UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

RASTREO DE CORREOS ELECTRÓNICOS

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERA EN REDES

PRESENTA
KAREN IRLANDA RANGEL SOSA

SUPERVISORES
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA
DR. JAVIER VÁZQUEZ CASTILLO
MTI. MELISSA BLANQUETO ESTRADA

CHETUMAL QUINTANA ROO, MÉXICO, JULIO DE 2017

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO BAJO LA SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARA OBTENER EL GRADO DE:

INGENIERA EN REDES

COMITÉ DE TRABAJO MONOGRÁFICO

SUPERVISOR: _____
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISOR: _____
DR. JAVIER VÁZQUEZ CASTILLO

SUPERVISORA: _____
MTI. MELISSA BLANQUETO ESTRADA

CHETUMAL QUINTANA ROO, MÉXICO, JULIO DE 2017

Agradecimientos

Agradezco a Dios por darme vida, salud; al permitirme poder concluir mis estudios y para realizar este trabajo.

A mi madre por dejarme la mejor herencia que es la formación académica.

A mis profesores por la formación que me han brindado.

A mi tutor el MTI. Vladimir Cabañas por la guía y el apoyo en este trabajo de investigación.

Dedicatoria

Dedico este trabajo a mis padres, en especial a mi madre por todo el apoyo brindado.

Resumen

El presente proyecto de titulación tuvo como objetivo principal realizar el análisis de rastreo de correo electrónico, en la cual se realizó una amplia investigación del correo electrónico desde su origen, aspectos sociales del correo electrónico, su arquitectura y servicios, los agentes del correo electrónico, las características, el funcionamiento y la estructura del correo electrónico.

Se presentan los protocolos que intervienen en el servicio de correo electrónico, su estructura y funcionamiento, así como algunas vulnerabilidades que pueden comprometer el servicio de correo electrónico.

Se realizó, durante la elaboración del proyecto un breve análisis de las funcionalidades que nos proporcionan algunas herramientas de informática forense para determinar el origen y el camino que siguen los correos electrónicos, a través de diferentes técnicas como el análisis de encabezados del correo lo cual permite identificar información como la dirección IP, que después puede ser vinculada a un origen específico.

Finalmente se exponen los datos de geolocalización, traza de direcciones de forma cronológica, reportes de abuso, identificación del país/estado del origen de los correos, información de actores que intervienen en el servicio y técnicas de ocultamiento de información de usuarios y equipos que utilizan los spammers.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1 INTRODUCCIÓN

En la evolución de la humanidad ha sido imprescindible la comunicación como medio de interacción entre la colectividad; este proceso le ha permitido el entendimiento y ha ayudado en su desarrollo social, cultural y tecnológico.

En las últimas décadas, la comunicación ha sido objeto de innumerables estudios multidisciplinares, en los cuales se ha tratado de definir los alcances de este concepto en la era digital.

La tecnología informática se ha difundido muy rápidamente y es por ello que hoy en día prácticamente la totalidad de nuestras actividades personales, profesionales y comerciales se desarrolla utilizando algún medio informático y es allí donde quedan rastros de nuestras actividades cotidianas.

En el caso de una conducta delictiva haciendo uso de herramientas tecnológicas, un aspecto muy importante a considerar es que existe “evidencia digital” y se puede presentar frente a una instancia judicial; aunque muchas de estas conductas son delitos tradicionales, con el advenimiento de la tecnología también han aparecido delitos puramente informáticos y es por ello que se habla de crímenes electrónicos.

El correo electrónico es uno de los grandes y cotidianos medios que se practican en un sistema de cómputo; con la capacidad de entregar mensajes casi al instante en cualquier parte del mundo, proporciona la velocidad y eficacia que no puede ser igualada por el servicio postal regular. Desafortunadamente, eficaz como es entregando mensajes legítimos, el correo electrónico también es bastante eficaz distribuyendo software malicioso y llenando las bandejas de entrada con correo basura no solicitado (spam).

El correo electrónico se ha convertido en una vulnerabilidad potencial contra la seguridad. Es una puerta virtual que lleva directamente a la red informática corporativa e indirectamente a cada computadora. Puede ser usada por piratas informáticos para introducirse a hurtadillas o, por empleados para sacar en forma encubierta secretos de propiedad de la empresa. También

provee un portal para la destrucción de datos, ya sea mediante ataques aleatorios con virus o por ataques dirigidos por activistas o competidores.

La seguridad informática es un tema que mucha gente no le da la importancia que realmente tiene; muchas veces por el hecho de considerar que es inútil o que jamás la utilizará. Pero en el mundo moderno, cada día más y más personas mal intencionadas pretenden tener acceso a los datos de nuestros sistemas de cómputo.

El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas. Una de las posibles consecuencias de una intrusión es la **pérdida de datos**. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día en las copias de seguridad, y aun así no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el **robo de información** sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano es el de las contraseñas de las cuentas de correo por las que intercambiamos información con otros.

1.1 DEFINICION DEL PROBLEMA

En la actualidad el correo electrónico es uno de los servicios de internet con mayor demanda, con él que se puede compartir una gran cantidad de datos instantáneamente y desde cualquier lugar al estar integrado en diversos dispositivos.

En el ambiente académico (por ejemplo), el correo electrónico es el medio por el cual investigadores y alumnos comparten información científica y escolar. En el contexto laboral es uno de los medios de comunicación más utilizado; sin embargo, esta tecnología lleva consigo una serie de riesgos tecnológicos que pueden ocasionar serios problemas de seguridad a la información.

En este aspecto, desde hace muchos años se ha visto un incremento en el número de crímenes cibernéticos utilizando específicamente el correo electrónico, la información que se maneja en el correo electrónico tiene mucho valor para nosotros y existen personas interesadas en darle un mal uso, es por ello que se ha observado de manera amplia y constante los numerosos correos electrónicos anónimos de dudosa procedencia llegan en nuestra bandeja de entrada, surge el interés por conocer más detalladamente acerca de la procedencia de los correos electrónicos anónimos.

A pesar de que el tema abordado en la presente investigación abarca todos los aspectos de nuestra vida diaria, y se refleja en cada característica de nuestro contexto de vida, es imposible abarcar de manera pertinente cada una de ellas, por lo tanto, se realizara una investigación detallada acerca de los correos electrónicos de dudosa procedencia llegan a la bandeja de entrada de un correo electrónico.

1.2 JUSTIFICACIÓN

Para sustentar la razón, importancia y visión de la presentación del proyecto de investigación consideramos aspectos técnicos y sociales, encaminados al aporte investigativo, así como el aprovechamiento de los recursos tecnológicos.

El entorno social en el que nos desenvolvemos hace que, día a día, lleguen a nuestra bandeja correos electrónicos, una gran parte de la dinámica de las instituciones descansa sobre aplicaciones que dependen del correo electrónico, algunos de estos usos son:

- Comunicación entre directores y empleados
- Canales de distribución de información interna o externa
- Canal de comunicación y soporte de ayuda a clientes y ciudadanos
- Seguimiento de concursos públicos
- Correspondencia con otras entidades de la distribución
- Distribución de ofertas de empleo público

Desafortunadamente, el correo electrónico se ha convertido en una vulnerabilidad potencial contra la seguridad. La configuración e implementación de un servidor de correo se hicieron principalmente para analizar el rastreo de correos electrónicos.

1.3 OBJETIVO GENERAL

Analizar el proceso de rastreo de correo electrónico, así como también definir los protocolos utilizados y el nivel de seguridad de los datos.

1.4 OBJETIVOS ESPECÍFICOS

- Describir la estructura, los protocolos y los conceptos relacionados con el servicio de correo electrónico.
- Analizar los protocolos de correo electrónico con sus principales características en seguridad de datos en los mensajes.
- Recopilar la información necesaria sobre las herramientas informáticas a utilizar.
- Analizar el rastreo de correos electrónicos.
- Analizar los encabezados de los correos electrónicos
- Obtener direcciones IP mediante el análisis del encabezado de los correos electrónicos.
- Obtener el nombre del propietario de la dirección IP.

1.5 ALCANCE

El alcance de este proyecto se centrará en los correos electrónicos no deseados que llegan a la bandeja de entrada de una cuenta personal.

1.6 METODOLOGÍA

La presente investigación se ha desarrollado conforme a un enfoque de tipo cualitativo basada más en una lógica y proceso inductivo la cual abarca algunos procesos de la fase del modelo cualitativo como son el planteamiento del problema, revisión de la literatura, desarrollo del marco teórico, la elaboración de hipótesis, definición de las variables, recolección y análisis de los datos obtenidos por herramientas para el rastreo de correo electrónicos; teniendo como

objetivo principal el estudio y análisis de la procedencia de diversos correos electrónicos que recibimos en nuestra bandeja de entrada de una cuenta de correo personal.

La información recolectada se procesará para llegar al objetivo general planteado con la ayuda de las variables y los indicadores que aportaran en la investigación.

VARIABLES INDICADORES

Dependientes

- Herramientas de informática forense
  - Indicador.
    - De tipo software libre.
- Características de herramientas
  - Indicador.
    - Servicios que brindan las herramientas para el rastreo de correos electrónicos.

Independientes

- Localización de origen de correo electrónico.
  - Indicador.
    - Uso de la herramienta para el rastreo de correo electrónico.

CAPÍTULO 2 MARCO TEÓRICO

2.1 INTRODUCCIÓN

El correo electrónico, o e-mail, que es enviado por Internet debe formatearse de acuerdo con una serie de reglas comunes. Los usuarios utilizan diferente software de e-mail para leer y enviar correo electrónico, entre los que están Microsoft Outlook, Netscape Messenger, Eudora, PINE y muchos otros. Un creciente número de gente emplea un lector de correo que se ofrece como parte de un sitio web, como Yahoo! Mail o Hotmail. Aunque los mensajes de correo electrónico no siguieron las reglas estándar, un e-mail creado por una persona en una compañía (o mediante el uso de un sitio web) no podría ser leído por otra persona en otra compañía (o sitio web) que usara un lector distinto.

Los distintos tipos de redes públicas y privadas han originado la existencia de diferentes formatos de especificación de correo electrónico. Se debe tener en cuenta, al implementar un sistema de correo electrónico, la utilización de una norma estándar que unifique procedimientos de gestión y transferencia de mensajes. De este modo se pueden efectuar intercambios de mensajes entre sistemas distintos, incluso de aquellos que incorporen información multimedia, como imágenes o videos.

Teniendo en consideración lo que es la comunicación con el exterior, existen dos tipos de mensajería electrónica, ampliamente difundidas:

- SMTP (Simple Mail Transfer Protocol), que es la utilizada en Internet y la que tiene mayor difusión (recogida en la norma RFC822).
- X.400, una norma del CCITT para interconectar Agentes de Usuario con Agentes de Transferencia de Mensajes, mucho más compleja que la anterior:

En ambos casos se hace necesario contar con completo directorio electrónico de empresas y/o personas con las que se mantiene contacto habitual, algo equivalente a las guías telefónicas que consultamos cuando queremos hacer una llamada a alguien y desconocemos su número.

2.2 ANTECEDENTES

El correo electrónico antecede a internet y fue una herramienta crucial para su creación. El nombre <<correo electrónico>> tiene su origen en la analogía con el correo postal: ambos sirven para enviar y recibir mensajes rápidamente "también denominados mensajes electrónicos o cartas electrónicas" mediante sistemas de comunicación electrónicos; estos mensajes pueden contener o no archivos adjuntos, y se utilizan <<buzones>> intermedios (servidores), en donde los mensajes se guardan temporalmente antes de dirigirse a su destino, y antes de que el destinatario los revise (Benbunan, 2011, pág. 12); estos mensajes pueden contener o no archivos adjuntos.

El correo electrónico fue creado por Ray Tomlinson en 1971. Ray Tomlinson se graduó en ingeniería eléctrica en el Instituto de Tecnología de Massachusetts (MIT) y entro a trabajar en la empresa BBN1 en 1967, poco antes de que su empresa recibiera el encargo de trabajar para ARPANET (red de ordenadores creada por encargo del Departamento de Defensa de los Estados Unidos como medio de comunicación para los diferentes organismos del país), la red precursora de Internet.

En esa empresa utilizó un programa llamado SNDMSG para enviar mensajes entre los distintos usuarios de un mismo sistema de cómputo. Eran tiempos en que los usuarios trabajan en informática mediante una pantalla y un teclado, sin memoria ni procesador propios, conectadas a un sistema de cómputo central. Estas terminales recibieron ese nombre porque no realizaban ningún computo, solo eran usadas para enviar datos de forma asíncrona a la computadora principal para que esta los procesara.

En septiembre de 1971, cuando la empresa BBN ya estaba conectada a ARPANET y haciendo un amplio uso de ella, Ray adapto el programa SNDMSG de forma que sirviera también para enviar mensajes entre diferentes sistemas conectados en red. Fue entonces cuando se le ocurrió utilizar el símbolo @ para unir el nombre del usuario y el de la computadora que utilizaba como servidor. Según algunas teorías se trataba de utilizar un símbolo que estuviera en todos los teclados pero que no apareciera en los nombres de las personas ni de las computadoras. En realidad, la @ estaba en los teclados, pero no se utilizaba prácticamente

para nada por lo que no era probable que entrara en conflicto con ninguna otra cosa. Otras teorías, dicen que el término empleado como divisor entre el usuario y la máquina fue la arroba porque está en ingles se pronuncia “at” (en), lo que hace que una dirección X@Y se lea como “usuario x en máquina y”.

La aparición de ARPANET, la antecesora de Internet, supuso un cambio radical en el ámbito de aplicación del correo electrónico y el inicio de su enorme crecimiento. La gran innovación de ARPANET se basaba en la separación de los mensajes que se comunicaban a través de la red en paquetes de datos o datagramas, con dos ventajas principales: primero, que un mismo canal de comunicación (por ejemplo, una línea telefónica entre dos ciudades distintas) podía emplearse para comunicar muchos ordenadores a la vez; y segundo, al separarse en paquetes la información podía encaminarse por vías diferentes, haciendo así la comunicación más segura e independiente del estado de las líneas de transmisión de la información (Moro, 2010, pág. 340).

ARPANET hizo posible comunicar muchas computadoras distantes unas con otras de modo relativamente barato y fiable. La transmisión de la información ya no estaba limitada, como el pasado, a los usuarios de una misma supercomputadora, ni tampoco a los de unas pocas computadoras conectadas a través de una Red de Área Local.

El desarrollo de ARPANET, inicialmente vinculado al Departamento de Defensa estadounidense, pronto desbordó el marco en el que se había creado; a lo largo de la década de los ochenta, la evolución en paralelo de otras redes, la creación de protocolos estándar de comunicación entre ellas y, finalmente, el desarrollo del lenguaje HTML, desembocaron en lo que hoy conocemos como internet. (Moro, 2010, pág. 340)

A partir de ahí la expansión fue imparable. Surgieron los primeros programas de correo electrónico como RD (el primero en crearse), NRD, WRD y MSG considerado el primer programa moderno de gestión de correo electrónico. Ya en 1973 un estudio señalaba que el correo electrónico representaba el 75% del tráfico en ARPANET.

En 1982, se publicaron las propuestas de correo electrónico de ARPANET como el RFC 821 (protocolo de transmisión) y el RFC 822 (formato de mensaje). Las revisiones menores, los RFCs 2821 y 2822, se han vuelto estándares de Internet, pero todas las personas aún se refieren al correo electrónico de Internet como el RFC 822 (Tanenbaum A. S., Correo electrónico, 2003, pág. 589).

En 1984, el CCITT redactó la recomendación X.400. Después de dos décadas de competencia, los sistemas de correo electrónico basados en el RFC 822 se utilizan ampliamente, mientras que aquellos basados en X.400 han desaparecido (Tanenbaum A. S., Correo electrónico, 2003, pág. 589).

La razón del éxito del RFC 822 no es que sea tan bueno, sino que X.400 estaba tan pobremente diseñado y era tan complejo que nadie podía implementarlo bien. Dada la opción entre un sistema de correo electrónico basado en el RFC 822 simple, pero funcional, y un sistema de correo electrónico X.400 supuestamente maravilloso, aunque complejo, la mayoría de las organizaciones eligen el primero (Tanenbaum A. S., Correo electrónico, 2003, pág. 590).

En 1989 desapareció ARPANET y, por otro lado, el investigador Tim Berners-Lee del centro europeo CERN en Suiza, desarrolló una propuesta de sistema de hipertexto, lo que daría lugar a la World wide Web (www).

El correo electrónico o email, ha existo por más de dos décadas. En la década de 1990, se dio a conocer al público y creció en forma exponencial al punto que el número de mensajes de correo electrónico enviados por día ahora es mayor que el número de cartas por correo postal.

El correo electrónico, como la mayoría de otras formas de comunicación, tiene sus propias convenciones y estilos. En particular, es muy informal y tiene un umbral bajo de uso. Las personas que nunca hubieran soñado con escribir una carta a un personaje importante, no dudarían un instante para enviarle un mensaje de correo electrónico. (Tanenbaum A. S., 2003, pág. 588)

El correo electrónico está lleno de abreviaturas, como BTW (By The Way, por cierto), ROTFL (Rolling On The Floor Laughing, rodando por el suelo muerto de risa) e IMHO (In My Humble Opinión, en mi humilde opinión). Muchas personas también utilizan pequeños símbolos ASCII llamados caritas o símbolos de emociones en sus mensajes de correo electrónico. Algunos de los más interesantes se listan en la tabla 1 (Tanenbaum A. S., Correo electrónico, 2003, pág. 589).

Emoticón	Significado	Emoticón	Significado	Emoticón	Significado
☺	Estoy feliz	=|:-)	Abe Lincoln	:+)	Nariz grande
☹	Estoy triste/enojado	=):-)	Tío Sam	:-))	Realmente feliz
:-I	Estoy apático	*<:-)	Santa Claus	:-{)	Con bigote
;-)	Estoy guiñando un ojo	<:-(	Bobo	#:-)	Peinado yuppy
:- (O)	Estoy gritando	(-:	Zurdo	8-)	Con gafas
:- (*)	Estoy vomitando	:-)X	Hombre con moño	C:-)	Inteligente

Tabla 1 Algunos emoticones

Los primeros sistemas de correo electrónico simplemente consistían en protocolos de transferencia de archivos, con la convención de que la primera línea de cada mensaje (es decir, archivo) contenía la dirección del destinatario. A medida que pasó el tiempo, las limitaciones de este enfoque se hicieron obvias (Tanenbaum A. S., Correo electrónico, 2003, pág. 589).

Algunas de las quejas eran:

1. El envío de un mensaje a un grupo de personas era laborioso. Los administradores con frecuencia necesitaban esta facilidad para enviar memorandos a todos sus subordinados.

2. Los mensajes no tenían estructura interna, lo que dificultaba el proceso por computadora. Por ejemplo, si un mensaje reenviado se incluía en el cuerpo de otro mensaje, era difícil extraer la parte reenviada del mensaje recibido.
3. El originador (remitente) nunca sabía si el mensaje había llegado o no.
4. Si alguien planeaba ausentarse por un viaje de negocios durante varias semanas y quería que todo el correo entrante fuera manejado por su secretaria, esto no era fácil de arreglar.
5. La interfaz de usuario estaba mal integrada al sistema de transmisión, pues requería que el usuario primero editara un archivo, luego saliera del editor e invocara el programa de transferencia de archivos.
6. No era posible crear y enviar mensajes que contuvieran una mezcla de texto, dibujos, facsímiles y voz.

A medida que se acumuló experiencia, se propusieron sistemas de correo electrónico más elaborados. (Tanenbaum A. S., Correo electrónico, 2003, pág. 589)

En la actualidad el correo electrónico es la aplicación más popular de Internet, y se calcula que la cantidad de información que se mueve a través del correo supera varias veces a la información contenida en páginas Web.

2.3 ASPECTOS DEL CORREO ELECTRÓNICO

El correo electrónico, es una de las funciones de Internet más utilizadas en la actualidad, a cualquier persona que tenga acceso a internet le permite enviar y recibir mensajes entre emisor y receptor cuando éstos han acordado el intercambio. Es uno de los servicios más utilizados debido a que facilita las comunicaciones en cualquier momento y a cualquier parte. Se basa en el protocolo TCP/IP y su esquema de conexión es asíncrono, es decir, no requiere establecer una conexión entre emisor y receptor para transmitir. Por lo tanto, al enviar un mensaje se requiere que el receptor revise su correo electrónico para leerlo, de lo contrario este permanece almacenado en un servidor de correo hasta que el usuario lo busque. Es un error pensar que en el correo electrónico el receptor conocerá el mensaje inmediatamente después de enviado, para esto se requiere una conexión sincrónica o en línea, donde tanto transmisor como receptor están listos para iniciar la charla (Tanenbaum A. S., Correo electrónico, 2003, pág. 590).

2.3.1 ASPECTOS NEGATIVOS

Algunos de los aspectos negativos del servicio de correo electrónico son:

- No garantiza que los mensajes lleguen a su destino.
- No asegura que el remitente sea quien dice ser.
- No mantiene el compromiso de avisar de las anomalías en el transcurso del envió del mensaje.
- Problema de seguridad si no se usa con los debidos controles. (Como antivirus, antispam, etc.).
- El envío de mensajes, permite adjuntar al mensaje, archivos de texto, de video, de audio, imágenes, etc.
- Sigue el modelo cliente/servidor: en el equipo servidor están definidas las cuentas de correo de los usuarios y sus buzones, y los clientes gestionan la descarga de correo, así como su elaboración.

2.3.2 ARQUITECTURA Y SERVICIOS

Para enviar o recibir un mensaje de correo, el usuario sólo ve el programa de correo electrónico que utiliza, cuando en realidad entran en funcionamiento otras aplicaciones de correo electrónico que realizan una determinada función en el proceso de mover y manipular los mensajes.

Normalmente consisten en dos subsistemas: los **agentes de usuario**, que permiten a los usuarios leer y enviar correo electrónico, y los **agentes de transferencia de mensaje**, que mueven los mensajes del origen al destino. Los agentes de usuario son programas locales que proporcionan un método basado en comandos, en menús o en una interfaz gráfica para interactuar con el sistema de correo electrónico. Los agentes de transferencia de mensajes son por lo común **demonios (daemons)** del sistema que operan en segundo plano y mueven correo electrónico a través del sistema.
Por lo general, los sistemas de correo electrónico desempeñan cinco funciones básicas, como se describe a continuación.

- La **redacción** se refiere al proceso de crear mensajes y respuestas. Aunque es posible utilizar cualquier editor de texto para el cuerpo del mensaje, el sistema mismo puede proporcionar asistencia con el direccionamiento y los numerosos campos de encabezado que forman parte de cada mensaje. Por ejemplo, al contestar un mensaje, el sistema de correo electrónico puede extraer la dirección del remitente e insertarla en forma automática en el lugar adecuado de la respuesta.

