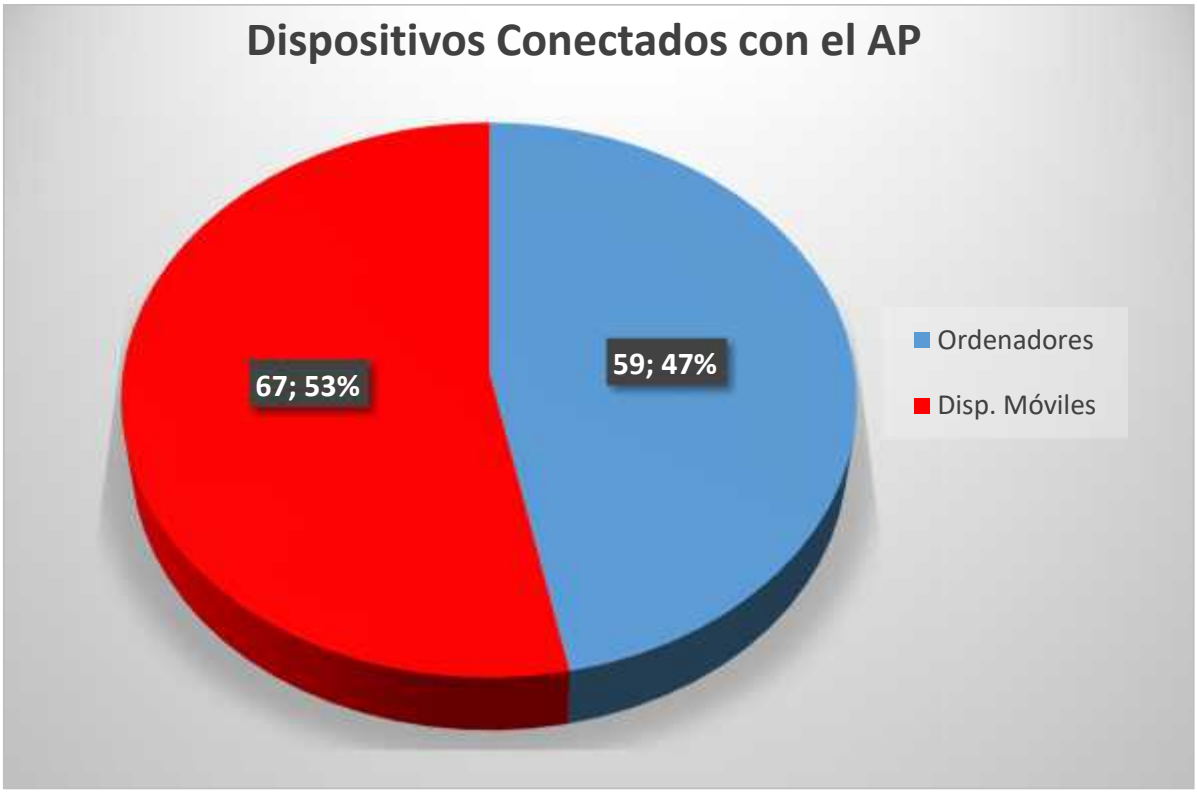
8. Análisis y Resultados.

En el siguiente apartado se muestran los resultados obtenidos en esta investigación, empezando por el total de dispositivos que se conectaron a la red proveída durante la práctica de esta investigación, seguido por sistemas operativos que esos dispositivos ejecutaban, luego los sitios y/o aplicaciones web a los que los usuarios accedían, y por último el tiempo que un usuario generó tráfico web.

8.1. Total de Dispositivos que se conectaron al AP.

Se obtuvo que la población total de dispositivos que se conectaron con el punto de acceso fue de 184, del cual se obtuvo como muestra a 126 dispositivos, que representan el 68% de la población, esta operación para obtener la muestra puede verse en la Figura 7 en anexos 4 de la sección de anexos. A continuación se observa en el gráfico n° 1 a la muestra de la cantidad de dispositivos móviles y computadoras u ordenadores.

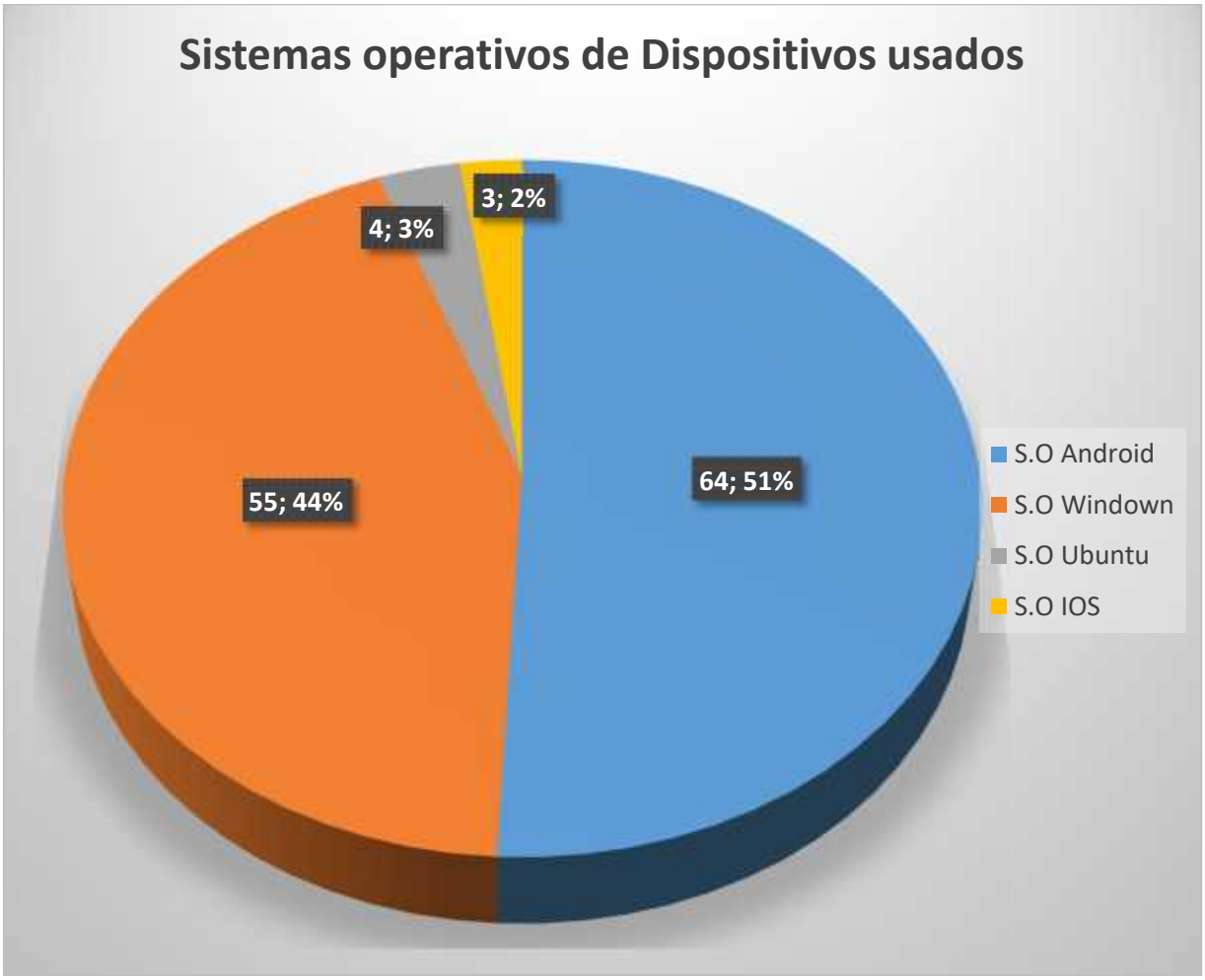
Gráfico N° 1: Total Dispositivos con conectados al AP.



8.2. Sistemas Operativos de los dispositivos usados.

En este apartado se exponen los resultados que se obtuvieron respecto a los sistemas operativos que ejecutan los dispositivos utilizados por los usuarios para acceder a la red durante el período establecido, lo cual se puede observar en el gráfico n° 2:

Gráfico N° 2: Sistemas Operativos de los Dispositivos.



8.2.1. Dispositivos con Sistemas Windows.

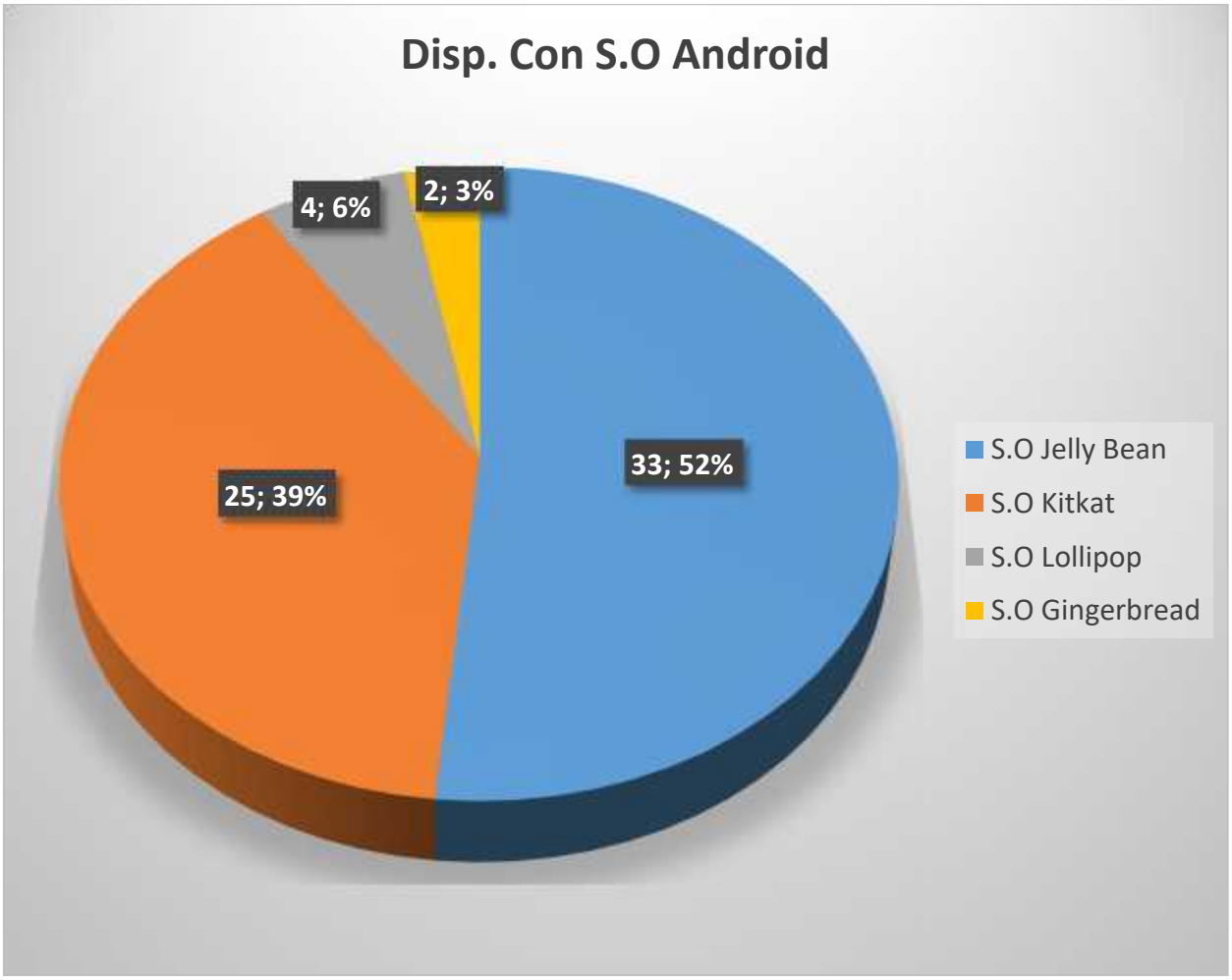
En este apartado se exponen los resultados que se obtuvieron respecto a las distribuciones de sistemas operativos Windows que ejecutan los dispositivos utilizados por los usuarios para acceder a la red durante el período establecido; obteniendo un total de 7 dispositivos con sistema operativo Windows 10; 26 dispositivos con sistema operativo Windows 8.1; 10 dispositivos con sistema operativo Windows 8; 12 dispositivos con sistema operativo Windows 7; siendo un total de 55 equipos con este tipo se S.O y obteniendo como resultado que los dispositivos con sistema operativo Windows 8.1 fue mayor, esto se puede observar en el gráfico n° 3 que se muestra a continuación:

Gráfico N° 3: Sistemas Windows.

8.2.2. Dispositivos con Sistemas Android.

En este apartado se exponen los resultados que se obtuvieron respecto a las distribuciones de sistemas operativos Android que ejecutan los dispositivos utilizados por los usuarios para acceder a la red durante el período establecido; obteniendo un total de 2 dispositivo con sistema operativo Android Gingerbread; 4 dispositivos con sistema operativo Android Lollipop; 25 dispositivos con sistema Android Kitkat; 33 dispositivos con sistema Android Jelly Bean; siendo un total de 64 equipos con este tipo de S.O y obteniendo que los dispositivos con sistema operativo Android Jelly Bean predominó sobre el resto. Esto se puede observar en el gráfico n° 4 que se muestra a continuación:

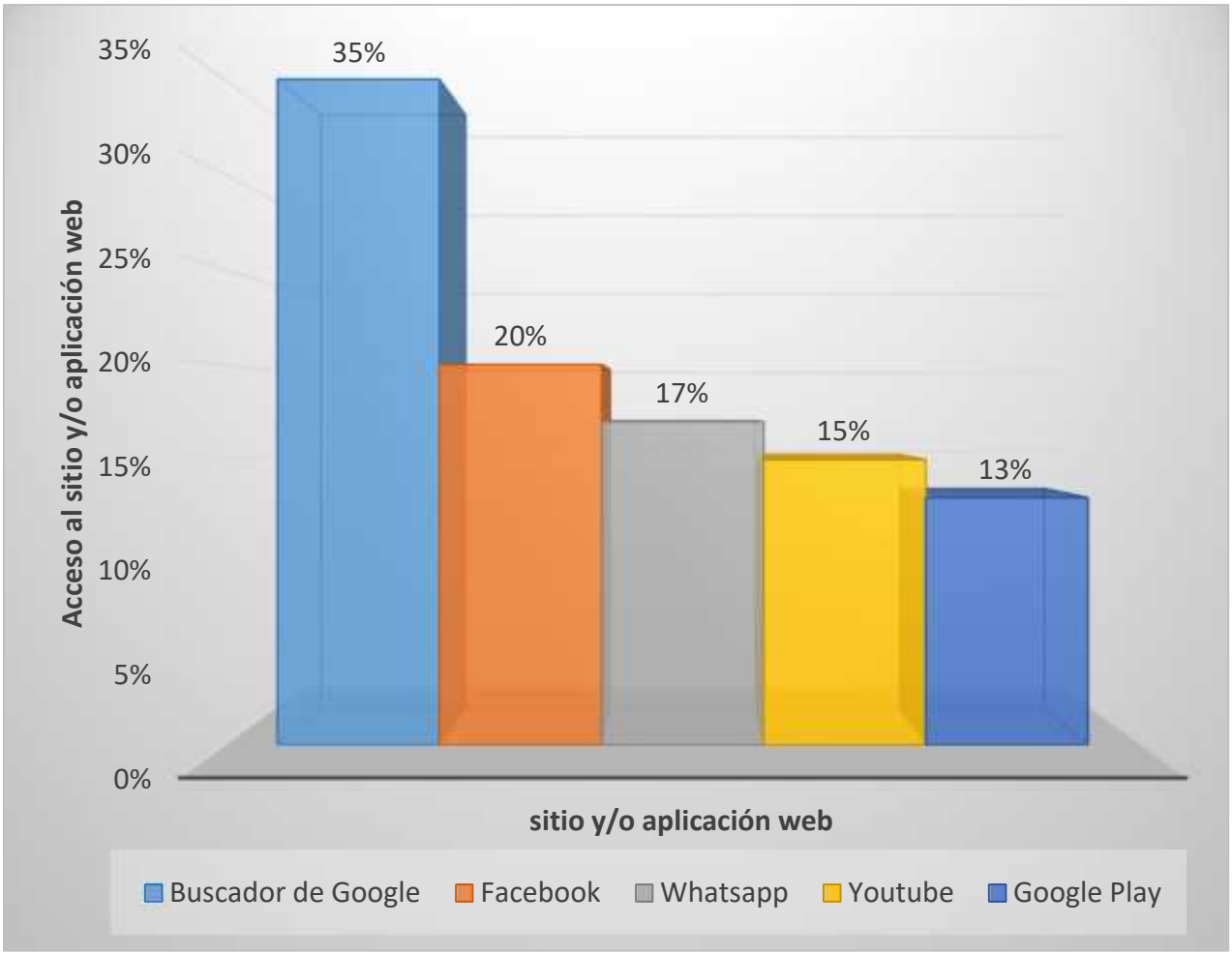
Gráfico N° 4: Sistemas Android.