- La **transferencia** se refiere a mover mensajes del remitente al destinatario. En gran medida, esto requiere establecer una conexión con el destino o alguna máquina intermedia, enviar el mensaje y liberar la conexión. El sistema de correo electrónico debe hacer esto en forma automática, sin molestar al usuario.

- La **generación del informe** tiene que ver con indicar al remitente lo que ocurrió con el mensaje: ¿se entregó, se rechazó o se perdió? Existen muchas aplicaciones en las que la confirmación de la entrega es importante y puede incluso tener una aplicación legal (“Bien, Su Señoría, mi sistema de correo electrónico no es muy confiable, por lo que creo que la citación electrónica se perdió en algún lado”).

- La **visualización** de los mensajes de entrada es necesaria para que la gente pueda leer su correo electrónico. A veces se requiere cierta conversión o debe invocarse un visor especial, por ejemplo, si el mensaje es un archivo PostScript o voz digitalizada. Algunas veces también se intentan conversiones y formateo sencillos.

- La **disposición** es el paso final y tiene que ver con lo que el destinatario hace con el mensaje una vez que lo recibe. Las posibilidades incluyen tirarlo antes de leerlo, desecharlo después de leerlo, guardarlo, etcétera. También debe ser posible recuperar y releer mensajes guardados, reenviarlos o procesarlos de otras maneras.

Además de estos servicios básicos, la mayoría de los sistemas de correo electrónico, especialmente los corporativos internos, proporcionan una gran variedad de características avanzadas. Cuando la gente se muda, o cuando está lejos durante cierto tiempo, podría querer

el reenvío de su correo electrónico, por lo que el sistema debe ser capaz de hacer esto de manera automática (Tanenbaum A. S., Arquitectura y servicios, 2003, pág. 590).

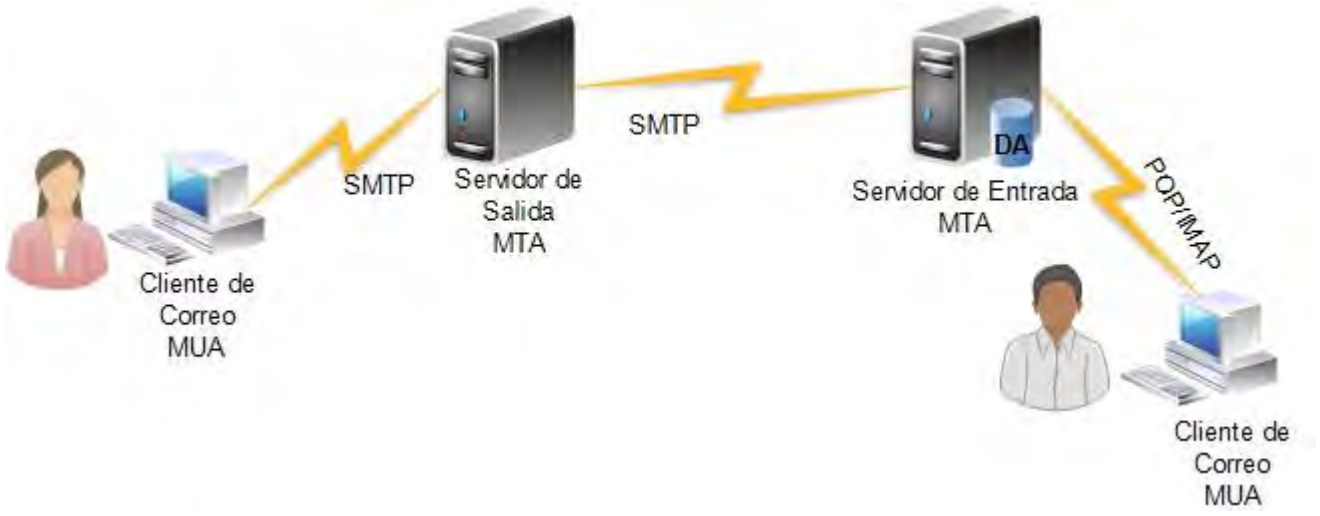


Ilustración 1 Arquitectura de un correo electrónico.
Gráfico de elaboración propia.

2.3.3 AGENTES

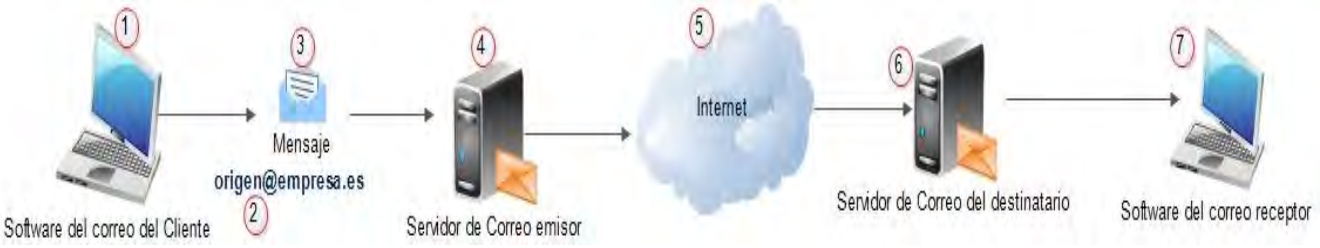


Ilustración 2 Agentes en una comunicación de correo o electrónico.
Gráfico de elaboración propia.

1. El software de correo-e del cliente.
2. La cuenta de origen del emisor. Esta puede ser enmascarada por varios sistemas.
3. El mensaje puede ser alterado, eliminado o puede contener virus.
4. El servidor de correo del emisor y su software, alojado en proveedor de servicios internet (o en la propia empresa caso de disponer de software de correo servidor).
5. El canal: internet, donde los hackers pueden interceptarlo, otros proveedores de telecomunicaciones, los routers servidores DMZ, etc.
6. El servidor de correo del destino y su software (asociado al dominio de la cuenta y al ISP donde esté alojado este dominio).
7. El software del correo receptor (MS Outlook, Lotus Notes, Thunderbird, etc.).

Todos estos agentes son potencialmente puntos de riesgo en la seguridad de un envío de correo electrónico.

2.3.4 CARACTERÍSTICAS COMÚNES DEL CORREO ELECTRÓNICO.

Las características más importantes del correo electrónico son las que se detallan a continuación, que suelen ser las comunes a cualquier paquete el usuario adquiera.

- **Acuse de recibo automático**: El emisor puede comprobar si el receptor ha recuperado el mensaje. Esto, con algunos sistemas, no siempre es posible.
- **Distribución múltiple**: El emisor puede dirigir su mensaje a distintos destinatarios sin necesidad de repetir el mensaje. Un ejemplo de utilización se da cuando un departamento de la empresa envía un memorándum a los demás departamentos.
- **Respuesta automática:** El receptor puede dar respuesta al emisor sin repetir la dirección ni la cabecera del mensaje.
- **Re direccionamiento:** El receptor de un mensaje puede transmitir, a su vez, ese mensaje a otra dirección de correo simplemente introduciendo el destinatario.
- **Privacidad:** Restricción del acceso a los contenidos de los mensajes.
- **Caducidad:** Automatización del borrado de los mensajes en una fecha de caducidad del mismo (por ejemplo, borrado de los mensajes recuperados un número de días atrás).
- **Archivo:** El mensaje puede ser tratado como cualquier archivo, y por tanto es susceptible de ser almacenado, copiado, eliminado y clasificado.

2.3.5 FUNCIONAMIENTO DE UN SISTEMA DE CORREO ELECTRÓNICO

El funcionamiento del envío de correo electrónico es el siguiente:

- Se fragmentará el mensaje en pequeños paquetes de datos individuales. Cada uno de estos paquetes recibe una “etiqueta” con la dirección del destinatario.
- A través de dispositivos de comunicación (enrutadores, por ejemplo) transmiten estos paquetes por el camino más rápido al destinatario. También es posible que los paquetes lleguen al destinatario a través de caminos diferentes. Si una de las vías en Internet ya no está disponible, el Router busca un camino alternativo y envía el resto de los paquetes de datos por él.

- Una vez que todos los paquetes hayan llegado al destinatario, éstos se volverán a reunir en un solo mensaje.

En la práctica, este proceso es algo distinto. Los mensajes llegan al proveedor de servicios por la red, el cual reúne todos los mensajes destinados a una persona concreta. Si se establece una conexión con Internet, todos los mensajes personales del usuario se cargarán en su computadora.

2.4 ESTRUCTURA DE UN MENSAJE DE CORREO ELECTRÓNICO

El protocolo SMTP usa el estándar RFC 822 como formato para la creación de mensajes; en el año 2001 este RFC fue actualizado por el RFC 2822, y se basa en los elementos típicos de las cartas postales; es decir, el sobre que contiene la información del destinatario y del remitente de la carta, el contenido, que es el mensaje en sí (Barceló Ordinas, 2008, págs. 119-120).

El sobre (en la mayoría de los sitios se denomina cabecera) contiene la información necesaria para que se complete la transmisión y la entrega. El contenido es la información que va a ser entregada en el destino.

Según el RFC 822 el estándar afecta sólo al contenido del mensaje y no al sobre, si bien algunos sistemas de mensajes pueden necesitar usar información del contenido para formar el sobre, por lo que el estándar se encarga también de facilitar la adquisición de estos datos por parte de dichos programas.

El estándar especifica que los mensajes de correo electrónico están formados por dos partes siguientes:

- **La cabecera**, que recoge la información general del mensaje. Equivale al sobre de la carta postal y está formada por una serie de campos de cabecera, cada uno de los cuales incluye un tipo concreto de información. La cabecera tiene que llevar una especie de campos. Los campos básicos de la cabecera son:
  - **Remitente (De o From):** quien envía el correo, cuenta de correo electrónico del emisor del mensaje. Este campo puede ser alterado por el emisor para que aparezca otra dirección.

- **Destinatario (Para o To):** correo electrónico del destinatario es la dirección y nombre (opcional) del usuario al que va dirigido el correo; en este campo pueden aparecer varias direcciones.
- **Destinatario de copia (CC):** campo opcional que permite que enviemos correos electrónicos hasta a 256 destinatarios, separados por coma (,) o punto y coma (;) y siguiendo de espacios en blanco. Esta opción permite al remitente enviar una respuesta al emisor o a TODOS los destinatarios iniciales.
- **Destinatario de copia oculta (CCO o BCC):** dirección y nombre (opcional) del usuario al que queremos que se envíe una copia del mensaje. En este campo pueden aparecer varias direcciones o ninguna. Tiene la misma utilidad que el campo CC, solo que envía los correos a los destinatarios sin que estos puedan ver las demás direcciones. Esto es recomendable para comunicaciones de empresa, publicidad permitida, etc.
- **Responder (Reply To):** campo opcional que lleva la dirección a la queremos que nos responda. Si está vacío utiliza el campo DE, si contiene una dirección es la que se escribe al pulsar RESPONDER.
- **Fecha (Date):** en este campo se reflejan la fecha y la hora del sistema emisor del mensaje.
- **Tema (Asunto o Subject):** breve descripción o título que queremos que figure en el mensaje, y que informa al destinatario de la naturaleza de éste. Este campo se puede dejar en blanco, pero no es recomendable.

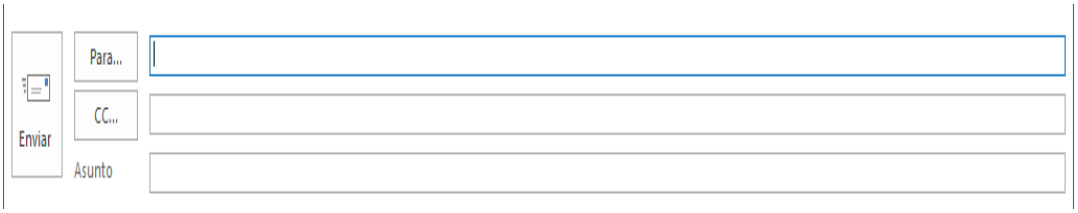


Ilustración 3 Campos de la cabecera del mensaje de correo.
Gráfico de elaboración propia.

- **El cuerpo del mensaje,** que contiene el mensaje en sí. Corresponde al contenido de la carta postal. Esta parte es opcional (Gómez Andreu, Formato de los mensajes de correo electrónico, 2010, pág. 116).

Los campos que se explican a continuación no suelen ser mostrados por defecto por los MUA o al consultar el correo desde el servidor. Para verlos suele ser necesario seleccionar opciones como encabezado completo, ver todas las cabeceras,
etc.:

- **Return-Path:** este campo es añadido por el último servidor por el que pasa el mensaje antes de ser entregado a su destino, y se usa para hallar la ruta de retorno en caso de devolución del mensaje.
- **Received:** en este campo están registrados todos los servidores por los que pasa el mensaje, por si se necesita realizar un seguimiento del mismo.
- **Message-ID:** este campo contiene un identificador que hace que el mensaje asociado a él sea único en todo Internet.
- **X-Priority:** indica la prioridad con la que el lector debe considerar al mensaje.
- **X-Mailer:** Nombre del *software* o aplicación utilizada para transferir el correo.
- **MIME-Version:** indica la versión de MIME que utiliza el mensaje. MIME son las siglas de *Multipurpose Internet Mail Extension* (Extensiones Multipropósito de Correo por Internet). Básicamente, permiten enviar información adicional junto con el texto de un correo, de manera que se pueda identificar correctamente cada uno de estos bloques de información y la naturaleza de su contenido.
- **Content-Type:** indica la naturaleza de los bytes que constituyen el contenido del mensaje para que el sistema receptor del mismo pueda tratar los datos de forma apropiada: imagen, audio, video, texto, etc.
- **Content-Transfer-Encoding:** indica el tipo de codificación que se ha usado con el mensaje, para que el sistema receptor sepa como decodificarlo. (Sergio, 2017)

Existen muchos más campos (no obligatorios en la mayoría de los casos) que forman la cabecera de un mensaje. El lector que desee conocer todas las posibilidades puede consultar el RFC 2822 y los RFC que tratan sobre MIME: RFC 2045 a 2049. (Sergio, 2017)

2.4.1 PROTOCOLOS

2.4.1.1 PROTOCOLOS DE TRANSPORTE DE CORREO (SMTP)

SMTP (Simple Mail Transfer Protocol) es el protocolo responsable de transferir los mensajes desde un servidor de correo a otro a través de redes basadas en TCP/IP. SMTP pertenece a la capa de aplicación del modelo OSI y se basa en la capa de transporte de TCP. Opera desde el puerto 25. (Es decir, las solicitudes para recibir y enviar correo electrónico pasan por el puerto 25 en el servidor SMTP) (Dean, SMTP, 2009, pág. 501).

SMTP, sirve de base para el correo electrónico a través de Internet; aunque SMTP viene con un conjunto de comandos legibles (texto) que posiblemente podrían utilizarse para transportar el correo desde una máquina a otra, este método podría ser laborioso, lento y propenso a errores. En cambio, otros servicios, tales como el software Sendmail para sistemas UNIX y Linux proporcionan interfaces de correo más amigables y sofisticados que dependen de SMTP como sus medios de transporte (Dean, SMTP, 2009, pág. 501).

SMTP es un simple subprotocolo, incapaz de hacer nada más que el transporte electrónico o mantenerlo en una cola. Siguiendo el concepto del correo postal, SMTP se basa en el almacenamiento y el reenvío. Es decir, cuando un mensaje llega a otra oficina, queda almacenado en la misma cierto tiempo antes de ser entregado a otra oficina o al destinatario final.

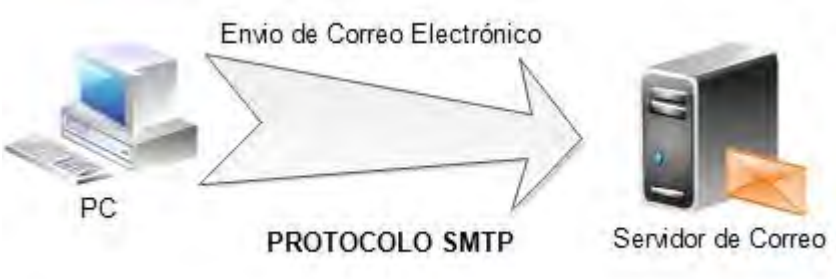


Ilustración 4 Protocolo SMTP.
Gráfico de elaboración propia.

2.4.1.2 PROTOCOLO DE OFICINA DE CORREO (POP)

Uno de los procedimientos definidos por Internet que trata sobre los mensajes de correo electrónico entrantes recae en el protocolo POP (protocolo de oficina de correo) el cual consiste en un protocolo estándar, ampliamente utilizado, que forma parte de la suite de Internet de protocolos reconocidos. POP es la forma abreviada de Post Office Protocol

POP, también llamado POP3 (tercera versión), utiliza un servidor para almacenar temporalmente los mensajes entrantes. Cuando se accede al servidor, un programa cliente descarga todos los mensajes a la computadora y los elimina de dicho servidor.

Una de las principales desventajas del protocolo de correo POP es la siguiente: una vez que descarga sus mensajes del servidor a una computadora, ya no puede descargarlos a otra computadora, es decir, solo puede descargarlos una vez a un sólo equipo. Para evitar esta limitante, se puede direccionar el correo de tal manera que descargue sus mensajes a su disco duro o a un sitio en la red para poder acceder a ellos de manera permanente (Maryann, 2001, pág. 49).

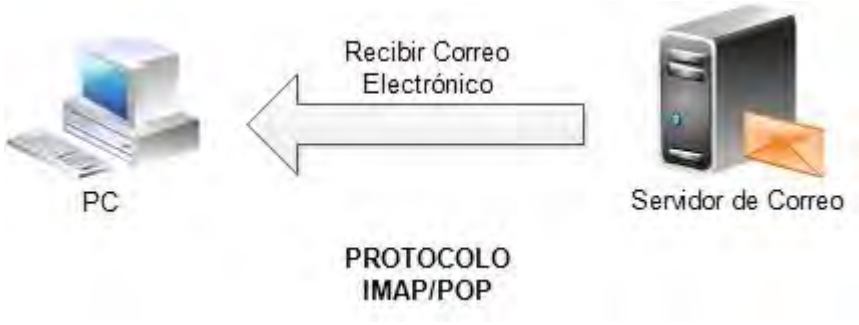


Ilustración 5 POP.
Gráfico de elaboración propia.

Ventajas del protocolo POP

- Poder utilizar un programa especializado en la gestión de correos para descargarlos al equipo y leerlos posteriormente aun sin disponer de conexión a internet.
- El servidor de correo no tiene porqué disfrutar de un amplio espacio de almacenamiento ya que todos los correos se descargan al equipo.
- Al encontrarse los correos almacenados en local es más rápido trabajar con correos electrónicos y sus archivos adjuntos.

- Es bastante sencillo instalar y configurar un servidor POP. (Saavedra Fernández T. , 2014, págs. 46-47)

2.4.1.3 PROTOCOLO DE ACCESO A MENSAJES DE INTERNET (IMAP)

Es un protocolo de recuperación de correo electrónico que se ha desarrollado como una alternativa más sofisticada para POP3. La versión más actual de IMAP es la versión 4, o IMAP4.

IMAP4 puede reemplazar POP3 sin que el usuario tenga que cambiar los programas de correo electrónico. La ventaja que tiene sobre POP3 es que los usuarios pueden almacenar los mensajes en el servidor de correo, en vez de siempre tener que descargar luego a una máquina local. Esta función beneficia a los usuarios que pueden consultar el correo desde diferentes estaciones de trabajo. Además, IMAP4 proporciona las siguientes características: los usuarios pueden recuperar la totalidad o sólo una parte de cualquier mensaje de correo, el resto se puede dejar en el servidor de correo.

Esta función beneficia a los usuarios que se trasladan de una máquina a otra, y los usuarios con conexiones lentas a la red o el espacio libre en disco duro mínimo (Dean, IMAP, 2009, págs. 502-503).

Los usuarios pueden revisar sus mensajes y eliminarlos mientras el mensaje permanezca en el servidor, la función de este servidor conserva el ancho de banda de red, especialmente cuando los mensajes son largos o cuando contienen archivos adjuntos, ya que los datos no necesitan “trasladarse” desde el servidor al cliente en la estación de trabajo. Para los usuarios con una conexión de internet lenta, borrar mensajes sin tener que descargarlos representa una gran ventaja sobre POP3.

El usuario puede crear sofisticados métodos de organizar los mensajes en el servidor, por ejemplo, construir un sistema de carpetas que contienen mensajes con contenido similar. Además, un usuario puede buscar a través de todos los mensajes para los que contienen sólo una palabra clave particular, o línea de asunto.

Los usuarios pueden compartir un buzón en una ubicación centra, por ejemplo, si varios miembros del personal de mantenimiento que utilizan diferentes estaciones de trabajo deben recibir los mismos mensajes dirigido a *"Departamento de instalaciones"*, pero no tienen una cuenta de correo electrónico para ningún otro fin, podrían entonces iniciar la sesión con el mismo ID y compartir el mismo buzón de correo en el servidor. Si POP3 se utiliza en esta situación, sólo un miembro del personal de mantenimiento podría leer el mensaje, y tendría que reenviar o copiar a sus colegas el mensaje.

Aunque IMAP4 proporciona ventajas significativas sobre POP3, también presenta algunas desventajas:

- Los servidores IMAP4 requieren más espacio de almacenamiento
- Por lo general requieren más recursos de procesamiento que los servidores POP.
- Los administradores de red deben mantener una vigilancia más estrecha sobre los servidores IMAP4 para garantizar las cuotas de almacenamiento de los usuarios.
- Si el servidor IMAP4 falla, los usuarios no pueden tener acceso al correo dejado allí (Dean, IMAP, 2009, págs. 502-503).