8.3. Sitios y Aplicaciones web más utilizados.

En este apartado se muestran los cinco primeros puestos obtenidos de acuerdo con los sitios y aplicaciones web que fueron más accedidos por los usuarios que dieron uso al AP; obteniendo como resultado que el buscador de Google fue el sitio web en primer lugar de accesos y Google Play obtuvo el quinto lugar en número de accesos.

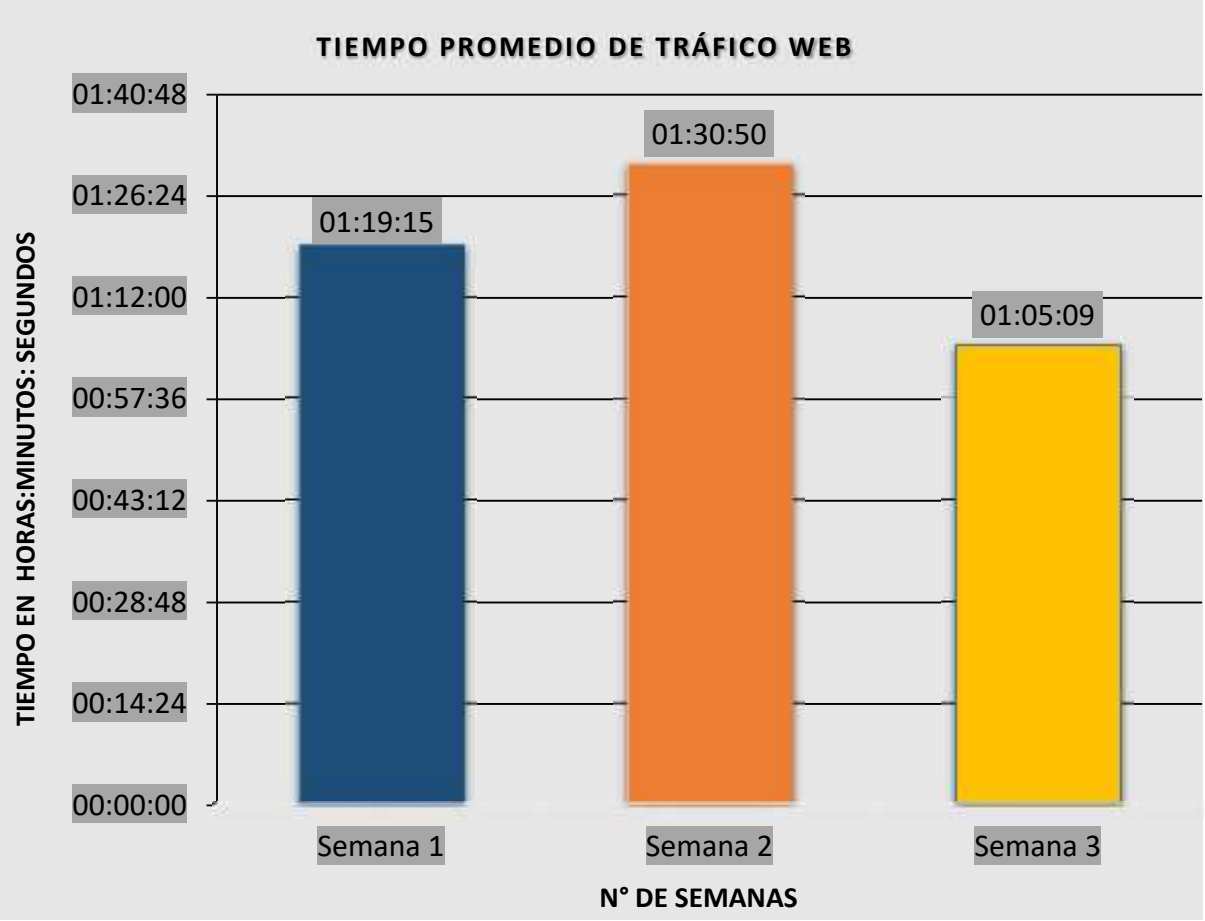
Gráfico N° 5: Páginas Web Visitadas.



8.4. Tiempo promedio de generación de tráfico web.

A continuación se muestra en el siguiente gráfico el promedio del tiempo obtenido por semana, en que los dispositivos de los usuarios que se conectaron con el AP, generaron tráfico web. Debido a que el tamaño de la muestra es de 126 dispositivos, se obtuvieron los tiempos de 42 dispositivos por semana, esto para realizar un análisis del promedio de manera equitativa respecto a la cantidad de dispositivos de los que se obtuvieron los tiempos en cada semana. Estos tiempos fueron sumados y el total se dividieron entre los 42 dispositivos de los se obtuvieron, esto dio como resultado los tiempos que se presentan la gráfica.

Gráfico N° 6: Tiempo de tráfico web.



9. Conclusiones

De acuerdo a las técnicas aplicadas y resultados obtenidos durante el desarrollo de este trabajo se ha concluye que:

1. Utilizando herramientas tales como Tcpdump, Wireshark y NetworkMiner es posible capturar información de tráfico de red para posteriormente, con ellas mismas, realizar un análisis detallado y obtener en esta ocasión los resultados establecidos como objetivos; como el identificar los dispositivos utilizados por los usuarios al momento de conectarse con él AP, así como los sistemas operativos que ejecutaban dichos dispositivos; también se obtuvieron los sitios web más visitados por los usuarios; y por último se conoció el tiempo promedio en que los usuarios generaron trafico web mientras estos accedían a los sitios web.

2. Con la realización de este trabajo se obtuvo como resultados que los sitios web más accedidos por los usuarios que se conectaron con el AP fueron (en este orden, de mayor a menor): El buscador de google, Facebook, WhatsApp, YouTube, Google Play.

3. Los usuarios que se conectaron con el AP utilizaron en su mayoría dispositivos móviles para conectarse.

4. Los sistemas operativos que ejecutaban los dispositivos móviles y/o computadoras usados por los usuarios fueron: Android, Ubuntu, Windows, IOS, siendo Android el sistema operativo más utilizado, y IOS el sistema menos utilizado.

5. De acuerdo con la información obtenida se puede afirmar que los usuarios navegaron por Internet a través de la conexión que se les ofreció por medio del AP instalado; esto lo podemos asegurar debido a los tiempos promedios en que los usuarios generaron tráfico web al acceder o visitar un sitio web; los resultados fueron de: 1 hora y 19 minutos en la primera semana; 1 hora y 30 minutos en la segunda semana y por último; 1 hora y 5 minutos en la tercera semana en que funcionó la conexión a Internet con el AP.

10. Recomendaciones

En este apartado se exponen algunas recomendaciones o sugerencias a tomar en cuenta ya que pueden ser de gran utilidad para aquellas personas o instituciones que hacen uso o proveen una red, ya que las siguientes 3 recomendaciones podrían ayudar hacer una mejor gestión de la red, así como el ancho de banda.

1. No brindar información privada o delicada a través de redes públicas.

Debido a la gran aceptación por parte de las personas o usuarios al conectarse con el AP con conexión a Internet que se brindó para el desarrollo de este trabajo, se recomienda a las personas de tener el debido cuidado de no brindar información privada y/o delicada cuando estas se conecten a Internet a través de una red pública o que resulte desconocida para ellos, como fue el caso de la red que se brindó, ya que en el mundo de la informática esto resulta peligroso ante la potencial amenaza de hackers que intentan adueñarse de información privada para su propio beneficio.

2. Hacer más rápida la carga de páginas web, por medio de cacheo web

Uno de los métodos más prácticos y sencillos para lograr que una página web cargue más rápido, es haciendo cacheo web, con esto nos referimos a la caché que almacena los documentos web que son solicitados en algún momento por primera vez y que luego son almacenados. Todos los navegadores poseen una cache (memoria) para reducir el tamaño y la cantidad de peticiones HTTP necesarias.

Esto permite hacer cacheables las páginas web, es decir, el mantener en la memoria del navegador los elementos que las componen permitiendo de esta manera una reducción considerable de consumo de ancho de banda.

Todo lo antes mencionado se debe de tomar en cuenta cuando se intenta acceder a plataformas webs que requieran mucha carga para el ancho de banda de la red; de lo contrario tomando en cuenta la primera recomendación es preferible hacer navegaciones por Internet a través del modo incognito que ofrecen los navegadores, esto cuando se utiliza redes públicas o desconocidas.

3. Implementar CDN Institucionales para maximizar el ancho de banda y hacer una mejor gestión de la red.

CDN o Red de entrega de contenidos son redes superpuestas de computadoras que contienen copias de datos, colocados en varios puntos de la red con el fin de maximizar el ancho de banda para el acceso a los datos de clientes a través de la red.

Si una institución implementará una CDN esto le brindará beneficios tales como:

- Obtendrá una mayor capacidad de conexión, esto debido a que los datos están dentro de la propia red y no en una red externa a la cual se debe acceder.
- Una disminución en el tiempo de repuesta de entrega de información al usuario; esto debido por lo mencionado en el punto anterior.
- Debido a que los datos estarían dentro de la misma red, habría una disminución de carga dentro de la red.
- Habría una disminución en la perdida y demora de paquetes ya que se trabaja con nodos muy cerca del usuario.
- Se tendría un 100% de disponibilidad de la información; esto incluso ante la caída de algunos de los servidores.

11. Bibliografías

Alegsa, L. (2010). *ALEGSA*. Obtenido de ALEGSA: http://www.alegsa.com.ar/Dic/trafico%20web.php

Catoira, F. (2013). *Welivesecurity*. Obtenido de Welivesecurity.

dd-wrt.com. (2 de Julio de 2010). *dd-wrt.com*. Obtenido de dd-wrt.com: http://www.dd-wrt.com/wiki/index.php/%C2%BFQu%C3%A9_es_%22DD-WRT%22%3F

Debian.org. (2015). *Debian*. Obtenido de Debian: https://www.debian.org/releases/stable/mips/ch01s02.html.es

Falcón, J. A. (2010). WI-FI, Lo que se necesita conocer. En J. A. Falcón, *WI-FI, Lo que se necesita conocer* (págs. 1-6). RC Libros.

Falcón, J. A. (2010). WI-FI, lo que se necesita saber. En J. A. Falcón, *WI-FI, lo que se necesita saber* (págs. 8-9). RC Libros.

Falcón, J. A. (2010). WI-FI, lo que se necesita saber. En J. A. Falcón, *WI-FI, lo que se necesita saber* (págs. 11-14). RC Libros.

Kioskena.net. (Marzo de 2015). *Kioskena.net.* Obtenido de Kioskena.net: http://static.ccm2.net/es.ccm.net/faq/pdf/que-es-un-router-2757-nlfz9y.pdf

Mansilla, P. C. (2016). *Facultad de Ciencias Agrarias (FCA),Universidad Nacional del Litoral.* Obtenido de Facultad de Ciencias Agrarias (FCA),Universidad Nacional del Litoral.: http://www.fca.unl.edu.ar/informaticabasica/Redes.pdf

Masadelante.com. (2016). *Masadelante.com*. Obtenido de Masadelante.com: http://www.masadelante.com/faqs/sistema-operativo

Miranda, C. V. (2015). *Sistemas informáticos y redes locales.* Paraninfo S.A.

Porto, J. P., & Gardey, A. (2013). *Definicion.de*. Obtenido de Definicion.de: http://definicion.de/protocolo-de-red/

Porto, J. P., & Merino, M. (2010). *Definicion.de*. Obtenido de Definicion.de: http://definicion.de/windows/

Porto, J. P., & Merino, M. (2014). *Definicion.de*. Obtenido de Definicion.de: http://definicion.de/trafico/

Ramirez, V. (2016). *Monografias.com*. Obtenido de Monografias.com: http://www.monografias.com/trabajos81/que-es-internet/que-es-internet.shtml

Ríos, R., & Fermin, J. (2009). Análisis de red local universitaria. *TELEMATIQUE, 8*(2), 15-27. Recuperado el 31 de Agosto de 2016, de http://publicaciones.urbe.edu/index.php/telematique/article/view/869/2146

Seguridad y Redes. (14 de Febrero de 2008). *Seguridad y Redes*. Obtenido de Seguridad y Redes: https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/

Tcpdump.org. (17 de Septiembre de 2015). *Tcpdump.org*. Obtenido de Tcpdump.org: http://www.tcpdump.org/tcpdump_man.html

Untiveros, S. (2010). *AprendaRedes.com*. Obtenido de AprendaRedes.com: http://www.aprendaredes.com/dev/articulos/aprende-a-mirar-dentro-de-la-red-con-un-sniffer.htm

Wikipedia. (26 de Noviembre de 2015). *Wikipedia: Enciclopedia libre*. Obtenido de Wikipedia: Enciclopedia libre: https://es.wikipedia.org/wiki/Agente_de_usuario

Yashiroevil's Blog. (30 de Agosto de 2010). *Yashiroevil's Blog*. Obtenido de Yashiroevil's Blog: https://yashiroevil.wordpress.com/2010/08/30/networkminer-como-herramienta-de-analisis-forense/

12. Anexos

Anexo 1: Cronograma de actividades.