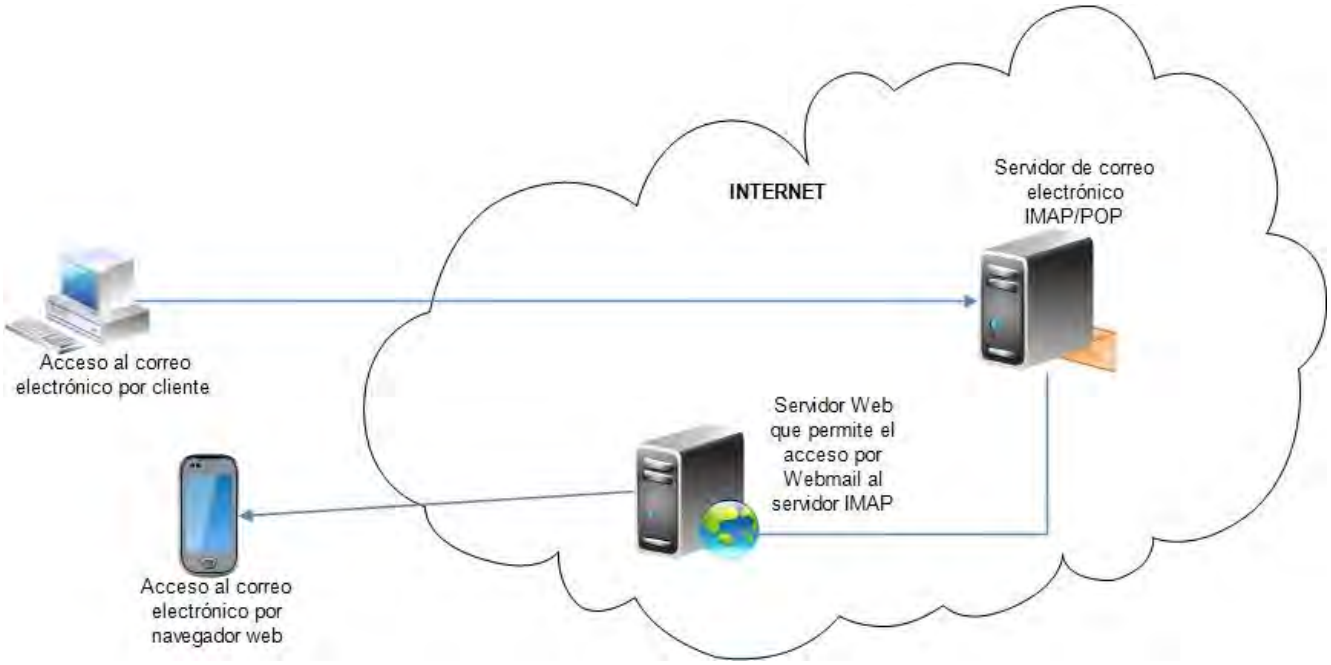


Ilustración 6 Protocolo IMAP.
Gráfico de elaboración propia.

Ventajas del protocolo IMAP

- Ofrece una comunicación bidireccional entre el servidor de correo web y el cliente de correo electrónico.

- Los correos están en todo momento en el servidor, por lo que se puede acceder a ellos desde cualquier lugar.
- Si el equipo se daña, se extravía o lo roban, los correos se encuentran seguros en el servidor.
- Acceso y gestión fácil y rápida desde cualquier equipo al disponer de sincronización bidireccional. Lo que se haga en el equipo se refleja en el servidor; por ejemplo, si se elimina del servidor; si se crea una carpeta en el equipo, se crea en el servidor. (Saavedra Fernández T. , 2014, pág. 50)

2.4.1.4 MIME (Multipurpuse Internet Mail Extensions)

MIME (Extensiones multipropósito para correo electrónico en Internet) es, actualmente, el protocolo más utilizado para enviar textos con formato no ASCII a través de Internet.

El protocolo MIME está definido en la RFC 1521 y se ha desarrollado para poder transmitir mensajes multimedia a través de las redes IP. Es pues, una ampliación de correo electrónico para la transmisión de información multimedia, que convierte en texto cualquier clase de información y que la regenera al formato original en el destino.

El correo electrónico a través de Internet constituye un mecanismo estándar para intercambiar mensajes entre millones de computadores conectados a la Red. Los estándares que sirvieron de base al correo electrónico se establecieron en 1982 y, aunque supusieron un avance significativo, actualmente están desfasados.

La aparición de elementos multimedia en los últimos años y la popularidad del correo electrónico, obligó a la creación de un nuevo estándar que permitiera mayor flexibilidad: MIME.

El nuevo estándar MIME fue creado en junio de 1992 por IETF (Internet Engineering Task Force). El objetivo de MIME es permitir a los clientes de correo electrónico enviar y recibir mensajes de texto plano y también textos con formatos y figuras, archivos ejecutables, sonidos, imágenes, etc. (Huidobro Maya, 2007, pág. 162).

El protocolo anterior a MIME, SMTP (Simple Mail Transfer Protocol), estaba limitado al juego de caracteres ASCII americano, y causaba problemas a los usuarios de otros países que necesitaban caracteres con tilde y símbolos especiales. Sin embargo, con MIME los mensajes de correo electrónico pueden contener:

- Múltiples objetos en un mensaje simple.
- Texto de longitud ilimitada.
- Conjuntos de caracteres (distintos de ASCII), permitiendo lenguajes diferentes al inglés.
- Mensajes con fuentes múltiples.
- Archivos binarios o de aplicación específicos.
- Mensajes con imágenes, audio, video y multimedia.
- Campos de encabezado.

MIME define los siguientes campos de encabezado, que son utilizados por los clientes de correo electrónico para enviar/recibir los mensajes:

- El campo de versión MIME, que especifica la versión del estándar MIME que se ha utilizado en el mensaje.
- El campo de “Content type”, que se utiliza para especificar el tipo y subtipo de los datos en el cuerpo del mensaje.
- Las aplicaciones que reciben información MIME manejan una tabla de definiciones que asocia a cada tipo MIME su nombre, las extensiones de archivos que habitualmente utilizan y la aplicación encargada de su tratamiento.

MIME es un sistema que se basa en parámetros y, por tanto, el conjunto de pares Tipo/Subtipo irán creciendo con el tiempo. Además, muchos otros campos MIME irán adquiriendo nuevos valores. Para garantizar que el desarrollo de estos valores se realiza de forma ordenada, MIME consta de un proceso de registro supervisado por el IANA (Internet Assigned Numbres Authority).

2.4.1.5 TIPOS MIME

Los tipos MIME son unas especificaciones de intercambio, a través de internet, de todo tipo de archivos (audio, video, documentos en PDF, en Word, etc.) de forma transparente para el

usuario. El correo electrónico y las páginas web nacieron en modo exclusivamente de texto, las nuevas necesidades obligaron a crear un sistema que permitiese el intercambio de todo tipo de archivos.

El correo es texto puro (en ASCII), mientras que los navegadores solo aceptan de forma nativa el texto (ASCII) y las imágenes (en formatos JPG y GIF). La evolución e internacionalización de internet han hecho que los tipos MIME sean capaces de soportar:

- Textos en caracteres no ASCII (España, Barça, Rodríguez, etc.).
- Ficheros adjuntos que no son del tipo texto.
- Cuerpos de mensajes con múltiples partes (varios megas).
- Internacionalización de las nuevas DNS.
- Los tipos MIME son una norma del IETF (Internet Engineering Task Force), y están especificados en los RFC 2045, 2046, 2047, 2077, 4288 y 4289.
- Principales tipos MIME soportados por los navegadores

Existe una lista de los tipos MIME donde se especifica los que soporta cada programa, cada navegador, cada servidor SMTP (Gómez Andreu, Tipos MIME, 2010, pág. 119).

Extensión	Tipo MIME	Aplicación
323	Text/h323	Videoconferencia
AI, PS, EPS	Application/postscript	Adobe PS
AVI	Video/x-msvideo	Video AVI
BMP	Image/bmp	Imagen BMP
CSS	Text/css	Estilos web
DOC	Application/msword	Microsoft Word
EPS	Application/postscript	Adobe PS
GIF	Image/gif	Imagen GIF
HTM, HTML	Text/html	Texto ASCII html
JPE, JPG, JPEG	Image/jpeg	Imagen JPEG
JS	Application/x-javascript	Java
MOV	Video/quicktime	Apple Video Quicktime
PPS	Application/vnd ms powerpoint	Microsoft PowerPoint
PDF	Application/pdf	Adobe Acrobat
SWF	Application/x-shockwave-flash	Flash
ZIP	Application/zip	Archivo comprimido

Tabla 2 Tipos de MIME

2.5 ELEMENTOS DEL SERVICIO DE CORREO ELECTRÓNICO

2.5.1 EL AGENTE DE USUARIO

Un agente de usuario normalmente es un programa (a veces llamado lector de correo) que acepta una variedad de comandos para redactar, recibir y contestar los mensajes, así como para manipular los buzones de correo. Algunos agentes de usuario tienen una interfaz elegante operada por menús o por iconos que requiere un ratón, mientras que otros esperan comandos de un carácter desde el teclado. Funcionalmente, ambos son iguales. Algunos sistemas son manejados por menús o por iconos, pero también tienen métodos abreviados de teclado.

2.5.2 Agente de transferencia de correo (MTA)

Agente de transferencia de correo: el MTA (Mail Transfer Agent) transfiere los mensajes de correo entre equipos mediante el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar a su destino. Los MTA son capaces de transferir correo local (en la misma máquina) y remoto (reenviarlo a otro MTA para que lo procese). Para evitar problemas de spam, el MTA debe estar correctamente configurado para prevenir dichos ataques.

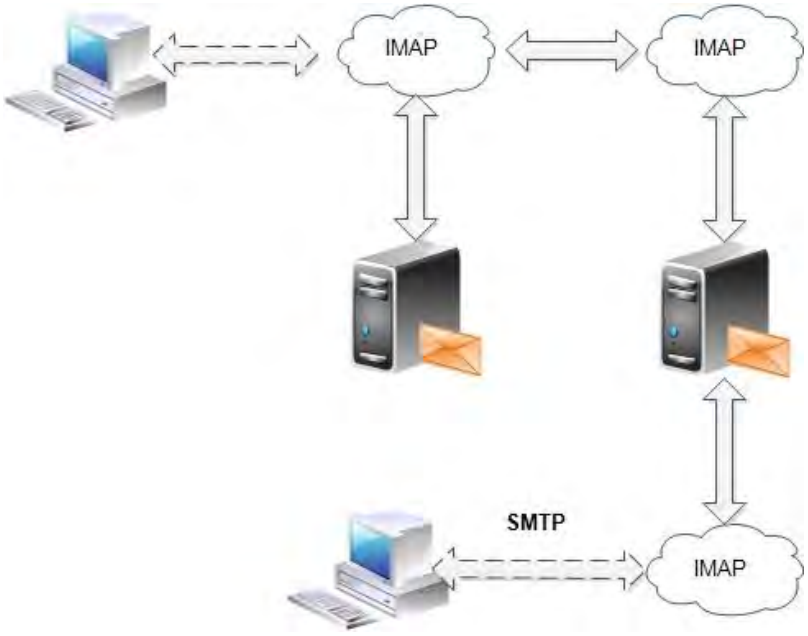


Ilustración 7 Agente MTA. Gráfico de elaboración propia.

Funciones

- Responsable del encaminamiento del correo entre dos sistemas.
- Es el que se conoce como servidor de correo.
- Gestiona la distribución de correo saliente, y está pendiente de la llegada de correo entrante desde Internet.

  Ejemplos: Sendmail, Postfix, Qmail, Exim.

2.5.3 Agente de Entrega de correo (MDA)

Agente de entrega de correo: El MTA utiliza un MDA (Mail Delivery Agent) para entregar los mensajes en el buzón del usuario correspondiente. En muchos casos el MDA es en realidad un agente de entrega local (Local Delivery Agent o LDA). Los MDA no transportan mensajes entre sistemas ni se relacionan con el usuario final, y una ventaja que ofrecen es la de poder ser utilizados para la clasificación de los mensajes antes de que el usuario los lea.

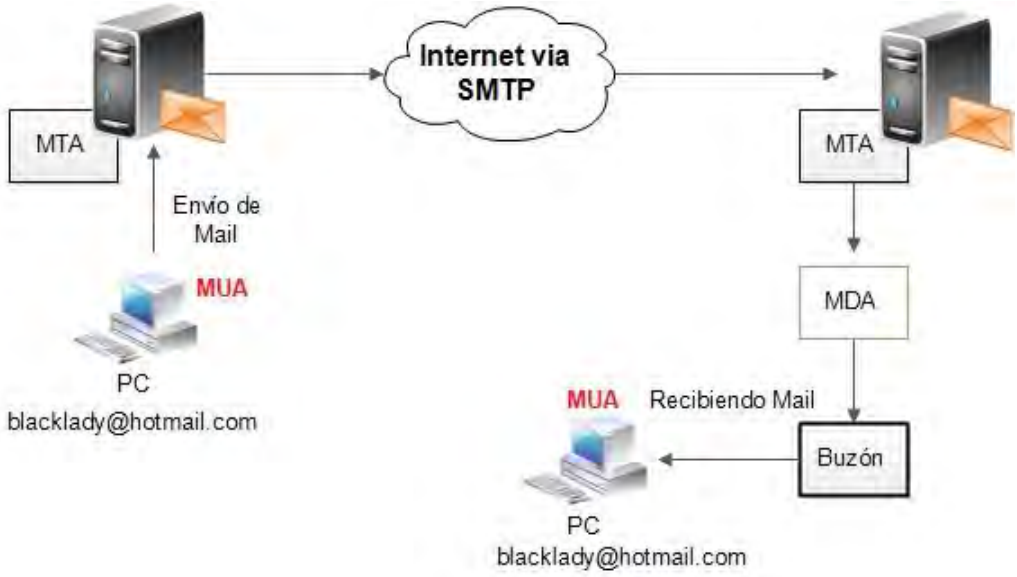


Ilustración 8 Agente MDA. Gráfico de elaboración propia.

Características

- Su función es copiar los mensajes del MTA al buzón de correo del usuario.
- No transporta mensajes entre sistemas ni es un interfaz de trabajo para el usuario.

  Ejemplos: Clientes de correo POP e IMAP.

2.5.4. Agente de Usuario de Correo (MUA)

Agente de usuario de correo: el MUA (Mail User Agent) es un programa que permite al usuario leer y crear mensajes de correo electrónico, cayendo en esta categoría la mayoría de los clientes de correo electrónico (Microsoft Outlook, Mozilla Thunderbird, Webmail,). La mayoría de los MUA actuales también permiten a los usuarios obtener los mensajes y configurar sus buzones. Los sistemas de correo electrónico tienen dos partes básicas, como hemos visto: los agentes de usuario de correo y los agentes de transferencia de correo.

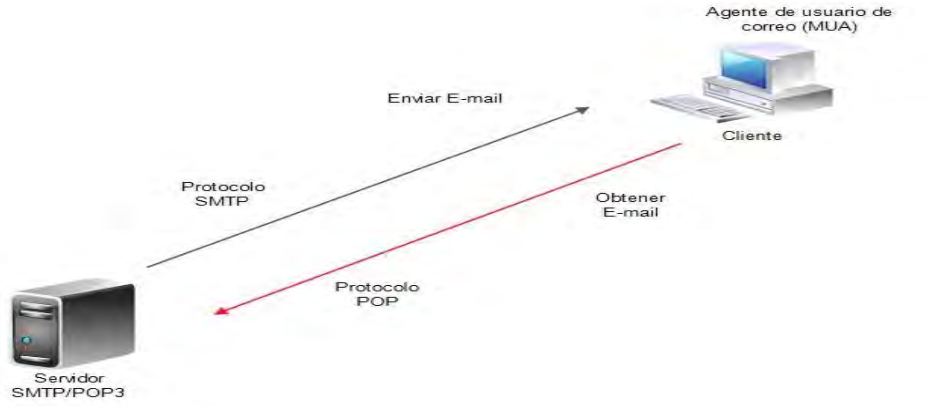


Ilustración 9 Agente MUA. Gráfico de elaboración propia.

Características

- Constituye el interfaz de usuario que le permite editar, componer, y enviar correo local. Son los llamados clientes de correo.

2.6 VULNERABILIDADES

Una vulnerabilidad es un fallo de seguridad. Puede ser flagrante y permitir a un pirata informático o hacker atacar el sistema, o ser un simple punto débil que puede ayudarle indirectamente.

Una vulnerabilidad puede entenderse también como la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos, incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información (Areitio, 2008, pág. 23).

Una vulnerabilidad, por si misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo (Areitio, 2008, pág. 23).

En los primeros años, los ataques involucraban poca sofisticación técnica. Los ataques internos se basaban en utilizar los permisos para alterar la información. Los externos se basaban en acceder a la red simplemente averiguando una clave válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar vulnerabilidades en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevaron a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automáticos,etc) (Peláez, 2002, pág. 23).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo Bruce Schneier, en numerosos artículos, ha definido y clasificado las generaciones de ataques en la red existentes a lo largo del tiempo:

La primera generación: ataque físico.

Ataques que se centraban en los componentes electrónicos: ordenadores y cables. El objetivo de los protocolos distribuidos y de la redundancia es la tolerancia frente a un punto único de fallo. Son mayormente problemas para los que actualmente se conoce la solución.

La segunda generación: ataque sintáctico (Peláez, 2002, pág. 23).

Las pasadas décadasse han caracterizado por ataques contra la lógica operativa de los ordenadores y las redes, es decir, pretenden explotar las vulnerabilidades de los programas, de los algoritmos de cifrado y de los protocolos, así como permitir la denegación del servicio prestado. En este caso se conoce el problema, y se está trabajando en encontrar soluciones cada vez más eficaces.

La tercera generación: ataque semántico.
Se basan en la manera en que los humanos asocian significado a un contenido. El hecho es que en la sociedad actual la gente tiende a creerse todo lo que lee (medios informativos, libros, la Web...). El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o *e-mails*, por ejemplo, para beneficiarse de las inversiones dentro de la bolsa financiera. También pueden llevarse a cabo modificando información caduca.

Esta generación de ataques se lleva a su extremo si se modifica el contenido de los datos de los programas de ordenador, que son incapaces de cotejar o sospechar de su veracidad, como por ejemplo la manipulación del sistema de control de tráfico aéreo, el control de un coche inteligente, la base de datos de los libros más vendidos o de índices bursátiles como el NASDAQ. Lo más curioso es que estos ataques han existido fuera del entorno informático desde hace muchos años como estadísticas manipuladas, falsos rumores..., pero es la tecnología la que potencia su difusión (Peláez, 2002, pág. 23).

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de la familia de protocolos TCP/IP (confidencialidad, integridad y disponibilidad de la información) (Peláez, 2002, pág. 25).
Los ataques pueden estar motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema, anulación de un servicio o simplemente el desafío de penetrar un sistema.

Éstos pueden provenir principalmente de dos fuentes:

- Usuarios autentificados, al menos a parte de la red, como por ejemplo empleados internos o colaboradores externos con acceso a sistemas dentro de la red de la empresa. También denominados *insiders*.
- Atacantes externos a la ubicación física de la organización, accediendo remotamente. También denominados *outsiders* (Peláez, 2002, pág. 25).

Las vulnerabilidades pueden ser permanentes, a no ser que se produzcan cambios en el activo, de forma que lo haga insensible a la vulnerabilidad. Las vulnerabilidades provocan debilidades en el sistema que pueden explotarse y dar lugar a consecuencias no deseadas.

Hay circunstancias diversas que pueden permitir que una amenaza se materialice y cause daño. Por ejemplo, la ausencia de un mecanismo de control de accesos es una vulnerabilidad que podría permitir la materialización de la amenaza de intrusión.

Dentro de un sistema u organización, pueden existir vulnerabilidades que no tengan ninguna amenaza asociada que pueda aprovecharlas. Sin embargo, como el entorno puede cambiar de forma dinámica, todas las vulnerabilidades deberían controlarse para identificar aquellas que pueden permitir la materialización de nuevas amenazas, además de las ya existentes.

La evaluación de la vulnerabilidad es el examen de las debilidades del sistema que pueden explotar las amenazas identificadas. Este análisis debe tener en cuenta el entorno y las salvaguardas existentes. Las vulnerabilidades se clasifican según sean su naturaleza (estáticas o dinámicas), el tipo de acceso (locales o remotas), su impacto (peligrosas o inocuas) y el nivel donde se localizan (físico, enlace de datos, (MAC), red, transporte o aplicación).

Las vulnerabilidades pueden clasificarse según dos criterios:

- Número de paquetes a emplear en el ataque:
  - *Atomic*: se requiere un único paquete para llevarla a cabo.
  - *Composite*: son necesarios múltiples paquetes.

- Información necesaria para llevar a cabo el ataque:
  - *Context*: se requiere únicamente información de la cabecera del protocolo.
  - *Content*: es necesario también el campo de datos o *payload*.

2.7 AMENAZAS DE SEGURIDAD

Una amenaza puede causar un incidente no deseado, que puede provocar daños o pérdidas de todo tipo en la organización. Estas pérdidas pueden proceder de un ataque directo o indirecto sobre el sistema de información, los TIC, o los procedimientos manuales. Los ataques son principalmente en forma de revelación, de destrucción, de modificación no autorizada, de indisponibilidad o de pérdida de información.

Una amenaza necesita explotar una vulnerabilidad del activo para producir un daño. Existen datos estadísticos relativos a amenazas de tipo medioambiental, como inundaciones, rayos o terremotos, que se deben utilizar en el proceso de valoración.

Una amenaza puede materializarse desde el interior de una organización, como el sabotaje de un empleado, el robo de contraseñas con un sniffer (escuchas clandestinas), mediante acceso por internet no autorizado o un DoS (denegación de servicios).

El daño causado por una amenaza puede ser temporal o permanente y se puede asociar con una escala de severidad como otros fenómenos. Por ejemplo, los terremotos son de diferente gravedad según la escala Richter, o un virus, puede causar diferentes daños según sus acciones.
Entre las características más relevantes de una amenaza se encuentran las siguientes:

- El origen, que puede ser interno o externo.
- La motivación, como son las ventajas competitivas, los beneficios económicos, etc.
- La frecuencia o periodicidad de los ataques.
- La severidad, dependiendo de si es o no irreversible.

Al tratar las amenazas, se deben considerar, además de los aspectos de contexto y ambientales, también los culturales, ya que algunas amenazas pueden no ser consideradas dañinas en algunas culturas.

Una amenaza es una condición del entorno del sistema de información (por ejemplo, persona, máquina, etc.) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Las amenazas de seguridad pueden caracterizarse modelando el sistema como un flujo de información; desde una fuente, como por ejemplo un archivo o un equipo, a un destino, como por ejemplo otro archivo o un usuario.

Las cuatro categorías generales de amenazas o ataques son los siguientes:

- **Interrupción**: un recurso del sistema es destruido o deja de estar disponible. Este es un ataque contra la disponibilidad. Un ejemplo de ataque es la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

- **Intercepción**. Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada puede ser una persona, un programa o un ordenador. Un ejemplo de este ataque es escuchar una línea para registrar los datos que circulen por la red y la copia ilícita de archivos o programas (interrupción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de unos o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- **Modificación**: una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Un ejemplo de este ataque es alterar un programa para que funcione de forma diferente, modificar el contenido de un archivo o de un mensaje transferido por red.

- **Fabricación**: un ataque contra la autenticidad es cuando una entidad no autorizada inserta objetos falsificados en el sistema. Un ejemplo de este ataque es la inserción de mensajes espurios (mensajes basura) en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

2.8 ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información de lo que está siendo transmitido. Sus objetivos son la intercepción de datos y análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en: Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

Control de las horas habituales de intercambio de datos entre las entidades de la comunicación para extraer información acerca de los periodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitarlos mediante el cifrado de las comunicaciones.

2.9 ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitidos o la creación de un falso flujo de datos, se pueden dividir en cuatro categorías:

- **Suplantación de identidad.** El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, las secuencias de autentificación pueden ser capturadas y repetidas, lo que permite a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Re actuación.** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta.

- **Modificación de mensajes.** Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de euros en la cuenta A” podría ser modificado para decir “Ingresa un millón de euros en la cuenta B”.