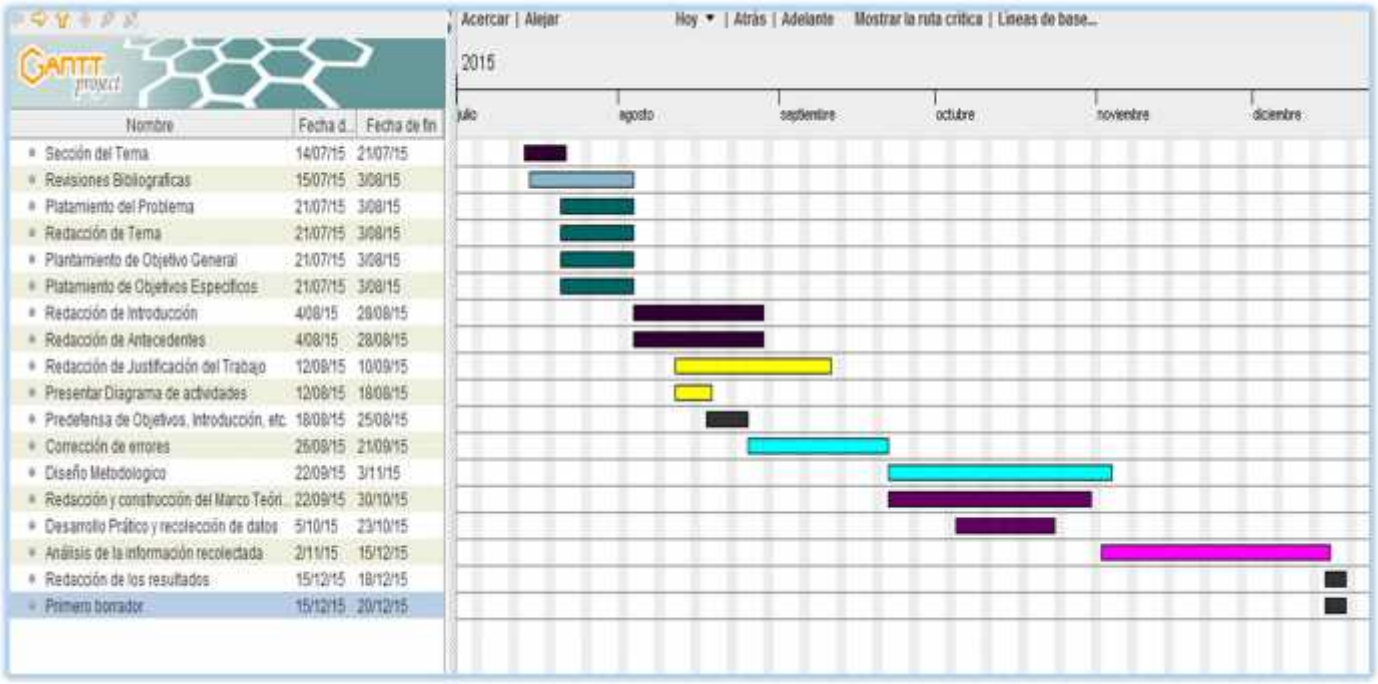


Figura 1: Muestra el cronograma de actividades.

Anexo 2: Router y firmware.

Figura 2: Diseño del Router Linksys WRT-610 V1.

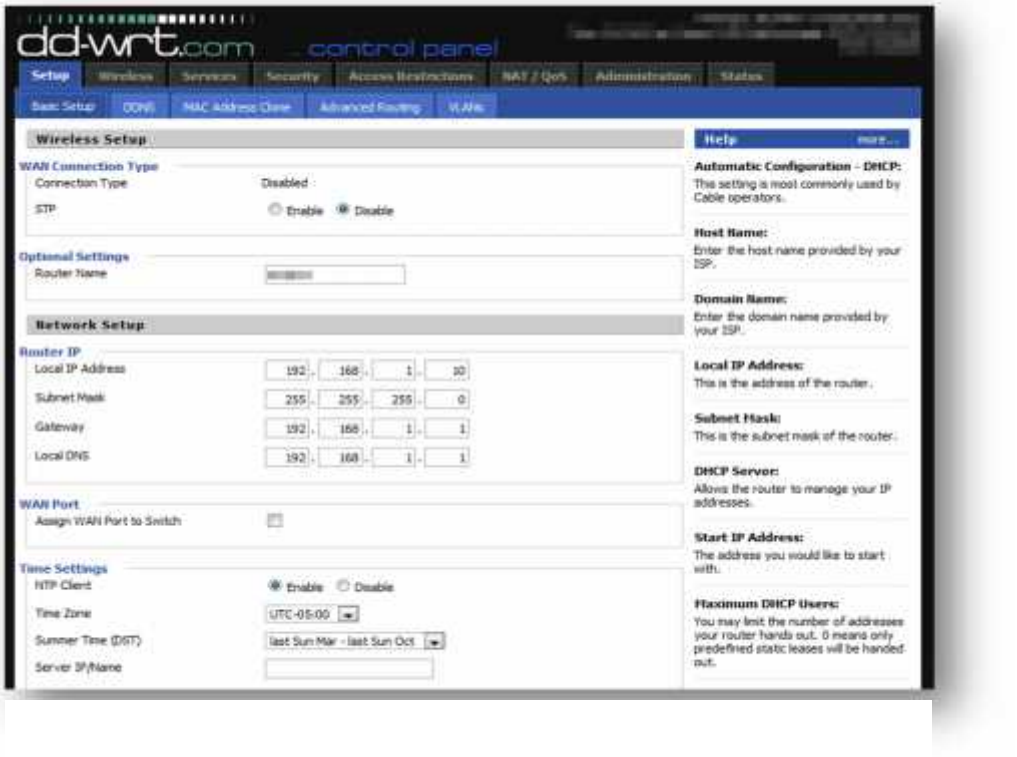


Figura 3: Interfaz gráfica de usuario del firmware DD-WRT.

Anexo 3: Análisis de tráfico con NetworkMiner.

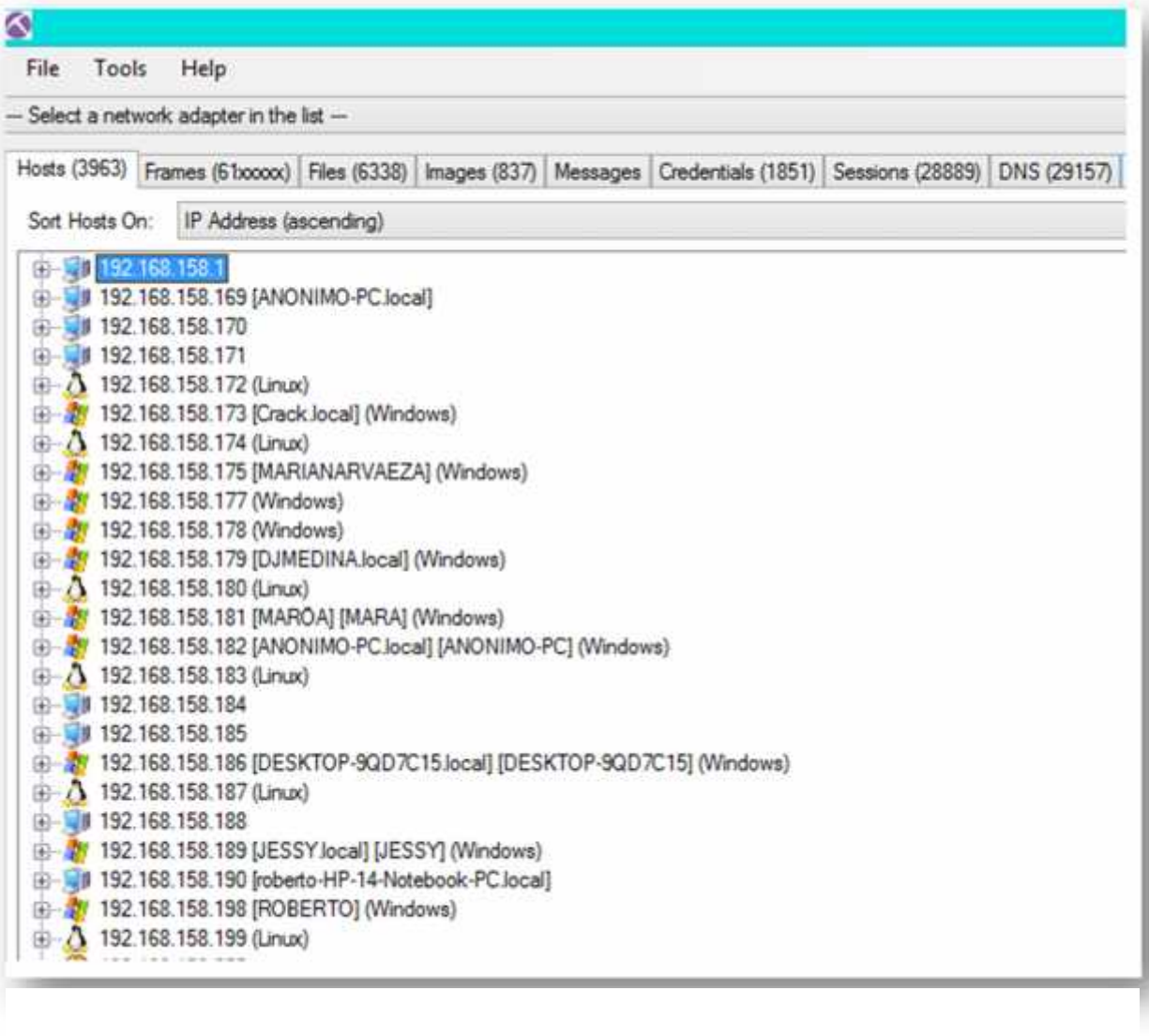


Figura 4: Interfaz gráfica de la aplicación NetworkMiner.