- **Denegación de servicio.** Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría interrumpir el servicio de una red inundándola con mensajes basura. Entre estos ataques se encuentran los de denegación de servicio que consisten en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

2.10 TIPOS DE ATAQUES

Algunos tipos de ataques se enlistan a continuación:

- **Adivinación de password:** Fuerza bruta o ataques basados en diccionarios. Fuerza bruta es una técnica que proviene originalmente de la criptografía, en especial de criptoanálisis (el arte de romper códigos o descifrar textos). Es una manera de resolver problemas mediante un algoritmo simple de programación, que se encarga de generar y de ir probando las diferentes posibilidades hasta dar con el resultado esperando o de mejor conveniencia.
- **Confianza transitiva:** Aprovechar las relaciones de confianza UNIX entre usuarios o hosts para tomar sus privilegios.

- **Explotar bugs del software:** Un ataque aprovecha los fallos del software para poder hacerse con el control de la máquina.
- **Hijacking o secuestro de sesión:** Permite a un usuario robar una conexión de otro usuario que ha sido autenticado en el sistema. El secuestro de sesión supone una intromisión en una comunicación. Para poder realizar un secuestro de sesión es necesario poder escuchar el tráfico entre los dos extremos de la sesión (sniffing). El objetivo es suplantar a uno de los extremos de la comunicación una vez realizado el proceso de autenticación para recoger, falsear o insertar información o simplemente para conseguir que termine la sesión. Afecta al nivel TCP de la red. Podemos tener una combinación de TCP Hijacking y sniffing.
- I**ngeniería social:** Un atacante convence a un usuario legítimo para que le facilite información (contraseñas, configuraciones, etc.).
- **Mensajes de control de red o enrutamiento fuente:** Se envían paquetes ICMP para hacer pasar los paquetes por un enrutador comprometido.
- **Negación de servicio:** Bloquear un determinado número de servicios para que los usuarios legítimos no los puedan usar.
- **Spam:** El Spam se puede distribuir de muchas formas, por email, por mensajería instantánea, por SMS, por VoIP, etc. (Castillo Sivianes, 2010, págs. 126-127). Se considera Spam lo siguiente:
    - Comercial: un tipo de Spam en el que nos anuncian un determinado producto. El producto que se anuncia puede ser de lo más variado: productos farmacéuticos, programas de ordenador, productos bancarios (tarjetas de crédito, reducción de deudas), venta de lotería, etc. Todos ellos provenientes de entidades que son. Cuanto menos, de dudosa legalidad (Castillo Sivianes, 2010, págs. 126-127).
    - Spam nigeriano: se conoce de esta forma (desde un punto de vista genérico, dado que no siempre proviene de ese país), al tipo de Spam en el que nos anuncian que, o bien somos los únicos herederos de una fortuna en cierto país (habitualmente africano) o que contactan con nosotros para servir de intermediarios (es decir, nosotros no somos los destinatarios de la herencia, pero nos piden <<que echemos una mano>>) (Castillo Sivianes, 2010, págs. 126-127). En general, en este caso nos suelen pedir un número de cuenta corriente

para o bien ingresarnos a la herencia o bien para que nuestra cuenta sea intermediaria de la persona que debe recibir la herencia (nos dicen que nos darán una suculenta comisión). Evidentemente, se trata de una trampa para hacerse con nuestro número de cuenta o peor aún. Podría tratarse de algún tipo de blanqueo de dinero (Castillo Sivianes, 2010, págs. 126-127).

- **Malware:** El termino malware abreviatura de software malicioso, se usa como comodín para para describir varias amenazas maliciosas como virus, gusanos, etc. Los malware posiblemente presentan la mayor amenaza para la seguridad a los usuarios informáticos.
- **Virus**: Un virus es un código malicioso que se reproduce. Se descubren virus nuevos a diario. Algunos existen simplemente para duplicarse ellos mismos. Otros pueden hacer mucho daño, como por ejemplo borrar archivos o incluso inutilizar por completo el ordenador (Caprani, 2006, pág. 166).
- **Gusano**: Un gusano es parecido a un virus. Se duplican como los virus, pero no modifican archivos como lo hacen los virus. La principal diferencia es que los gusanos viven en la memoria y, normalmente permanecen inadvertidos mientras que el porcentaje de duplicaciones reduce los recursos del sistema hasta el punto en el que se hace evidente.
- **Los Caballos de Troya:** El caballo de Troya le debe el nombre a la historia del caballo de troyano en la leyenda griega. Es un programa malicioso disfrazado de aplicación normal. Los programas caballo de Troya no se duplican como lo hacen los virus, pero se pueden propagar como adjuntos a un virus (Royer, 2004, págs. 19-20).
- **Hoax**: tan “popular” como el Phishing o el Spam, un hoax no es más que un correo electrónico en el que se avisa de la existencia de virus (naturalmente falso) de efectos devastadores contra los cuales no existen ningún antivirus que los pueda detectar.
- Las alarmas falsas (Hoax): son falsos avisos o mensajes de alarma difundidos por internautas que piensan que son auténticos. Esta información puede hacer que el usuario efectué operaciones más o menos peligrosas.
- **Spoofing:** Un ataque de Spoofing consiste en suplantar validadores, credenciales o identificadores estáticos, es decir, parámetros que permanecen invariables antes, durante y después de la concesión de un privilegio, una autentificación, etc… Los identificadores que se pueden suplantar mediante un ataque de Spoofing. Para

recopilar la información necesaria para hacer la suplantación de identificadores es necesaria una fase previa en la que se emplee algún tipo de ataque pasivo. Con este tipo de ataques, en concreto, el atacante puede, mediante la falsificación de información suplantar la identidad de algún usuario de la red WLAN (Abreu, 2006, pág. 38).

- **Detectores (sniffers)**: Se llaman detectores (sniffers) los programas que permiten la captura y la grabación de la información que circula por una red. Su funcionamiento se basa en la activación del modo promiscuo de las interfaces de red de las estaciones de trabajo podrá monitorizar, además de los paquetes de información que se dirige de una manera explícita, el transito entero de la red. Esto incluye, por ejemplo, la captura de nombres de usuario y contraseñas, o incluso la intercepción de correos electrónicos (o cualquier otro documento confidencial). La actividad de los detectores es difícilmente detectable porque no quedan huellas en ningún sitio. No podemos tener constancia de la información que puede haber sido interceptada por la acción de los detectores (sino es de manera indirecta, por medio de los ataques que puede padecer el sistema informático).
- **Sniffing:** Un ataque realmente efectivo, ya que permite la obtención de gran cantidad de información sensible enviada sin encriptar, como por ejemplo usuarios, direcciones de e-mail, claves, números de tarjetas de crédito. El Sniffing consiste en emplear Sniffers u olfateadores en entornos de red basados en difusión, como por ejemplo Ethernet (mediante el uso de concentradores o Hubs). El análisis de la información trasmitida permite a su vez extraer relaciones y topologías de las redes y organizaciones. Los Sniffers operan activando una de las interfaces de red del sistema en modo promiscuo. En este modo de configuración, el Sniffers almacenará en un log todo el tráfico que circule por la tarjeta de red, ya sea destinado o generado por el propio sistema o desde/hacia cualquiera de los sistemas existentes en el entorno de red compartido (segmento Ethernet). Asimismo, pueden ser instalados tanto en sistemas como en dispositivos de red. La efectividad de esta técnica se basa en tener acceso (habitualmente es necesario además disponer de dicho acceso como administrador o root) a un sistema interno de la red; por tanto, no puede ser llevado a cabo desde el exterior. Antes de la instalación de un Sniffers, normalmente se instalarán versiones modificadas (Trojanos) de comandos como “ps” o “netstat” en entornos (Unix) para evitar que las tareas ejecutadas en el Sniffers sean descubiertas.

- **Eavesdropping:** Es una variante del Sniffing caracterizada porque únicamente contempla la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la misma.
- **Phishing** El termino Phishing, en informática, denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas, etcétera, de manera fraudulenta. El accionar del phisher (los estafadores que utilizan esta técnica) es simple, ya que se hace pasar por una persona o entidad de confianza (por correo electrónico, SMS, mensajería instantánea o páginas web) imitando el formato, el lenguaje y la imagen de entidades bancarias o también corporaciones financieras (Pacheco, 2012, págs. 300-301). En todos los casos, la comunicación simula ser oficial y suelen pedir algún tipo de dato de accesos o información relevante alegando motivos diversos, como verificación de movimientos, cambio de políticas y posible fraude, entre otras acciones. El termino deriva de la palabra inglesa fishing (pesca), haciendo referencia en este caso al hecho de pescar contraseñas e información de usuarios. La primera mención del término data de enero de 1996 en un grupo de noticias de hackers, aunque apareció tempranamente en la edición impresa del boletín de noticias 2600 Magazine y, luego fue adoptado por crackers que intentaban obtener cuentas de miembros de grandes proveedores de Internet (Pacheco, 2012, págs. 300-301).
- **Spyware:** Aunque mucha gente llama tanto a los adware como a los spyware “spyware”, hay una diferencia. Adware es técnicamente legal, aunque no siempre éticamente correcto, y algunas veces así lo es, con lo que probablemente haya estado de acuerdo en instalar en su sistema sin darse cuenta. El spyware, por el contrario, es más una forma de adware converso o sigiloso. En realidad, muchas aplicaciones spyware están más cerca de ser programas troyanos que adware reales, debido al hecho de que vienen disfrazados como algo más y se instalan sin su consentimiento.
- **Adware:** El adware es un software que se utiliza para generar anuncios, de ahí el nombre. Los adware tienden a entrar en esa zona gris ética y detenerse antes de cruzar la línea.

2.11 SISTEMAS SEGUROS DE CORREO ELECTRÓNICO

El correo electrónico es uno de los sistemas telemáticos más vulnerables a los ataques a la seguridad, actualmente el correo electrónico es muy importante a nivel profesional y la herramienta que se ha desarrollado más rápidamente en internet, pero durante muchos años la parte pendiente ha sido la seguridad con sus cuatro formas: confidencialidad, integridad, autenticación y firmas.

Cuando un usuario envía un mensaje, pierde el control sobre él, es decir, su contenido puede ser leído por cualquiera que lo manipule hasta llegar a su destino.
Se define como correo seguro, aquel que garantiza los siguientes aspectos:

- Confidencialidad
- Autenticación
- Integridad
- No repudio

Algunos conceptos importantes relativos al correo seguro son:

- Autoridad de Certificación (CA)
- Certificado Digital
- Certificado raíz

2.12 ALTERNATIVAS PARA E-MAIL SEGUROS

Los servicios de seguridad pueden ser agregados a cada enlace de comunicación a lo largo de una trayectoria dada, o pueden ser integrados alrededor de los datos que están siendo enviados, siendo esto independiente de los mecanismos de comunicación, este enfoque avanzado es frecuentemente llamado seguridad “nodo-a-nodo”.

Las dos características de este tipo de seguridad son privacidad (donde el recipiente deseado sólo puede leer el mensaje) y la autentificación (en el otro caso, el recipiente puede asegurar la identidad del emisor). La capacidad técnica de estas funciones es bien conocida desde hace tiempo, sin embargo, recientemente ha sido sólo aplicada al correo electrónico.

Es usual que se cuente con un mecanismo de autentificación de quien origina el mensaje y privacidad para los datos. Además, de proveer un esquema de recepción firmada desde el

recipiente. El núcleo de estas capacidades en el uso de tecnología de llave pública y el uso a gran escala de llaves públicas, lo que requiere un método de certificación que dada una llave pertenece a un usuario dado.

Aunque, se ofrecen servicios parecidos al usuario final, los dos protocolos tienen formatos distintos. Adicionalmente, y esto es importante a los usuarios corporativos, en este caso se cuenta con diversos formatos distintos para los usuarios corporativos, en este caso se cuenta con diversos f7ormatos para los certificados. Lo que significa, que no solo los usuarios pueden comunicarse con los que usen otro, además, no pueden compartir los certificados de autenticación. La diferencia entre los dos protocolos es parecida entre los formatos GIF y JPEG, siendo que hacen las mismas cosas, mas no su formato entre ellos.
Existen dos propuestas principales para ofrecer los servicios de seguridad que hemos mencionado: S/MIME y PGP. Otros protocolos han sido propuestos en el pasado son PEM y MOSS, no han tenido mayor presencia. Sin embargo, ahora diversos proveedores de servidores de correo-e, incluyen en sus productos a S/MIME, PGP/MIME y OPenPGP que son versiones del protocolo PGP utilizadas para correo.

2.13 CRIPTOGRAFÍA

La criptografía proporciona métodos y técnicas para observar aspectos de seguridad en el servicio de correo electrónico. La criptografía comprende toda una familia de tecnologías que incluyen las siguientes:

- **Cifrado.** Transforma la información en una forma no legible asegurando la privacidad.
- **Descifrado.** Es el inverso de la encriptación; es decir, transforma la información encriptada a su forma original legible.
- **Autentificación.** Identifica a una entidad como un individuo, una máquina en la red o una organización.
- **Firmas digitales.** La relación de un documento con el dueño de una “llave” particular siendo el equivalente a la firma de un documento.
- **Verificación de firmas.** Es lo contrario de la firma digital; verifica que una firma en particular sea válida.
- **Llave simétrica o secreta**. Utiliza una misma llave para encriptar y des encriptar la información enviada a través de la red; pero el problema que se presenta es que tanto quien envía como quien recibe la información deben tener la misma llave asegurándose que nadie más pueda obtenerla porque si intercepta la información pudiera des encriptarla y leerla fácilmente.

- **Llave asimétrica o pública.** Fue inventada en 1976 por Whitfield Diffie and Martin Hellman para resolver el problema presentado por la llave simétrica. Es un método de transmisión de información en donde el que recibe la información puede estar seguro de la identidad de quien la envió. La idea básica de este método es el uso de un par de llaves:
    - Llave privada. Solamente su dueño la conoce y se usa para des encriptar la información enviada por otras personas.
    - Llave pública. Esta se publica y se usa por cualquier persona para encriptar la información antes de enviarla a su destino (dueño).

El par de llaves se genera simultáneamente, usando algoritmos especiales en donde los mensajes que se encriptan con la llave pública de una persona puedan ser des encriptados solamente con la llave privada de esa misma persona y viceversa. Por lo tanto, para establecer una comunicación segura ya no es necesario compartir primeramente una llave privada.

Por ejemplo, si un cliente deseara enviar información segura a un servidor, el servidor daría su llave pública (por correo electrónico) y el cliente haría lo siguiente:

a) Cifra la información usando la llave pública del servidor y luego se la envía.
b) El servidor recibiría la información y la descifraría usando su llave privada.

Esta transmisión es segura en el sentido de que nadie más que reciba la información podrá leerla porque no sabe el valor de la llave privada. Existe un problema que reside en el hecho de que la llave pública no puede ser verificada. Cómo sé que la llave pública realmente es suya y no una llave pública generada por algún impostor que desee interceptar sus mensajes. Este problema es más serio cuando es usado para verificar automáticamente la comunicación entre dos “hosts”, tales como un cliente (“browser”) y un servidor (DNS dinámico). Aquí es donde intervienen los certificados.

2.14 FIRMAS DIGITALES

El paradigma de firmas electrónicas (también llamadas firmas digitales) es un proceso que hace posible garantizar la autenticidad del remitente (función de autenticación) y verificar la integridad del mensaje recibido. Las firmas electrónicas también poseen una función de

reconocimiento de autoría, es decir, hacen posible garantizar que el remitente ha enviado verdaderamente el mensaje.

2.15 FUNCIÓN HASH

Una función hash es una función que hace posible obtener un hash (también llamado resumen de mensaje) de un texto, es decir, obtener una serie moderadamente corta de caracteres que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano (esto significa que la mínima modificación del documento causará una modificación en el hash). Además, debe ser una función unidireccional para que el mensaje original no pueda ser recuperado a partir del hash. Si existiera una forma de encontrar el texto plano desde el hash, Se diría que la función hash presenta una "trapdoor".

Como tal, puede decirse que la función hash representa la huella digital de un documento. Los algoritmos hash más utilizados son:

- **MD5** (MD que significa Message Digest; en castellano, Resumen de mensaje), el MD5 crea, a partir de un texto cuyo tamaño es elegido al azar, una huella digital de 128 bits procesándola en bloques de 512 bits. Es común observar documentos descargados de Internet que vienen acompañados por archivos MD5: este es el hash del documento que hace posible verificar su integridad.
- **SHA** (Secure Hash Algorithm; en castellano, Algoritmo Hash Seguro) crea una huella digital que tiene 160 bits de longitud. SHA-1 es una versión mejorada de SHA que data de 1994. Produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 264 bits y los procesa en bloques de 512 bits.

2.16 VERIFICACIÓN DE LA INTEGRIDAD

Al enviar un mensaje junto con su hash, es posible garantizar la integridad de dicho mensaje, es decir, el destinatario puede estar seguro de que el mensaje no ha sido alterado (intencionalmente o por casualidad) durante la comunicación. Cuando un destinatario recibe un mensaje simplemente debe calcular el hash del mensaje recibido y compararlo con el hash

que acompaña el documento. Si se falsificara el mensaje (o el hash) durante la comunicación, las dos huellas digitales no coincidirían.

Sellado de datos. Al utilizar una función hash se puede verificar que la huella digital corresponde al mensaje recibido, pero nada puede probar que el mensaje haya sido enviado por la persona que afirma ser el remitente. Para garantizar la autenticidad del mensaje, el remitente simplemente debe cifrar (generalmente decimos firmar) el hash utilizando su clave privada (el hash firmado se denomina sello) y enviar el sello al destinatario. Al recibir el mensaje, el destinatario deberá descifrar el sello con la clave pública del remitente, luego deberá comparar el hash obtenido con la función hash del hash recibido como adjunto. Esta función de creación de sellos se llama sellado.

2.17 AUTORIDAD CERTIFICADORA (CA)

Una Autoridad Certificadora es la encargada de confirmar que el dueño de un certificado es realmente la persona que dice ser. Una Autoridad Certificadora puede definir las políticas especificando cuáles campos del Nombre Distintivo son opcionales y cuáles requeridos.

También puede especificar requerimientos en el contenido de los campos. Existen varias Autoridades Certificadoras, puede que una autoridad certificadora certifique o verifique la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo, por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma.

Las Autoridades Certificadoras (o notarios electrónicos) deben ser entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, certificando con su propia firma la identidad del usuario. Por lo tanto, si se desea establecer una Autoridad Certificadora, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento.

Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada. No podemos olvidar que la Autoridad Certificadora es la responsable, en última

instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su negocio en la credibilidad que inspire en sus potenciales clientes.

Una Autoridad Certificadora con autentificaciones erróneas no tendrá más remedio que cerrar ya que los usuarios no considerarán sus certificados de la suficiente calidad. Las Autoridades Certificadoras no solamente ofrecen certificados, sino también los manejan; es decir, determinan cuánto tiempo van a ser válidos y mantienen listas de certificados que ya no son válidos (Listas de Revocación de Certificados o CRLs). Por ejemplo, si un empleado posee un certificado para una compañía y el empleado sale de la compañía, no solamente con el certificado se indica que ya no existe, sino que se tiene que registrar por medio del CRL para que dicho certificado que ya había sido utilizado quede invalidado y no pueda ser utilizado posteriormente.

Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. [http://www.verisign.com]
- Thawte Certification. [http://www.thawte.com]
- Xcert Sentry CA. [http://www.xcert.com]
- Entrust. [http://www.entrust.net]
- Cybertrust. [http://www.baltimore.com]

Estas compañías proveen los servicios de:

- Verificación de solicitud de Certificados.
- Procesamiento de solicitud de Certificados.
- Firma, asignación y manejo de Certificados.

2.18 CONTENIDO DE UN CERTIFICADO

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma del ITU-T X.509, la cual forma parte del servicio de directorio diseñado por ISO (International Organization for Standardization, Organización Internacional de Estandarización) para el modelo OSI (Open System Interconnection, Interconexión de Sistemas Abiertos).

Un certificado X.509 es típicamente un archivo pequeño que contiene la información mostrada a continuación:

- **Nombre Distintivo de la entidad.** Incluye la información de identificación (el nombre distintivo) y la llave pública.
- **Nombre Distintivo de la Autoridad Certificadora.** Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado.
- **Período de Validez.** El período de tiempo durante el cual el certificado es válido.
- **Información adicional.** Puede contener información administrativa de la CA como un número de serie o versión.

El Nombre Distintivo de la entidad se usa para proveer una identidad en un contexto específico de acuerdo a las necesidades de la aplicación. Los Nombres Distintivos están definidos en el estándar X.509, así como por las necesidades de la aplicación.

2.19 FUNCIONALIDAD DE LOS CERTIFICADOS

Los certificados se ofrecen por parte de una Autoridad Certificadora a la solicitud de una persona, entidad u organización que así lo requiera. Enviar información encriptado usando la verificación de certificados:

a) Se envía un mensaje pidiendo su certificado.
b) Usted regresa su certificado.
c) Se verifica con la Autoridad Certificadora que su certificado sea válido. Especialmente, que dicha Autoridad Certificadora fue quien le dio el certificado y que su llave pública es la misma que la de certificado.
d) Se recibe la confirmación de la Autoridad Certificadora que el certificado es válido. La información se encripta usando su llave pública y luego es enviada. Usted recibe la información y la des encripta usando su llave privada.

CAPÍTULO 3 HERRAMIENTAS DE INFORMÁTICA FORENSE DE CÓDIGO ABIERTO PARA EL RASTREO DE CORREOS ELECTRÓNICOS

3.1 HERRAMIENTAS DE CÓDIGO ABIERTO PARA EL RAESTRO DE CORREOS ELECTRÓNICOS

3.1.1 IPNETINFO

IPNetInfo es una herramienta que te permite encontrar fácilmente toda la información disponible sobre una dirección IP: El propietario de la dirección IP, el nombre del país / estado, rango de direcciones IP, información de contacto (dirección, teléfono, fax y correo electrónico), y más.

Esta herramienta puede ser muy útil para encontrar el origen de correo no solicitado. Simplemente se copia los encabezados de los mensajes de su software de correo electrónico y pegarlos en la herramienta IPNetInfo. IPNetInfo extrae automáticamente todas las direcciones IP de los encabezados de los mensajes, y muestra la información acerca de estas direcciones IP.

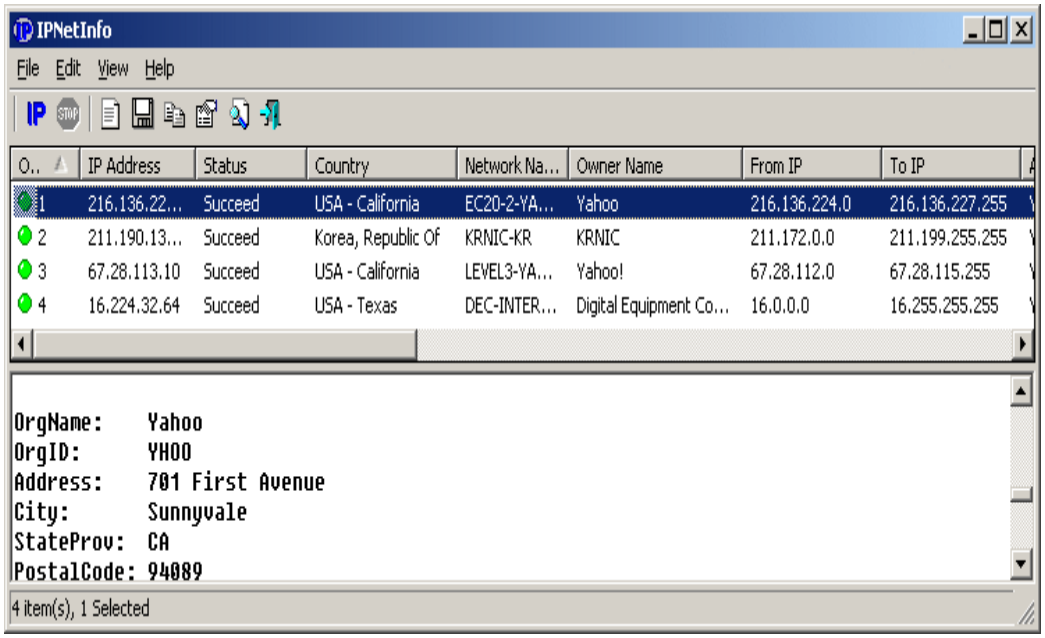


Ilustración 10 Pantalla de herramienta IPNetInfo. Fuente. Copyright (c) 2004 - 2017 Nir Sofer

Funcionamiento de IPNetInfo

La información de la dirección IP se recupera mediante el envío de una petición al servidor whois de **ARIN** . Si **ARIN** no obtiene la información acerca de la dirección IP solicitada, hace una segunda solicitud, se envía al servidor whois de **RIPE** , **APNIC , LACNIC** y **AfriNIC** . Después de que la información de la dirección IP se recupera, IPNetInfo analiza el registro Whois y lo muestra en una tabla.

Usando IPNetInfo

IPNetInfo es un programa independiente, por lo que no requiere ningún proceso de instalación o DLLs adicionales. Para comenzar a usarlo, solo se copia el archivo ejecutable (ipnetinfo.exe) a cualquier carpeta que se desee, y ejecutarlo.

Cuando se ejecuta IPNetInfo, la lista "Elija las direcciones IP" aparece la ventana. Se tiene que escribir una o más direcciones IP separadas por caracteres de coma, espacio o CRLF. Si se requiere encontrar el origen del mensaje de correo electrónico que se recibió, se copia el encabezado completo del mensaje al portapapeles, y luego se da clic en el botón "Pegar". También puede utilizar las siguientes opciones avanzadas:

- **Resolución de direcciones IP:** esta opción convierte todas las direcciones IP en el nombre del host. Una vez que se obtenga el nombre del host se muestra en la columna "Nombre Resuelto".
- **Convertir los nombres de host a direcciones IP:** esta opción convierte los nombres de host a direcciones IP. Esta opción se puede utilizar si se desea saber a quién pertenece la dirección IP de algún sitio web en específico.
- No debe seleccionar esta opción para los encabezados de los mensajes.
- Cargue sólo la última dirección IP: En la mayoría de los mensajes de correo electrónico, la última dirección IP en los encabezados de los mensajes es la dirección del equipo que envió el mensaje. Así que, si usted selecciona esta opción para cabeceras de los mensajes, obtendrá la dirección IP deseada en la mayoría de los casos (pero no en todos ellos). Sin embargo, para encontrar el origen de correo no solicitado, no se recomienda utilizar esta opción, ya que muchos spammers agregar encabezados falsos y las direcciones IP con el fin de engañar al usuario que trate de localizar. Al intentar

determinar el origen de correo no solicitado, usted debe examinar todas las direcciones IP que aparecen en los encabezados de los mensajes.

Después de seleccionar las opciones deseadas y las direcciones IP, haga clic en el botón 'OK' para iniciar la recuperación de la información de direcciones IP.

Después de recuperar los datos, el panel superior muestra un buen resumen de todas las direcciones IP que usted ha solicitado, incluyendo el nombre del propietario, país, nombre de la red, el rango de direcciones IP, información de contacto, y mucho más. Usted puede ver este resumen en el navegador como un informe HTML, copiar en el portapapeles, o guardarlo como texto / HTML / XML archivo.

Al hacer clic en un elemento en particular en el panel superior, el panel inferior muestra el original de registro WHOIS. Puede copiar los registros originales de WHOIS en el portapapeles, o guardarlos en archivo de texto mediante el uso de "Guardar registros Whois" opción.

El programa tiene unas ciertas limitaciones, ya que sobre aquellos rangos de IPs que son privadas no va a proporcionar ningún tipo de información. Los rangos de IPs privadas actuales son:

- 10.0.0.0 – 10.255.255.255.255
- 127.0.0.0 – 127-255.255.255
- 169.254.0.0 – 169.254.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255
- 224.0.0.0 – 239.255.255.255

3.1.2 EMAILTRACKERPRO

EmailtrackerPro es una herramienta capaz de rastrear un correo electrónico utilizando el encabezado de este al mismo tiempo que, previene de spam, virus, phishing, etc. mediante

un avanzado filtro de correo que analiza los mensajes. La mayoría de las veces la dirección del correo spam viene camuflada en el encabezado, EmailtrackerPro realiza un seguimiento del emisor esto es identificando el país de procedencia de quien lo ha enviado, la dirección de correo y como consecuencia, identificar la IP o sitio web responsable de esos correos por lo que se podrá informar de un abuso al proveedor del servidor del correo emisor.

Pros

- EmailtrackerPro analiza las rutas de mensajes de correo electrónico para localizar sus remitentes.
- EmailtrackerPro integra su funcionalidad con Outlook y Outlook Express que permite acceder fácilmente al origen geográfico.
- Puede enviar las quejas de spam de los ISP del spammers cómodamente.

Contras

- EmailtrackerPro es rígido en su análisis de cabecera e identifica tanto de correo como correo no deseado potencialmente.
- Usando EmailtrackerPro puede ser un poco engorroso.

Características generales

- Seguimiento del correo electrónico mediante el encabezado.
- Mapa mundial para la identificación de su procedencia.
- Red de datos de Whois "identifica los datos del emisor".
- Data Domain Whois "identifica los detalles de contacto del dominio que se emplea"
- Denuncia los abusos.
- Identifica la IP del remitente.
- Detecta los redireccionamientos "las manipulaciones ocultas que se emplean para ocultar la ubicación del remitente".
- Plugin para Outlook "2003, 2007 y 2013".
- Filtro Spam que analizará los correos entrantes y te alerta antes de que llegue a tu correo.
- Lista blanca y negra.
- Personalización de filtros.

- DNS Blacklist "Una lista global de las direcciones ip de los spammers más activos que te ayudará a identificar si eres víctima de alguno de ellos".

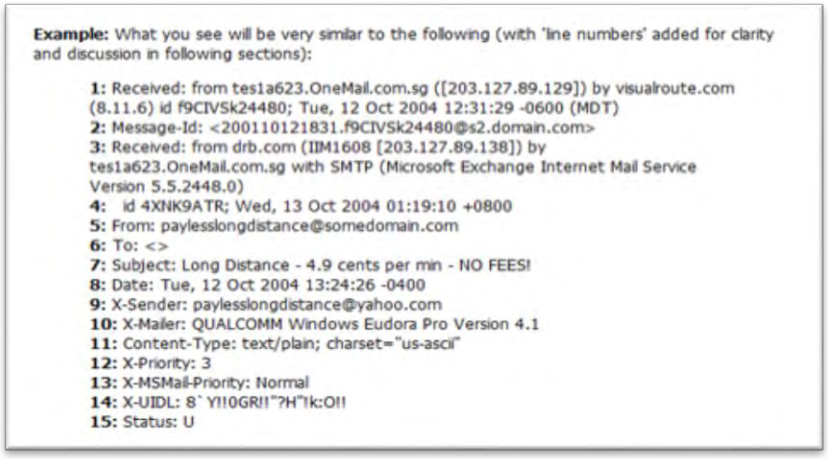
Ilustración 11 EmailtrackerPro.

Fuente. Autor

Características Principales

- **Rastrear un correo electrónico usando la cabecera**

La 'Cabecera' de un correo electrónico contiene toda la información necesaria para realizar un seguimiento de dónde vino. Se mantiene la huella de cada servidor de correo electrónico a través del cual viajó en casi todos los casos nos lleva de nuevo a la ciudad / pueblo donde se originó el correo electrónico.


Example: What you see will be very similar to the following (with 'line numbers' added for clarity and discussion in following sections):

1: Received: from tes1a623.OneMail.com.sg ([203.127.89.129]) by visualroute.com (8.11.6) id f9CIVSk24480; Tue, 12 Oct 2004 12:31:29 -0600 (MDT)
2: Message-Id: <200110121831.f9CIVSk24480@s2.domain.com>
3: Received: from drb.com (IIM1608 [203.127.89.138]) by tes1a623.OneMail.com.sg with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
4: id 4XNK9ATR; Wed, 13 Oct 2004 01:19:10 +0800
5: From: paylesslongdistance@somedomain.com
6: To: <>
7: Subject: Long Distance - 4.9 cents per min - NO FEES!
8: Date: Tue, 12 Oct 2004 13:24:26 -0400
9: X-Sender: paylesslongdistance@yahoo.com
10: X-Mailer: QUALCOMM Windows Eudora Pro Version 4.1
11: Content-Type: text/plain; charset="us-ascii"
12: X-Priority: 3
13: X-MSMail-Priority: Normal
14: X-UIDL: 8` Y!!0GR!!"?H"!k:O!!
15: Status: U

Ilustración 12 Ejemplo de Cabecera de correo electrónico.

Fuente. Autor.

- **Reporte de Abuso**

El reporte de abuso es una característica útil para los usuarios que quieren adoptar un enfoque más proactivo para tratar con el spam; proveedores de correo electrónico, como Hotmail y Yahoo!, tienen departamentos enteros establecidos para lidiar con el problema del spam.

EmailtrackerPro proporciona una plataforma que genera automáticamente un informe de abuso y se abre un nuevo correo electrónico (puede no funcionar para todos los clientes de correo electrónico) con la "a" dirección de lleno a la dirección de correo no deseado de correo electrónico detectada (como se muestra a la derecha).

Una vez que el informe de abuso ha sido enviado al proveedor de correo electrónico a continuación, es a ellos a tomar los pasos siguientes para cerrar la cuenta abajo.

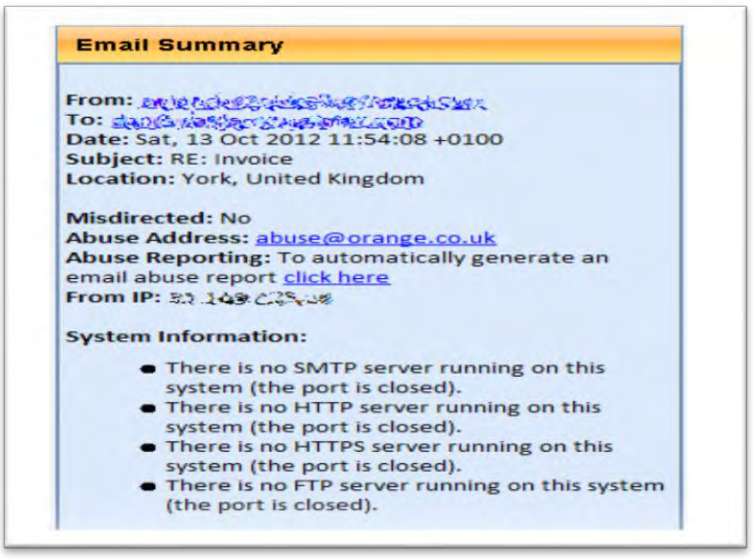


Ilustración 13 Ejemplo de Reporte de Abuso.

Fuente. Autor.

- **Filtro de spam**

la función de filtro de spam de EmailtrackerPro y detener el spam antes de que llegue a su bandeja de entrada.

El proceso es muy simple:

1. Introduzca los valores de POP para su servidor de correo electrónico en EmailtrackerPro.
2. Haga clic en el botón de correo reciben.
3. Cada correo electrónico que se recibe será remontado a recoger en las técnicas de spam.
4. Una vez que el proceso ha terminado, simplemente marcar todo el correo electrónico que no son legítimos para su eliminación y haga clic en limpio
5. se eliminarán todos esos mensajes de correo electrónico.

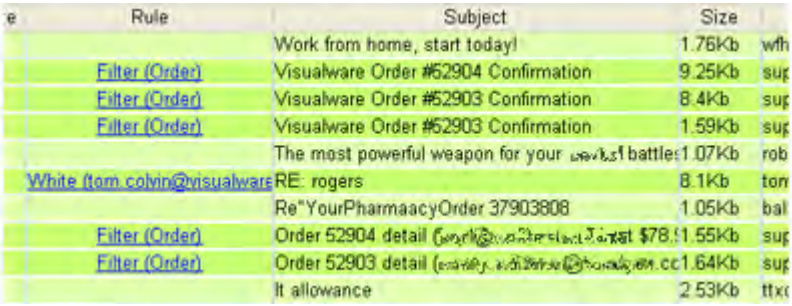


Ilustración 14 Ejemplo Filtro de Spam.

Fuente Autor.

3.1.3 TRACE EMAIL

Esta herramienta se encuentra en un sitio web la cual ayuda a determinar la dirección IP de origen de un correo electrónico basado en una de las cabeceras del correo electrónico. También muestra la ubicación aproximada en un mapa. Funciona mediante el examen de la cabecera que es una parte de los mensajes electrónicos recibidos para encontrar la dirección IP.

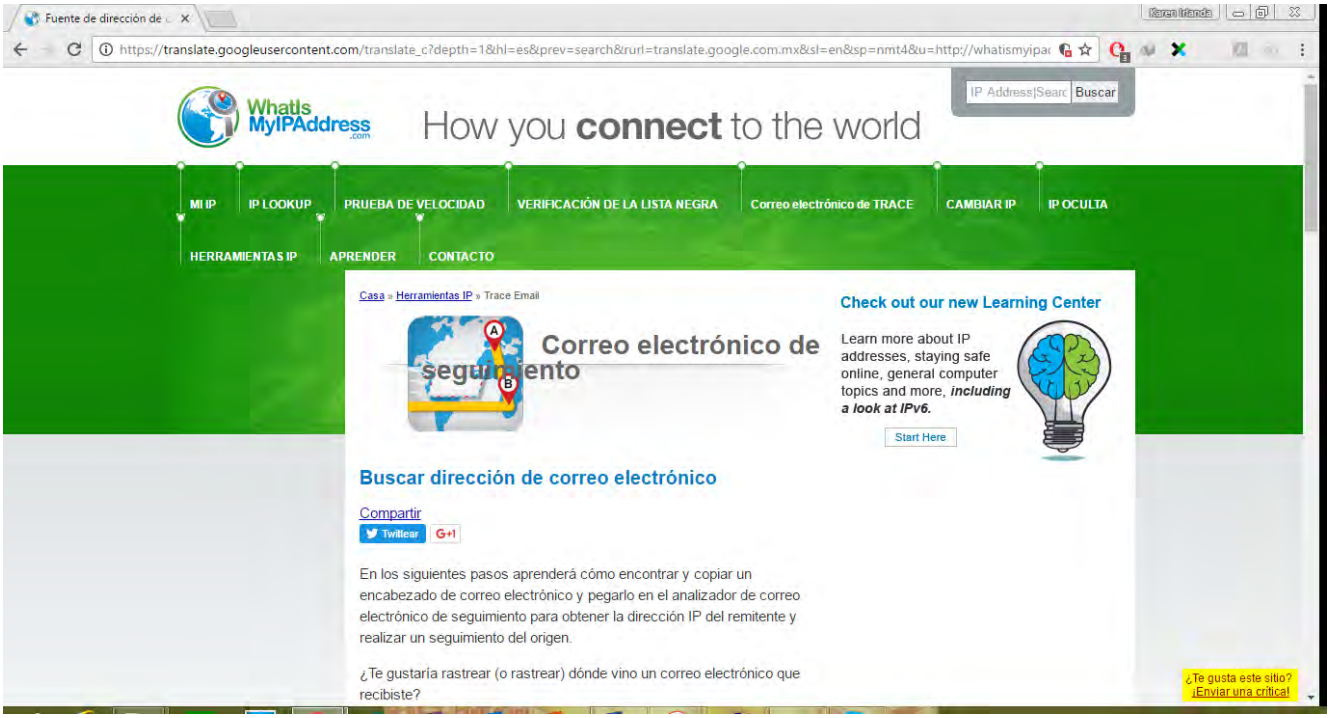


Ilustración 15 Sitio web Trace Email.

Fuente: Autor

3.1.4 EMAILTRACER

Es una herramienta para rastrear la identidad del remitente de correo electrónico. Se analiza la cabecera del correo y le da los detalles completos del remitente como dirección IP, que es el punto clave para encontrar al culpable y la ruta seguida por el correo, el servidor de correo, detalles de proveedor de servicios de correo electrónico, etc huellas Tracer hasta servicios de Internet Proveedor único nivel. Además, el seguimiento se puede hacer con la ayuda de agencias de aplicación de los ISP y la ley. El mensaje-id será útil para el análisis de los registros de correo en el ISP.

Ilustración 16 Sitio web EmailTracer.
Fuente: Autor

CAPÍTULO 4 ANÁLISIS DEL RATREO DE CORREOS ELECTRÓNICOS

En este capítulo se demostrará los resultados obtenidos del análisis de un correo electrónico en diferentes herramientas de rastreo de correo electrónico de código abierto.

4.1 RESULTADOS DE ANÁLISIS DE HERRAMIENTAS DE INFORMÁTICA FORENSE DE CÓDIGO ABIERTO PARA EL RASTREO DE CORREOS ELECTRÓNICOS

4.1.1 VISUALIZACIÓN DE LOS ENCABEZADOS DE CORREO ELECTRÓNICO EN HOTMAIL

Para poder extraer los encabezados que utilizaremos para el rastreo de un correo eléctrico se deberá de abrir el correo electrónico haciendo clic en él, como se muestra en la ilustración.

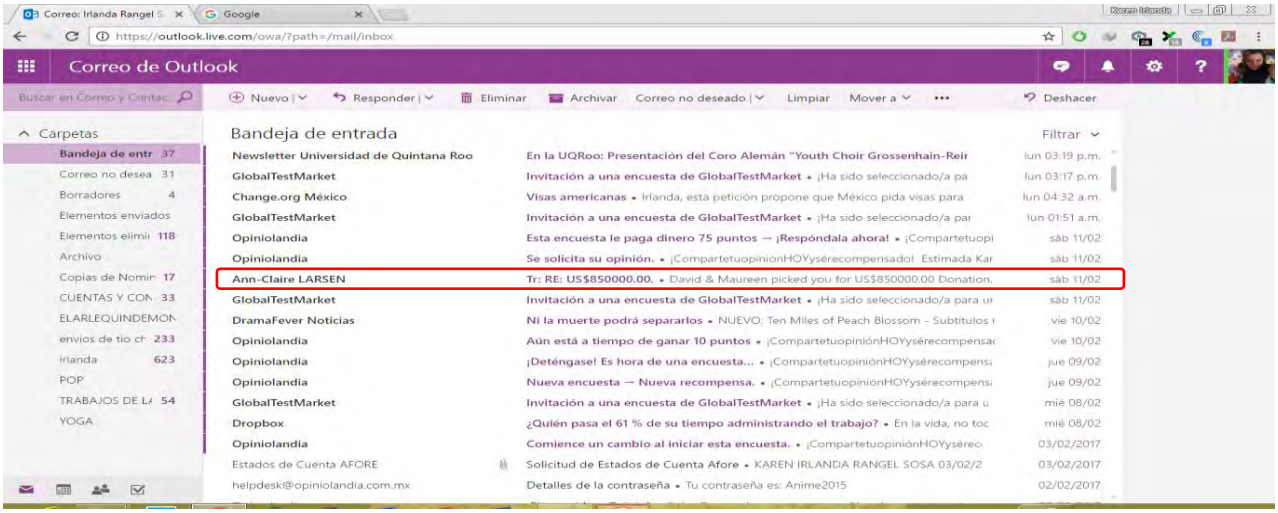


Ilustración 17 Ventana principal bandeja de entrada.

una vez que tengamos el correo electrónico abierto, habrá una flecha hacia abajo en la esquina superior derecha del correo electrónico como se muestra en la siguiente ilustración.

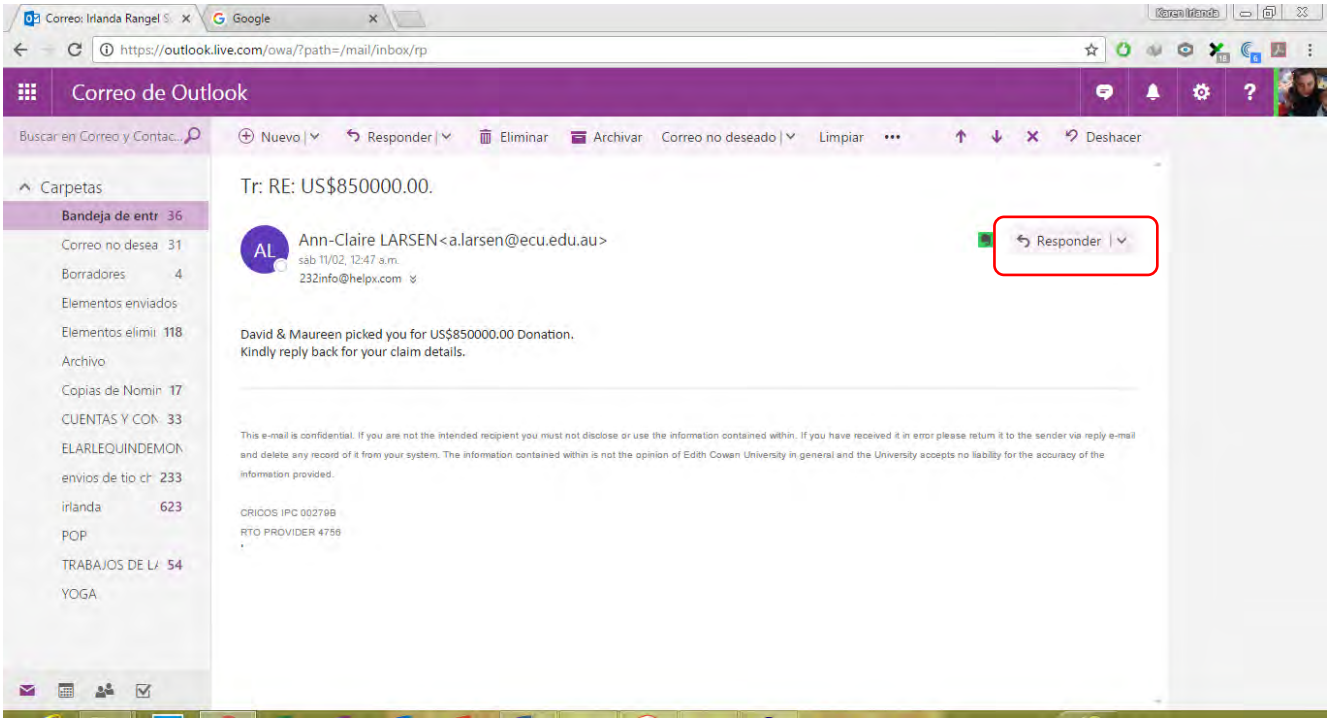


Ilustración 18 Ventana de correo electrónico recibido.