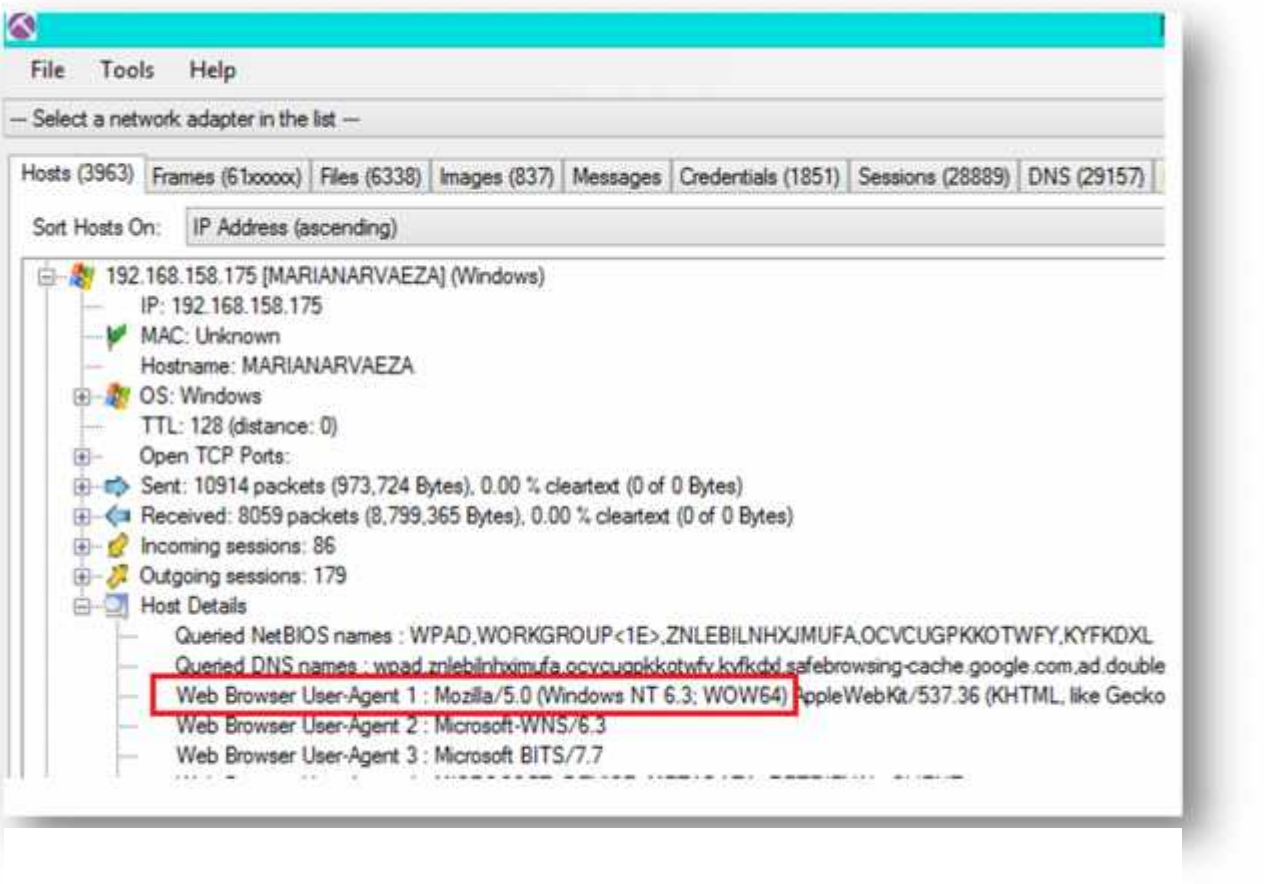


Figura 5: Identificando ordenadores con sistemas Windows.

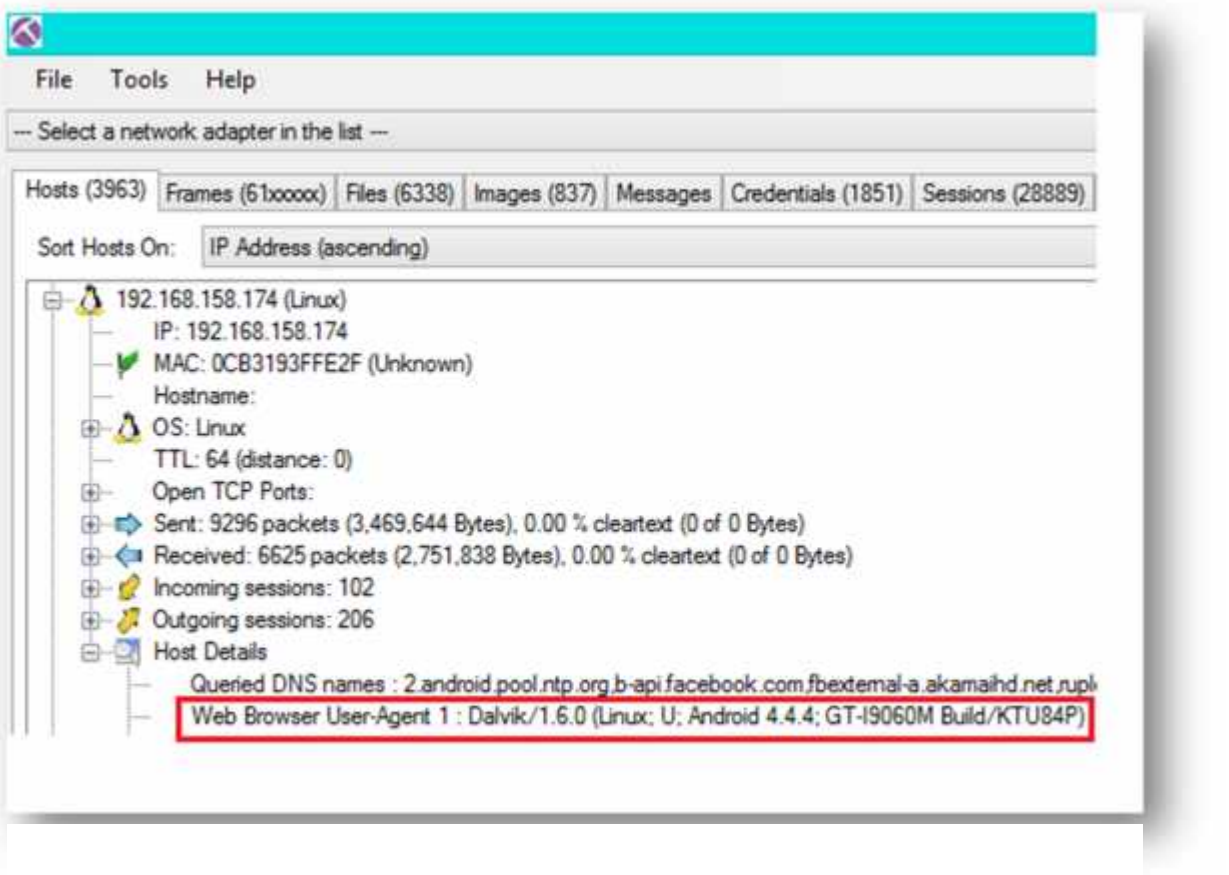


Figura 6: Identificando dispositivo móvil con sistema Android.

Anexo 4: Muestra de la Población total.

h = N / [P^2(N-1)+1]

h = Es la muestra.

N = Es el número de sujetos que constituyen la población, en este caso 184.

P = Es la probabilidad de error de la muestra que fija el investigador en este caso 0.05.

h = 184 / [$(0.05)^2$(184-1)+1]

h = 126

Figura 7: Fórmula para obtener la muestra.

Anexo 5: Análisis de paquetes con Wireshark.

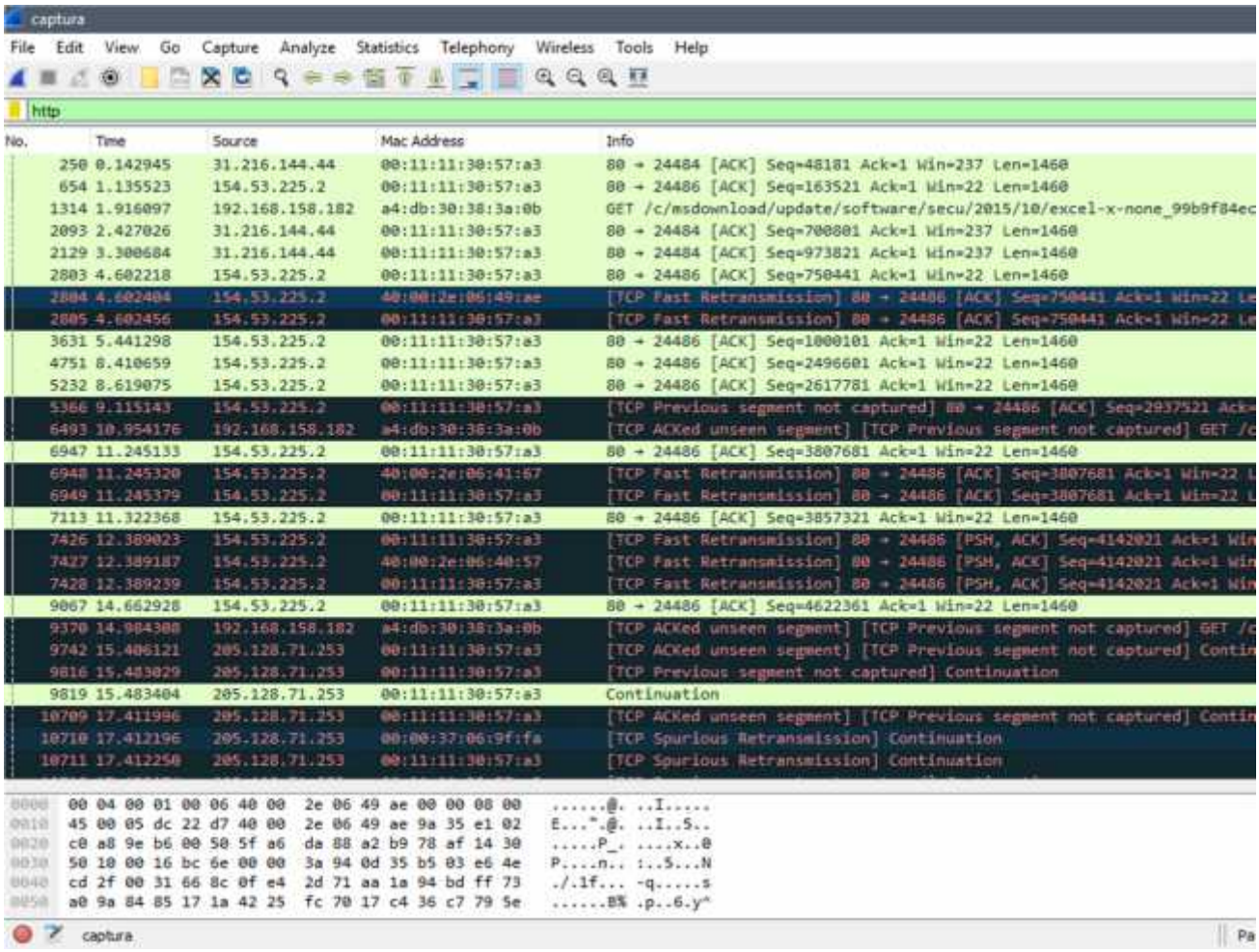


Figura 8: Analizando tráfico de red en la aplicación Wireshark.

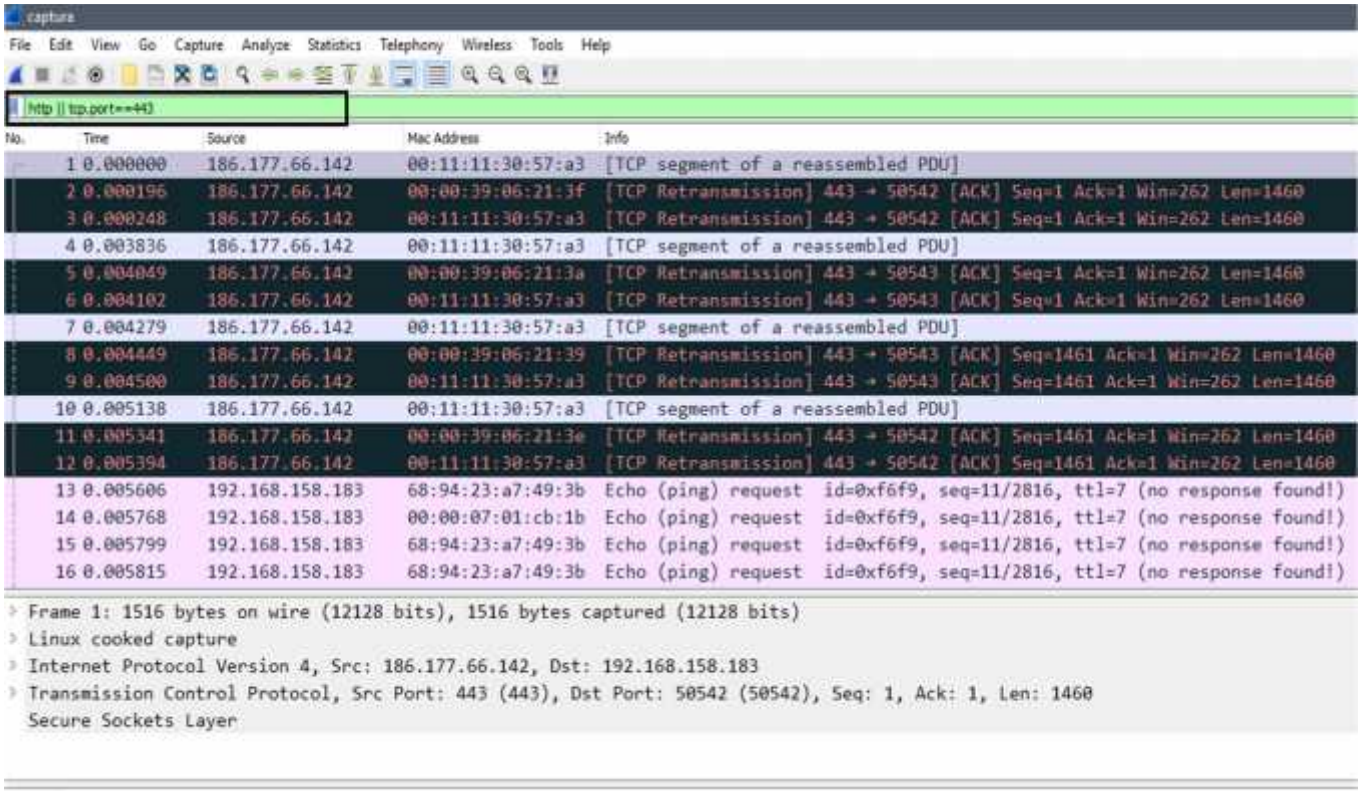


Figura 9: Usando filtro http||tcp.port==443 para obtener tráfico web.