Al hacer clic en la flecha este se desplegará un menú en el cual elegiremos la opción "Ver origen del mensaje" con un clic, como se muestra en la ilustración.

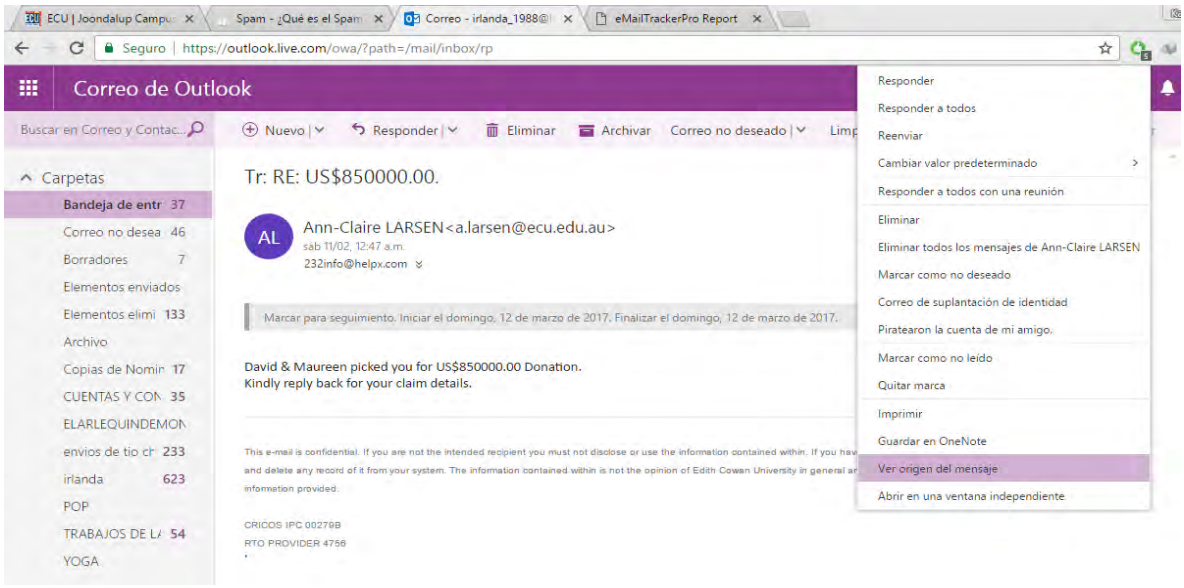


Ilustración 19 Extracción de encabezado en Hotmail.

Se abrirá una pestaña en el navegador y en esa ficha se mostrará todo el correo electrónico en forma de texto, donde el encabezado y el contenido del mensaje serán visibles

Todo lo que se requiere es la cabecera para poder extraer el encabezado como se muestra en la ilustración

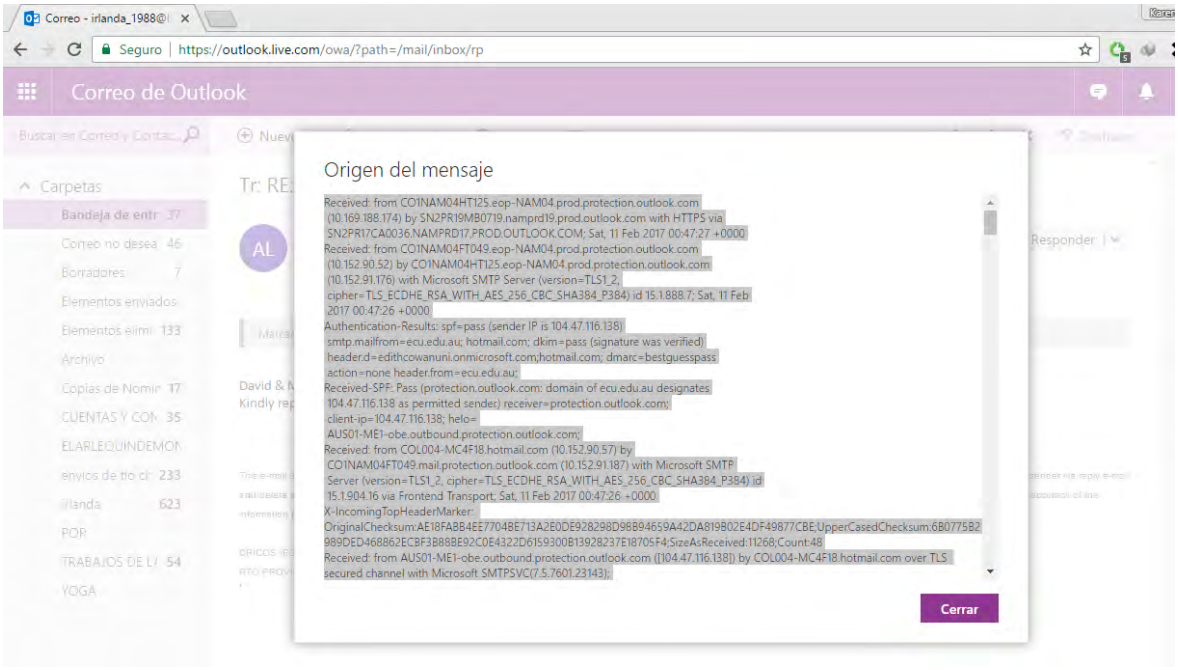


Ilustración 20 Encabezado de correo electrónico en Hotmail.

4.1.2 RESULTADOS IPNETINFO

IPNetInfo es una herramienta que te permite encontrar fácilmente toda la información disponible sobre una dirección IP: El propietario de la dirección IP, el nombre del país / estado, rango de direcciones IP, información de contacto (dirección, teléfono, fax y correo electrónico), y más. IPNetInfo nos dará toda la información relacionada con las IPs sin necesidad de tener que utilizar comandos difíciles de recordar y además toda la información es proporcionada en una interfaz.

Implementación de IPNetInfo

Se tomó un correo electrónico aleatoriamente de mi cuenta de correo electrónico personal, esta imagen se muestra la ventana del navegador Google Chrome y la selección de dicho correo electrónico, en el cual analizaremos la geolocalización del siguiente correo con diferentes herramientas de código abierto para rastreo de correo electrónico.

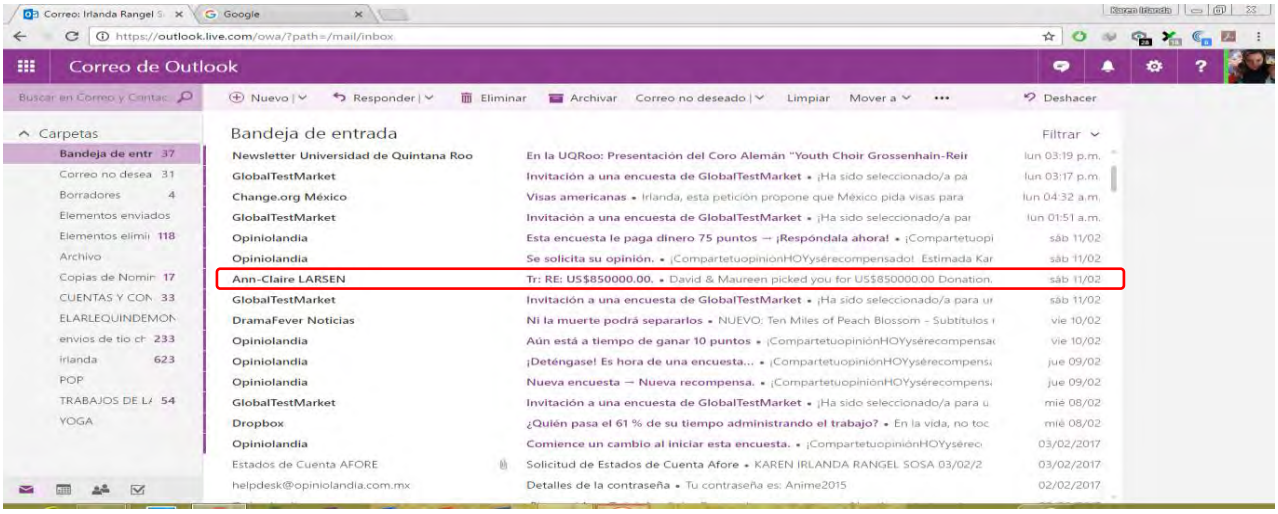


Ilustración 21 Ventana principal bandeja de entrada.

Abrimos el correo ya antes seleccionado, se copia el encabezado extraído del correo electrónico como se mostró anteriormente.

Antes de copiar el encabezado del correo electrónico a rastrear es importante verificar en la herramienta de IPNetInfo este seleccionado la conversión del hombre del host a una dirección IP como se muestra en la siguiente imagen, ya que esta nos servirá para la localización geográfica del remitente del correo electrónico recibido.

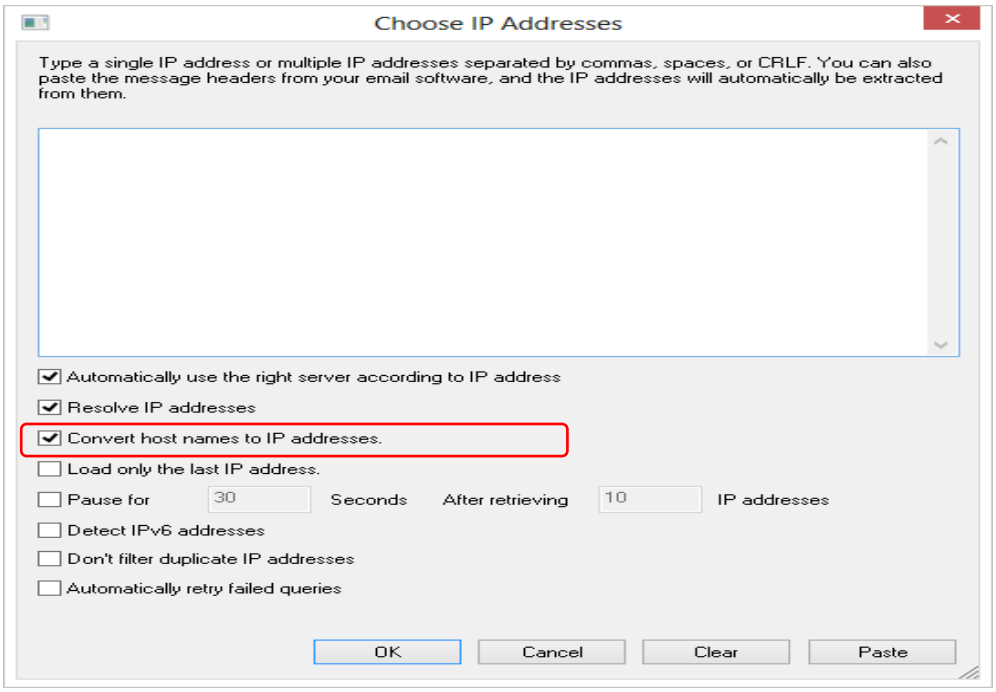


Ilustración 22 Ventana IPNetInfo Choose IP Addresses.

Una vez pegado la información de la cabecera del correo electrónico en el programa IPNetInfo, procedemos a seleccionar el botón OK que se encuentra en la parte inferior de la ventana como se muestra en la siguiente imagen.

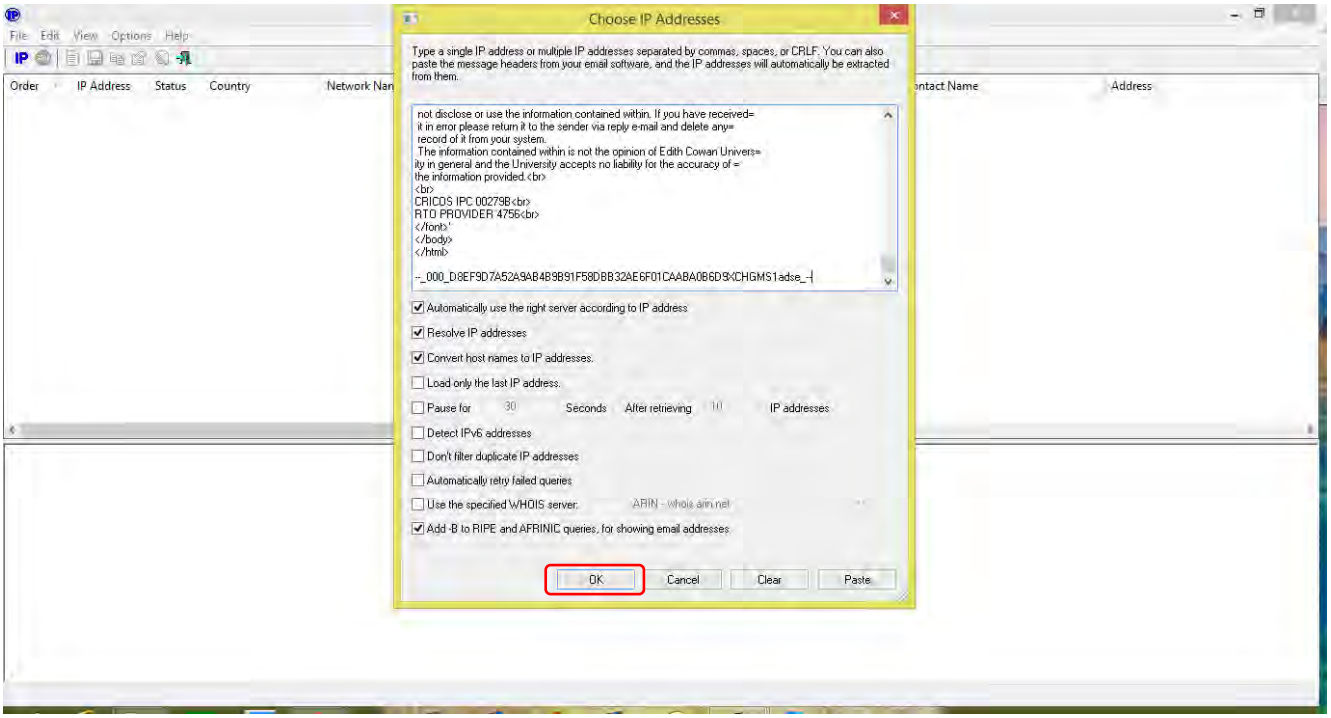


Ilustración 23 Ventana IPNetInfo Choose IP Addresses con información.

Para mostrar la información obtenida del encabezado del correo electrónico IPNetInfo envía una primera solicitud al servidor WHO IS de ARIN como se muestra en la ilustración.

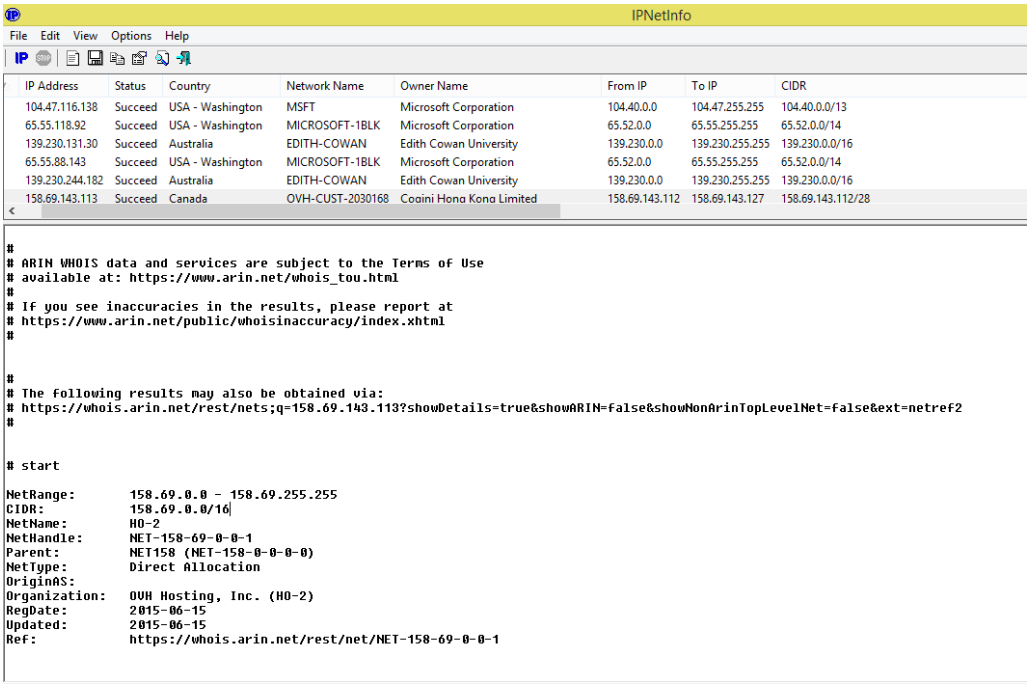


Ilustración 24 Interfaz gráfica IPNetInfo inicio de primera solicitud a WHO IS de ARIN.

En la siguiente ventana se muestra la finalización de la primera solicitud enviada por IPNetInfo a WHO IS de ARIN.

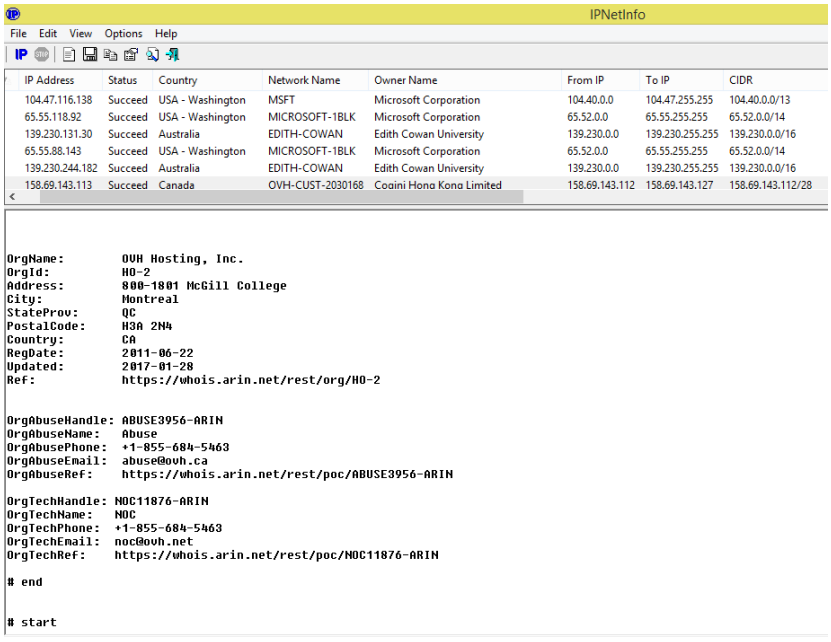


Ilustración 25 Interfaz gráfica IPNetInfo finalización de primera solicitud a WHO IS de ARIN.

Si ARIN no muestra sobre una determina dirección IP se envía una segunda solicitud al servidor de WHO IS de RIPE, APNIC, LACNIC o afriNIC, En la siguiente ventana se muestra

el inicio de la segunda solicitud enviada por IPNetInfo a WHO IS de ARIN para obtener más información de la dirección IP.

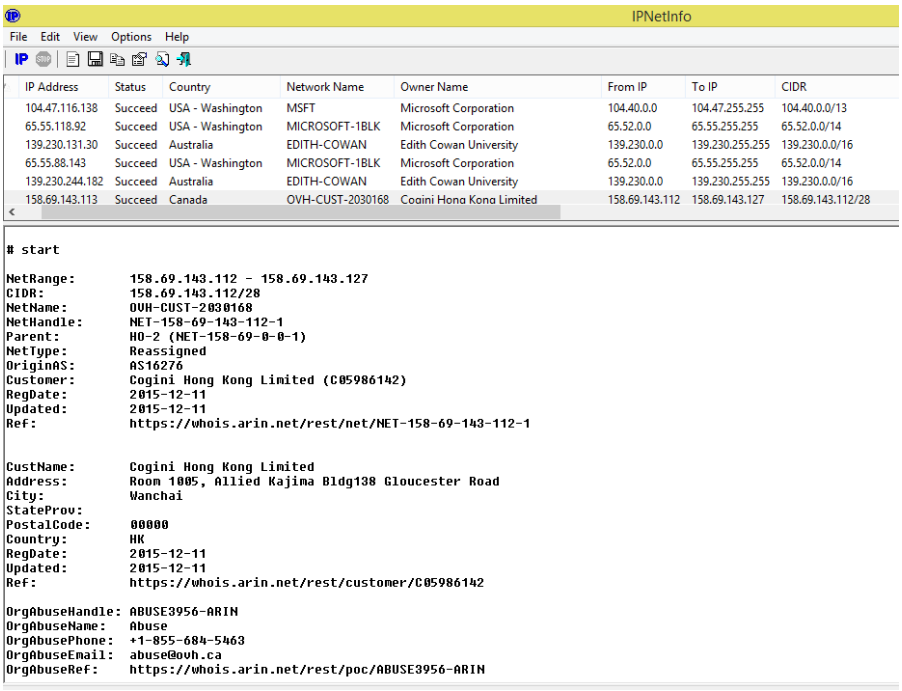


Ilustración 26 Interfaz gráfica IPNetInfo inicio de segunda solicitud a WHO IS de ARIN.

En la siguiente ventana se muestra la finalización de la segunda solicitud enviada por IPNetInfo a WHO IS de ARIN.