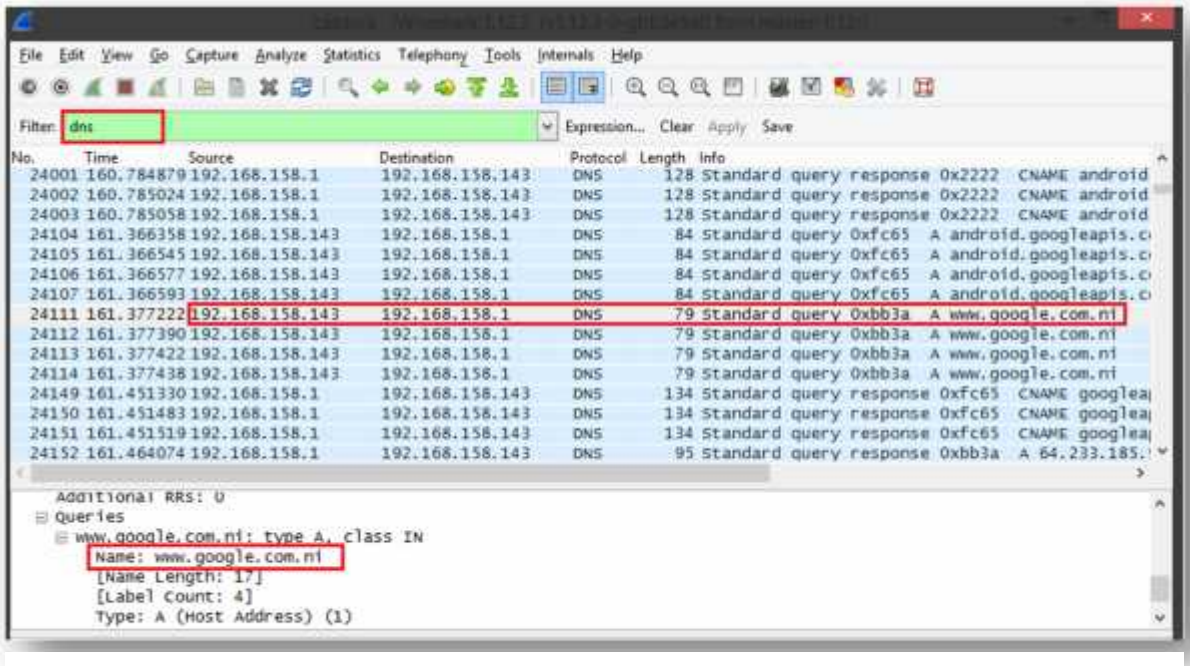


Figura 10: Obteniendo resoluciones DNS en Wireshark.

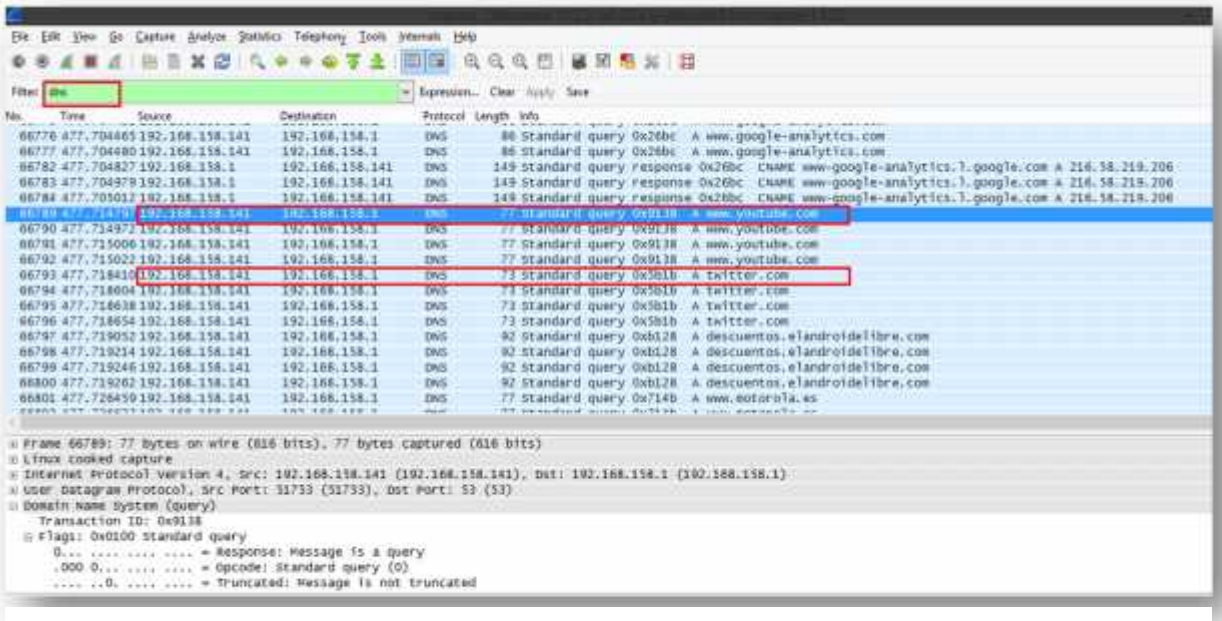


Figura 11: Obteniendo páginas web visitadas.

Anexo 6: Manejando información en Excel.

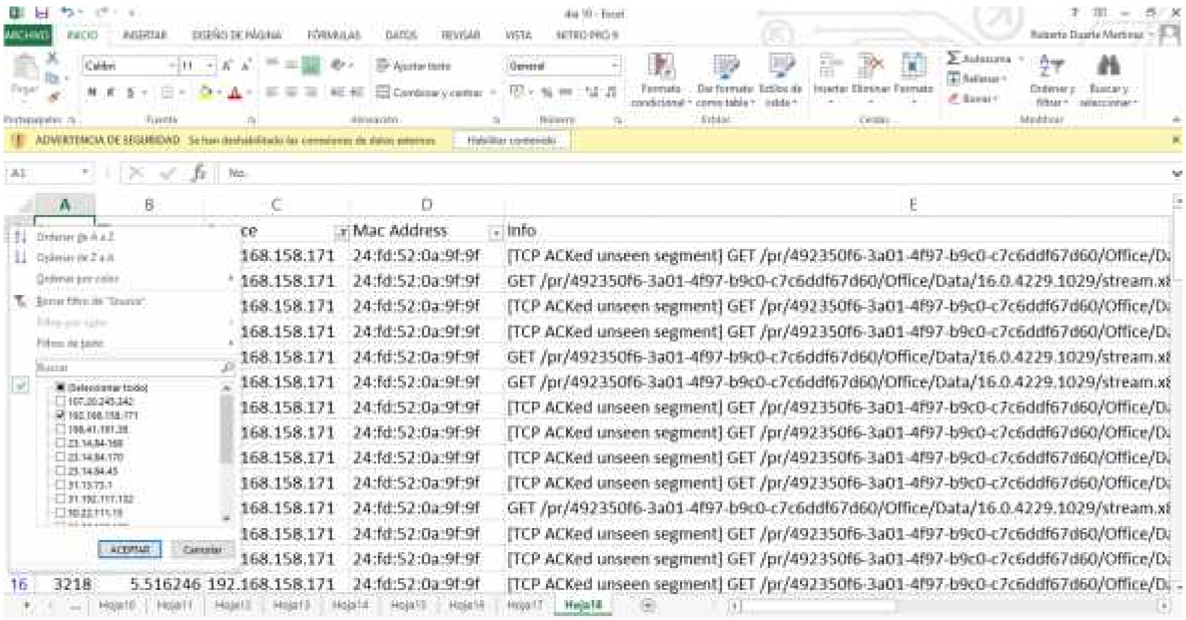


Figura 12: Manejando información de tráfico de red en Excel.