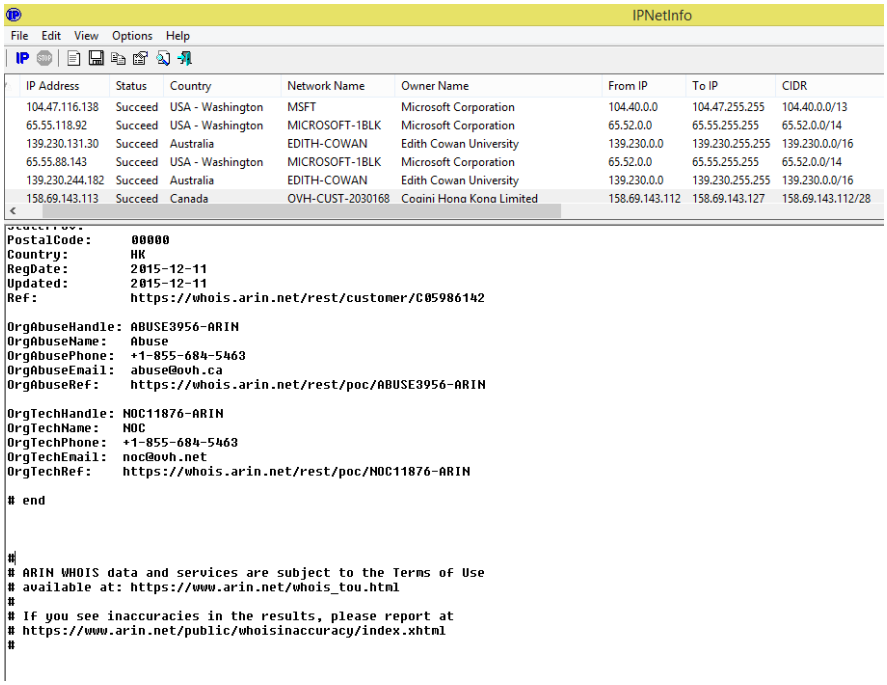


Ilustración 27 Interfaz gráfica IPNetInfo finalización de segunda solicitud a WHO IS de ARIN.

Como resultado IPNetInfo nos proporcionara toda la información disponible que sea capaz de encontrar de la cabecera del correo electrónico; información sobre el dueño, el país donde se encuentra localizada, operador a la que pertenece, rango en que se encuentra comprendida y las posibles formas de contactar con la persona que la tiene asignada (número de teléfono, correo electrónico, fax), como se muestra en la ilustración.

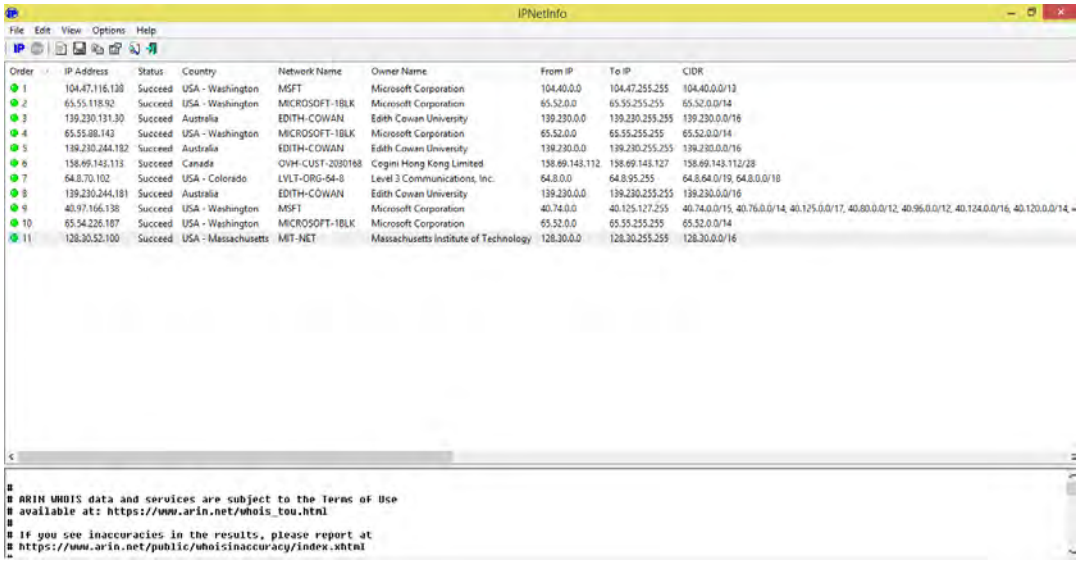


Ilustración 28 Interfaz gráfica IPNetInfo con información obtenida del encabezado del correo electrónico.

La información que nos proporcionó la herramienta de IPNetInfo del encabezado de nuestro correo electrónico seleccionado se muestra en la siguiente ilustración:

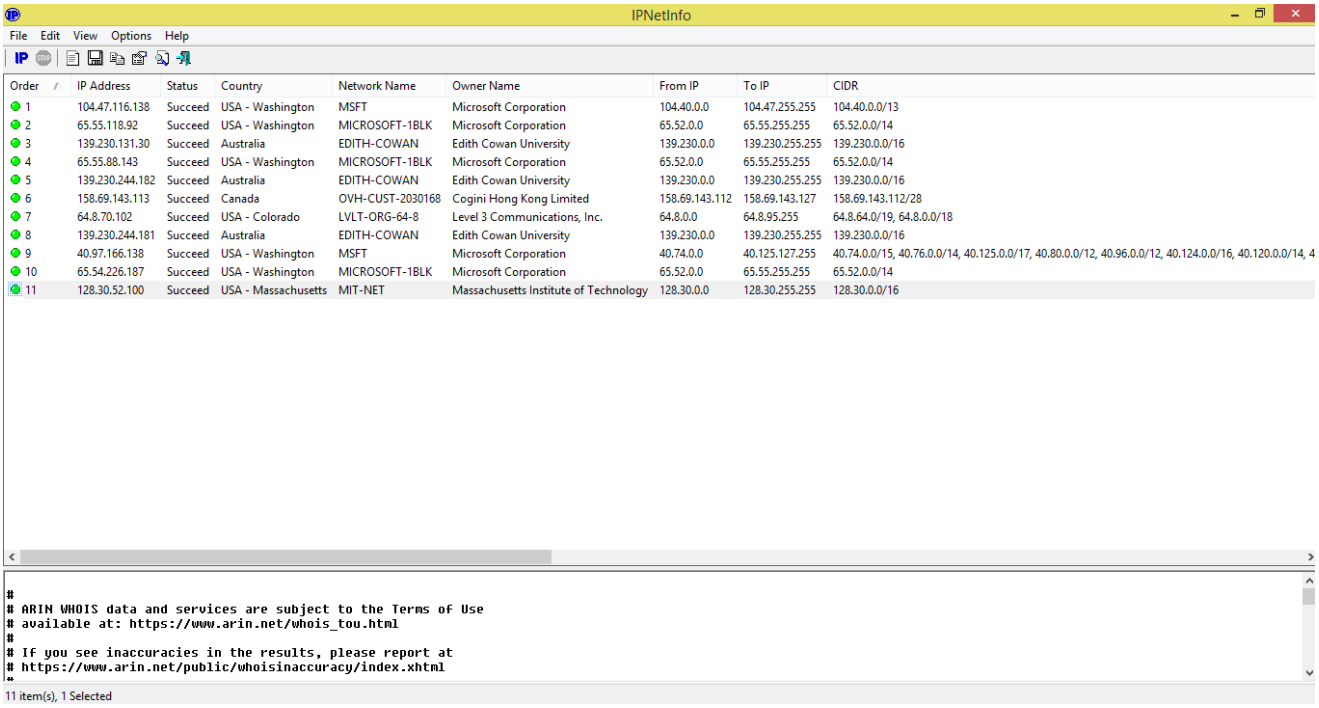


Ilustración 29 Direcciones ip obtenidas por IPNetInfo.

En la imagen anterior se puede ver toda la información que IPNetInfo fue capaz de obtener a partir del encabezado de un correo electrónico. Como se puede observar IPNetInfo fue capaz de obtener el nombre del propietario, el país, el nombre de la red, el rango de direcciones IP y la información del contacto de cada una de las direcciones IP como se muestra en la siguiente ilustración.

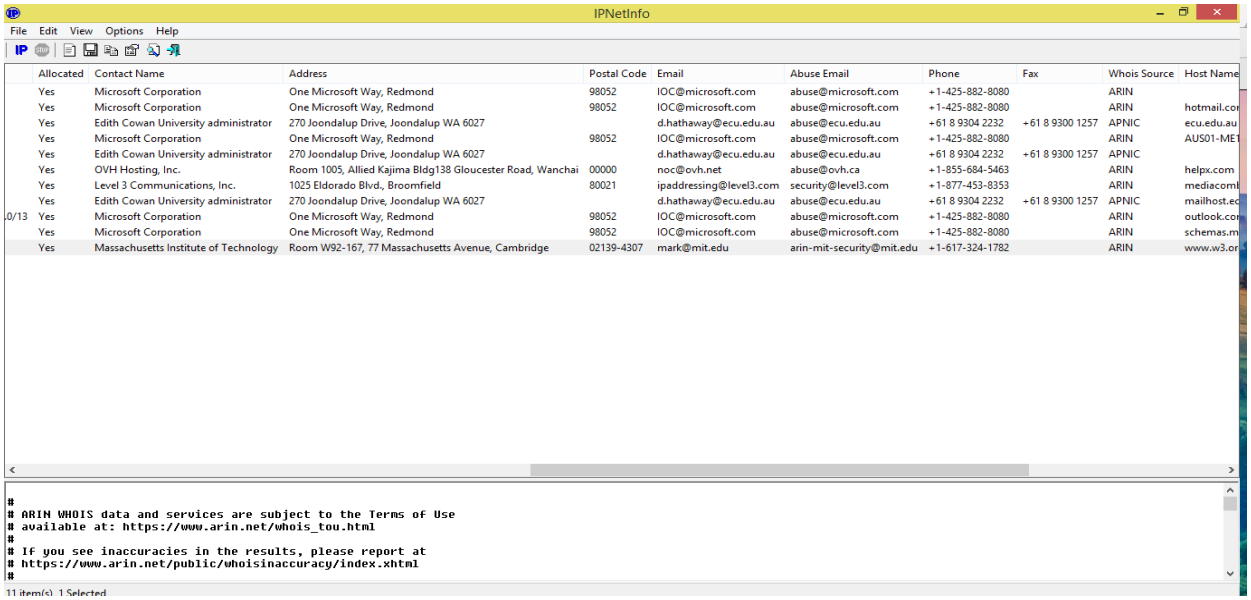


Ilustración 30 Información obtenida de IPNetInfo.

Sin embargo en este caso no se puede definir con exactitud de donde se originó el correo electrónico, con los dominios obtenidos por IPNetInfo podemos hacer una investigación adicional, para averiguar si es confiable el correo electrónico recibido, una opción que se puede seleccionar en IPNetInfo es **Load only the last IP addresses** la cual nos proporcionara la última dirección IP, esto con el fin de obtener información de la última dirección IP en la cual fue enviado el correo electrónico como se muestra en la siguiente ilustración.

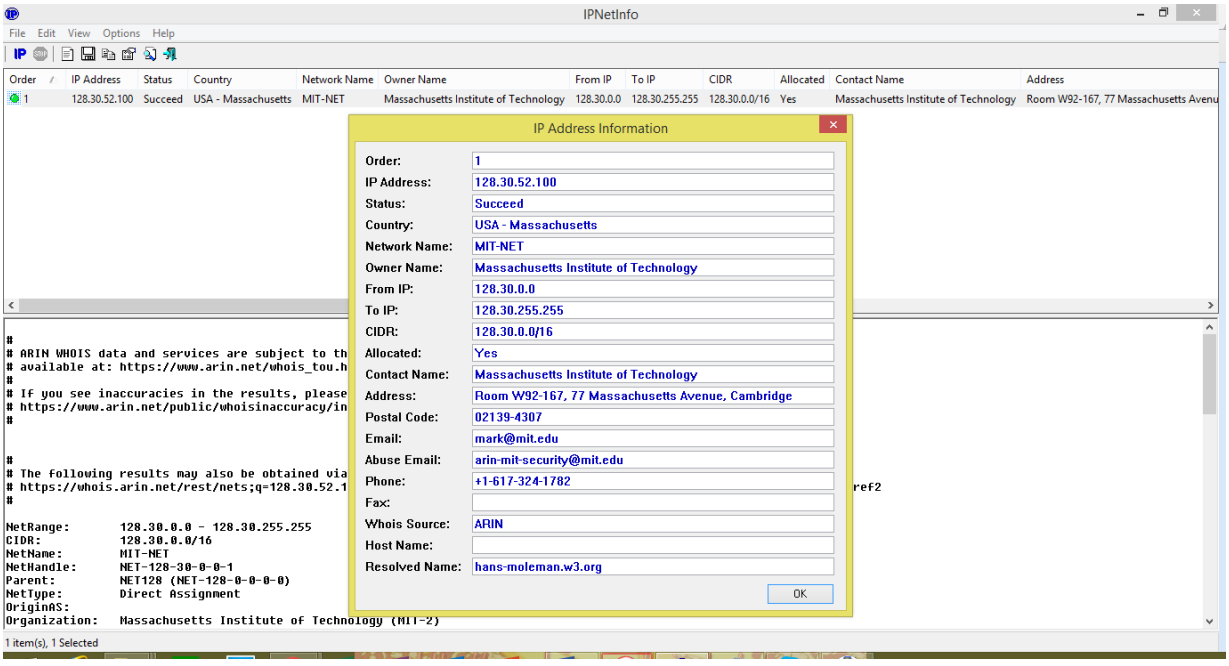


Ilustración 31 Información ultima dirección IP de IPNetInfo.

4.1.3 RESULTADOS EMAILTRACKERPRO

Seguimiento de un encabezado de correo electrónico

Para trazar la una cabecera en EmailtrackerPro debemos ir al menú de archivo y hacemos clic en My trace Reports, como se muestra en la ilustración.

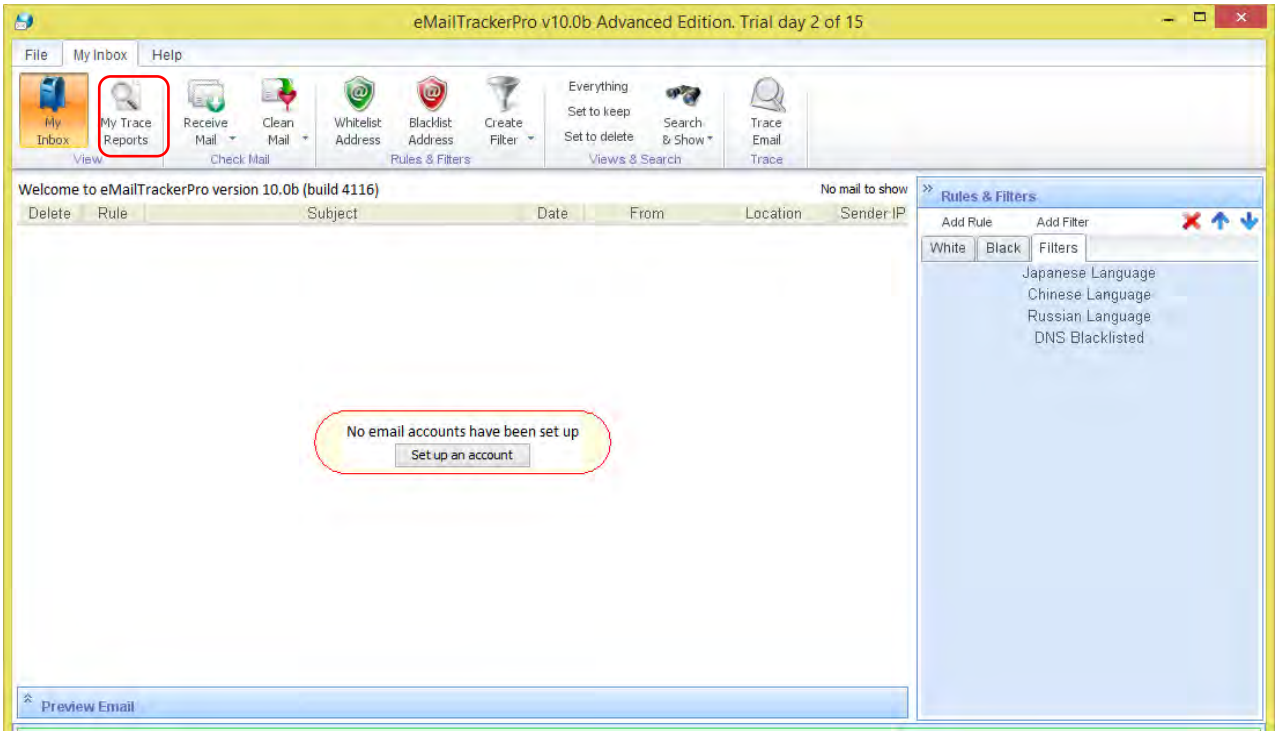


Ilustración 32 Ventana de inicio de EmailtrackerPro.

Una vez que tenemos seleccionado la opción My trace Reports, hacemos clic en la opción Trace Headers como lo muestra la ilustración; para poder empezar a rastrear el correo electrónico por medio encabezado.

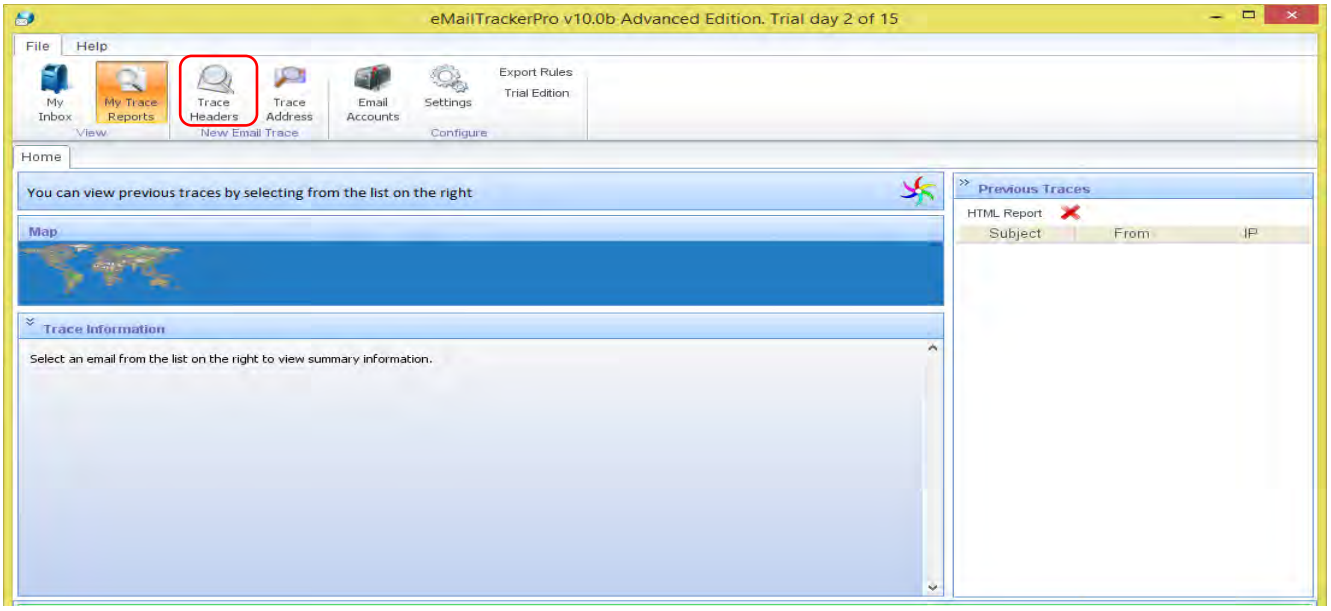


Ilustración 33 Opción trace Headers en EmailtrackerPro.

Una vez que tengamos seleccionado la opción trace Headers nos abrirá un cuadro de dialogo del filtro como se muestra a continuación; este cuadro de dialogo se divide en tres secciones, cada una de las cuales se explica debajo de la ilustración.

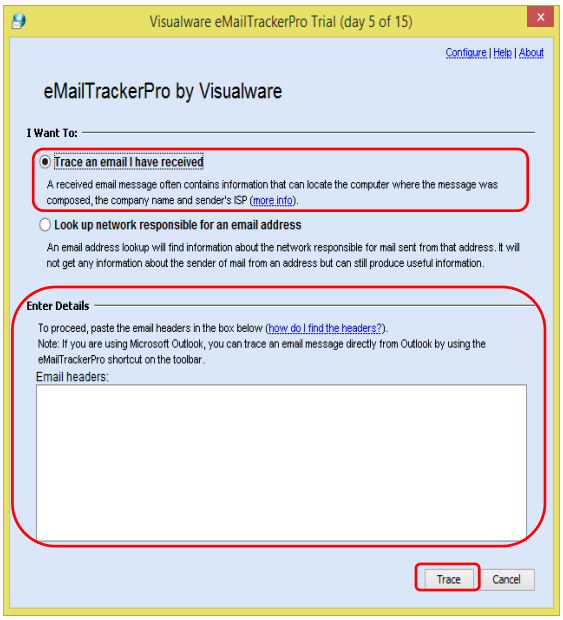


Ilustración 34 Cuadro de dialogo EmailtrackerPro.

La ilustración de arriba se ha divido en tres secciones para facilitar la comprensión y la implementación de EmailtrackerPro

1. Para trazar la ruta de una cabecera se tiene que seleccionar la primera opción como se muestra en la ilustración de arriba.

2. El cuadro de texto que se muestra en la parte de arriba es donde hay que pegar el encabezado de correo electrónico que desea rastrear.
3. Una vez que el encabezado se haya pegado, damos clic en el botón de Trace para el rastreo del correo electrónico, como se muestra en la ilustración de arriba.

Una vez que hayamos extraído el encabezado del correo electrónico, procedemos a pegarlo en el cuadro de texto y damos un clic en Trace como se muestra en la ilustración.

Ilustración 35 Cuadro de dialogo con encabezado.

Una vez que empezamos a trazar el encabezado del correo electrónico EmailtrackerPro comienza el proceso de rastreo como se muestra en la siguiente ilustración.

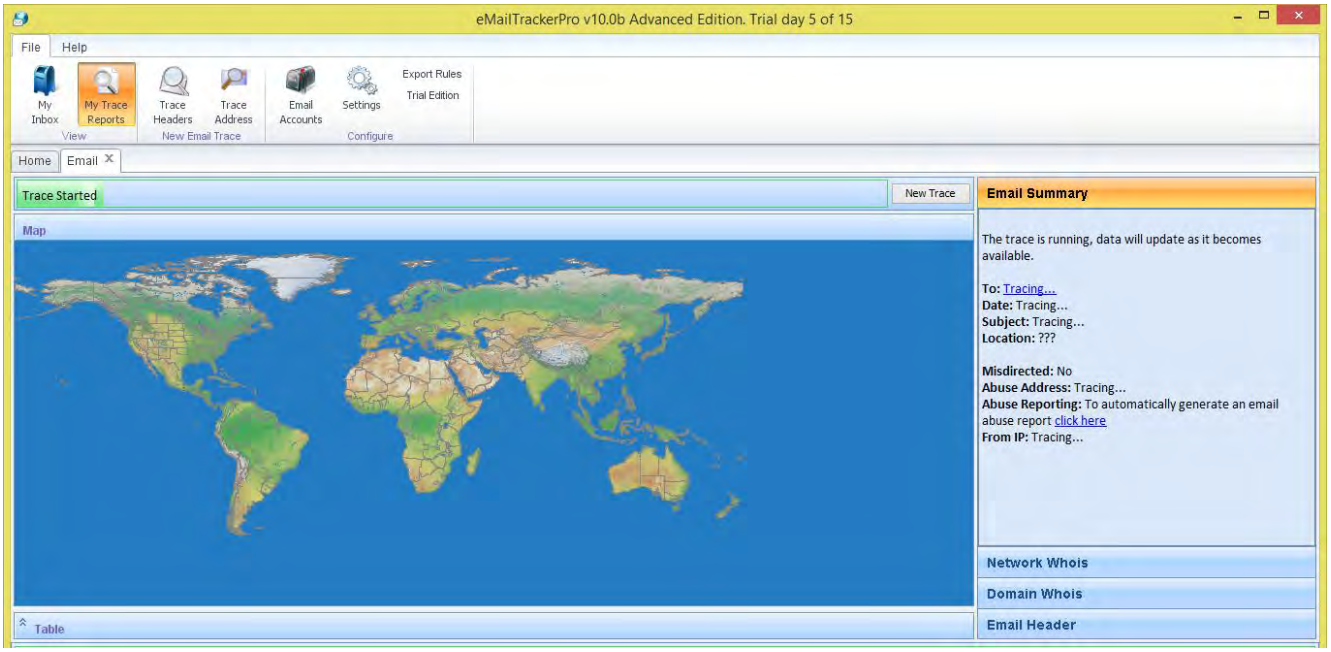


Ilustración 36 Inicio de trazado EmailtrackerPro.

Cuando la traza ha terminado se muestra como en la siguiente ilustración.

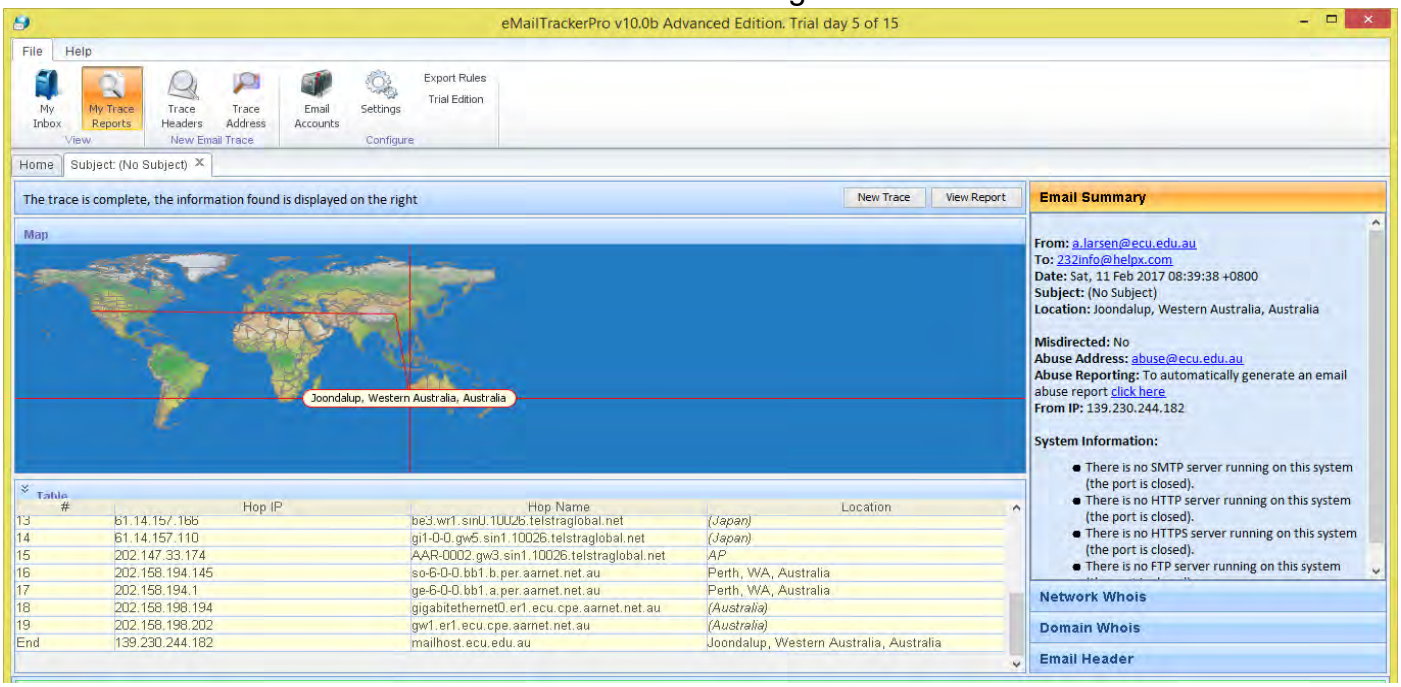


Ilustración 37 Consulta del correo en EmailtrackerPro.

La tabla muestra las rutas desde la dirección ip de donde se está realizando el rastreo hasta el origen probable del correo electrónico, la información de la primera línea de la tabla es del equipo en la que se está realizando la traza y la última entrada será el origen más probable. Una vez que la traza esté completada aparecerá la sección de My Trace Reports para ser revisada en una fecha posterior, como se muestra a continuación.

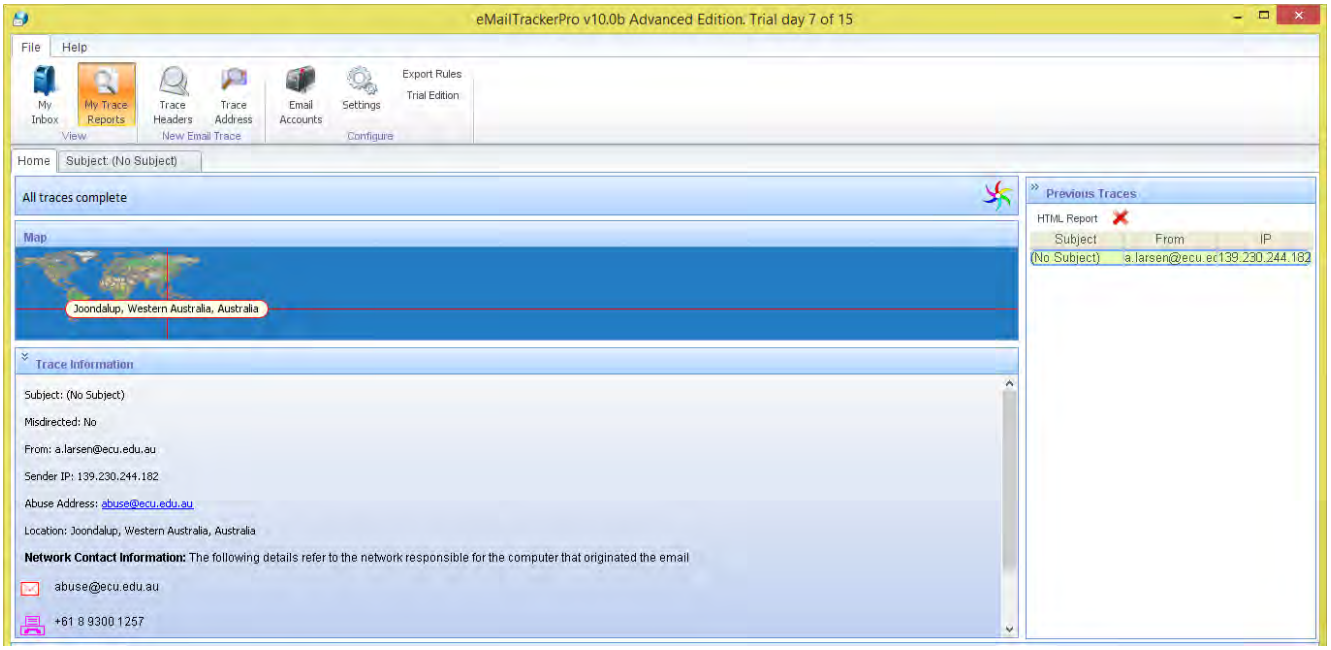


Ilustración 38 Sección My trace Reports.

A continuación, el reporte del análisis de cabeceras del correo electrónico en mención, generado con la herramienta EmailtrackerPro se muestra en la siguiente ilustración.

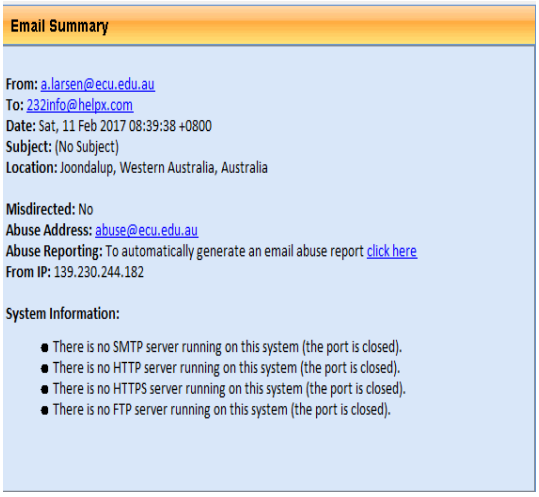


Ilustración 39 Resultado de consulta EmailtrackerPro.

Como se puede observar que el correo si se pudo haber originado desde el dominio de la universidad de Edith Cowan, la dirección IP obtenida 139.230.244.182, ubicado físicamente en la ciudad de Joondalup, western Australia, Australia. Consultando la página oficial de la universidad Edith Cowan como se muestra en la siguiente ilustración.

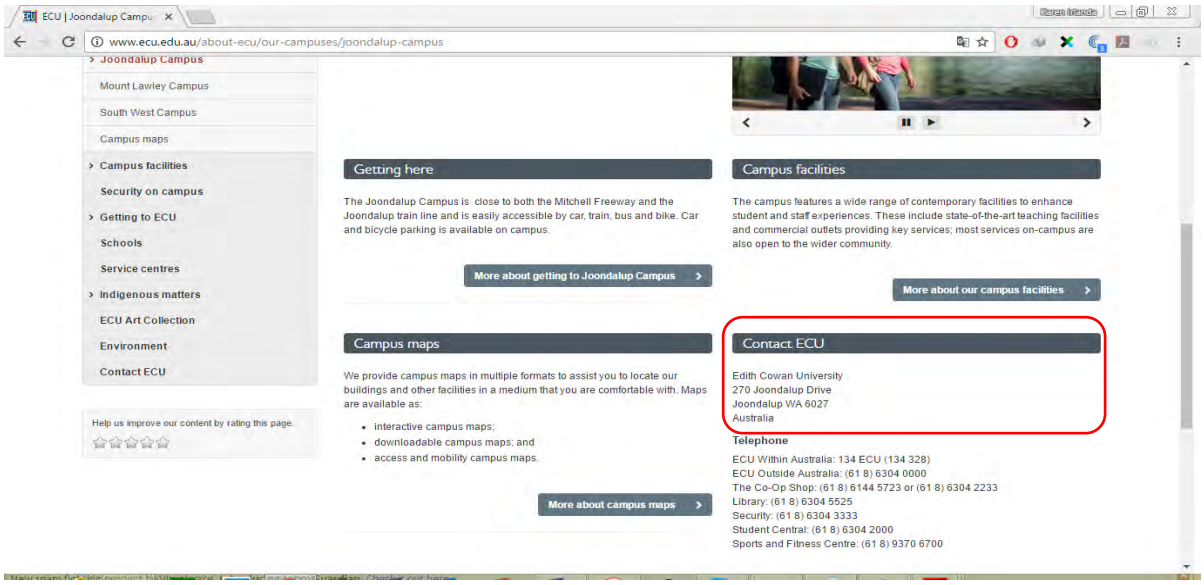


Ilustración 40 Página oficial universidad Edith Cowan.

se puede apreciar que es la misma dirección que nos dio como resultado en la herramienta EmailtrackerPro como se muestra en la siguiente ilustración

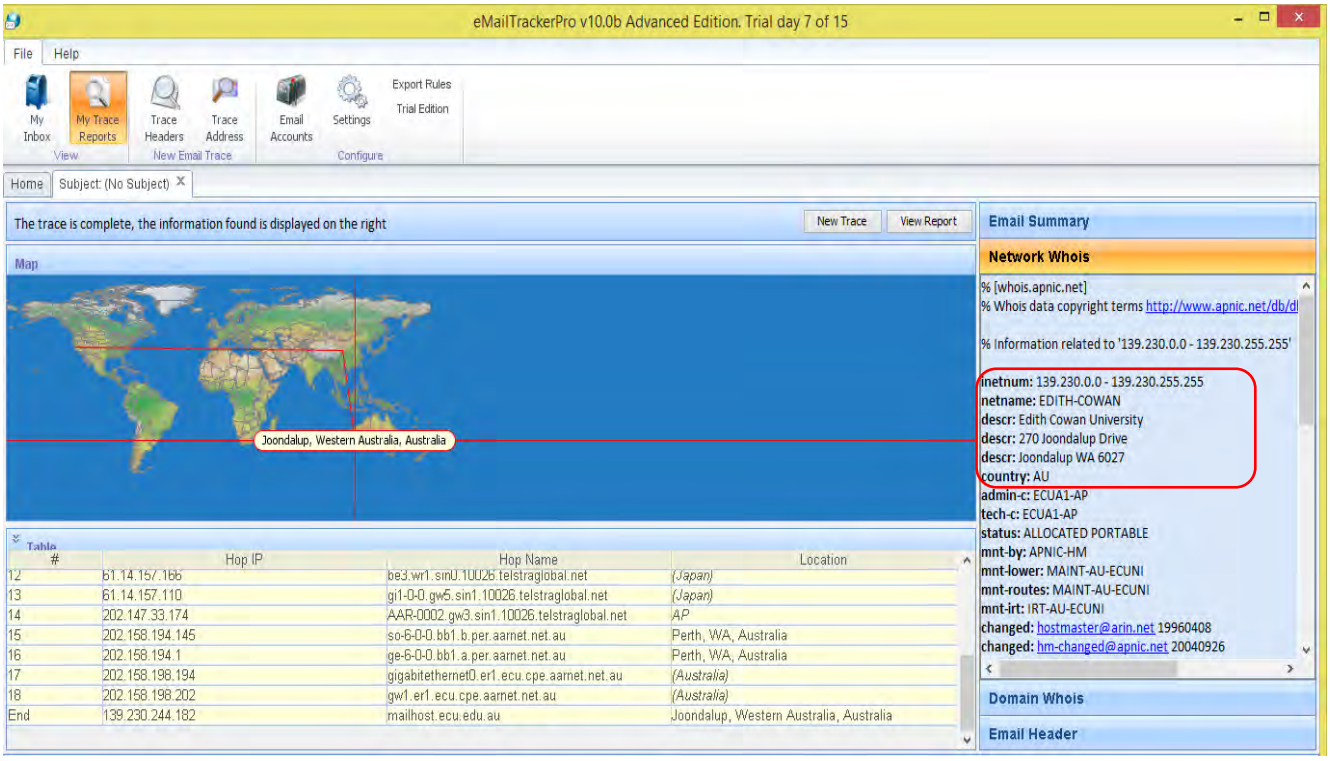


Ilustración 41 Identificación de información obtenida con EmailtrackerPro.

EmailtrackerPro tiene un mapa mundial en el que se muestra la localización sospechosa del correo electrónico actualmente, en la siguiente ilustración se puede apreciar la ruta entre el usuario y la entidad a la que se trazó. Una línea continua representa un salto en una ubicación conocida, y una línea de puntos representa un salto a un lugar imaginario.

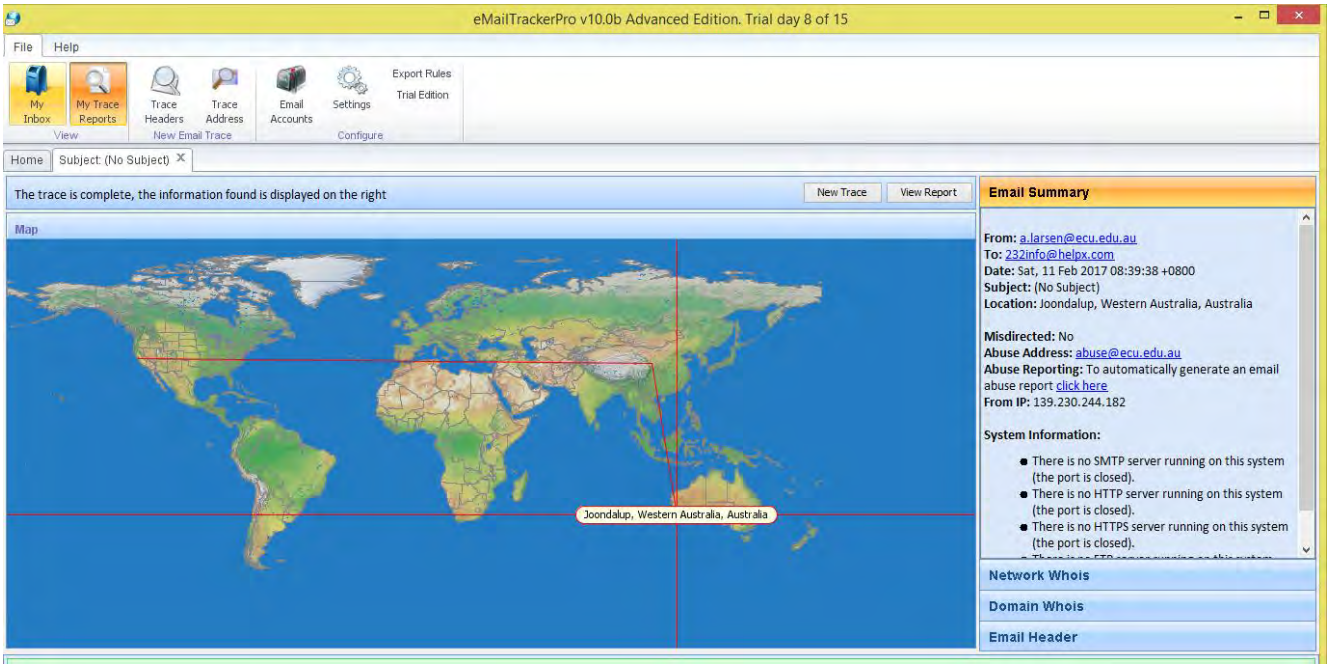


Ilustración 42 Resultado de trazo en EmailtrackerPro.

Consultando el informe que nos proporciona EmailtrackerPro podemos identificar en la tabla la ruta tomada de internet para llegar al destino deseado, como se muestra en la ilustración.

Address of Hop	Name of Hop	Location
192.168.0.1		(Private)
10.154.0.1		(Private)
10.3.65.130		(Private)
10.19.132.109		(Private)
192.168.200.245		(Private)
206.41.108.23		*Miami, FL, USA*
184.105.213.25	100ge11-1.core1.atl1.he.net	*Australia*
184.105.213.70	100ge11-1.core1.ash1.he.net	**Ashburn, VA, USA**
184.105.213.174	100ge12-1.core1.par2.he.net	*Australia*
184.105.222.114	10ge3-1.core1.sin1.he.net	*Australia*
74.82.46.190	pacnet-as10026.10gigabitethernet4-1.core1.sin1.he.net	*Fremont, California, USA*
61.14.157.166	be3.wr1.sin0.10026.telstraglobal.net	*Japan*
61.14.157.110	gi1-0-0.gw5.sin1.10026.telstraglobal.net	*Japan*
202.147.33.174	AAR-0002.gw3.sin1.10026.telstraglobal.net	*AP*
202.158.194.145	so-6-0-0.bb1.b.per.aarnet.net.au	**Perth, WA, Australia**
202.158.194.1	ge-6-0-0.bb1.a.per.aarnet.net.au	**Perth, WA, Australia**
202.158.198.194	gigabitethernet0.er1.ecu.cpe.aarnet.net.au	*Australia*
202.158.198.202	gw1.er1.ecu.cpe.aarnet.net.au	*Australia*
-	(unnamed)	
139.230.244.182	mailhost.ecu.edu.au	**Joondalup, Western Australia, Australia**

Ilustración 43 Trazado de ruta con direcciones IP en EmailtrackerPro.

Sin embargo, este correo electrónico se puede deducir que es un correo basura o spam, ya que la información del correo electrónico a.larsen@ecu.edu.au se puede falsificar fácilmente, por lo que no debe tratarse como concluyente.

4.1.4 RESULTADOS TRACE EMAIL ANALYZER

Para realizar el rastreo se necesita conocer la cabecera del correo electrónico que fue recibido. Con esta cabecera se puede utilizar la herramienta trace email analyzer para obtener la ip de origen donde fue enviado el correo electrónico. En este caso utilizamos el sitio web http://whatismyipaddress.com/trace-email que nos proporcionara la información deseada.
Para obtener la dirección IP es necesario copiar la cabecera del correo electrónico en el sitio web.

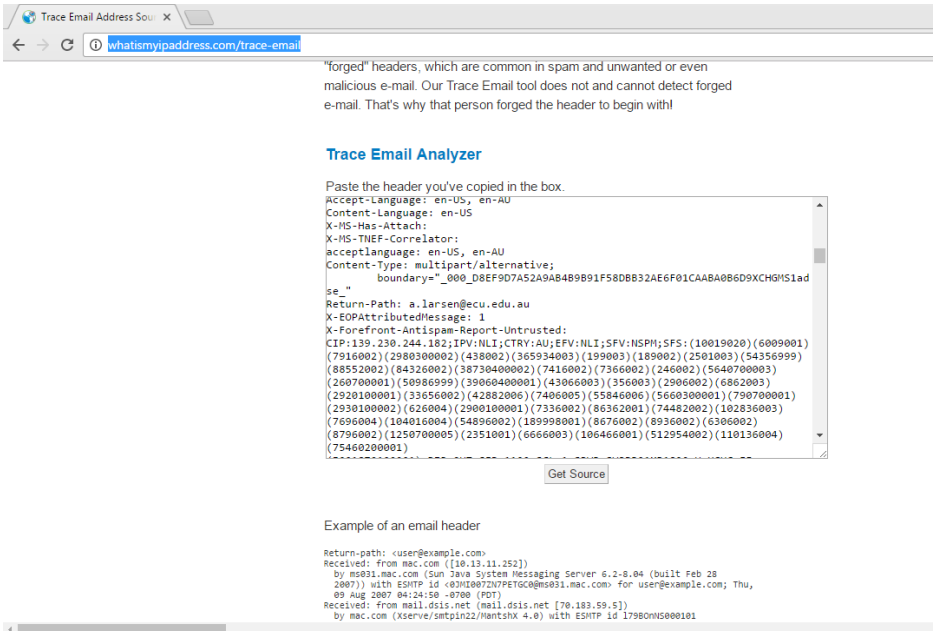


Ilustración 44 Encabezado sitio What´s my ip address.

Al hacer el análisis trace email nos muestra en la detección de direcciones IP en su análisis como lo muestra la siguiente ilustración.

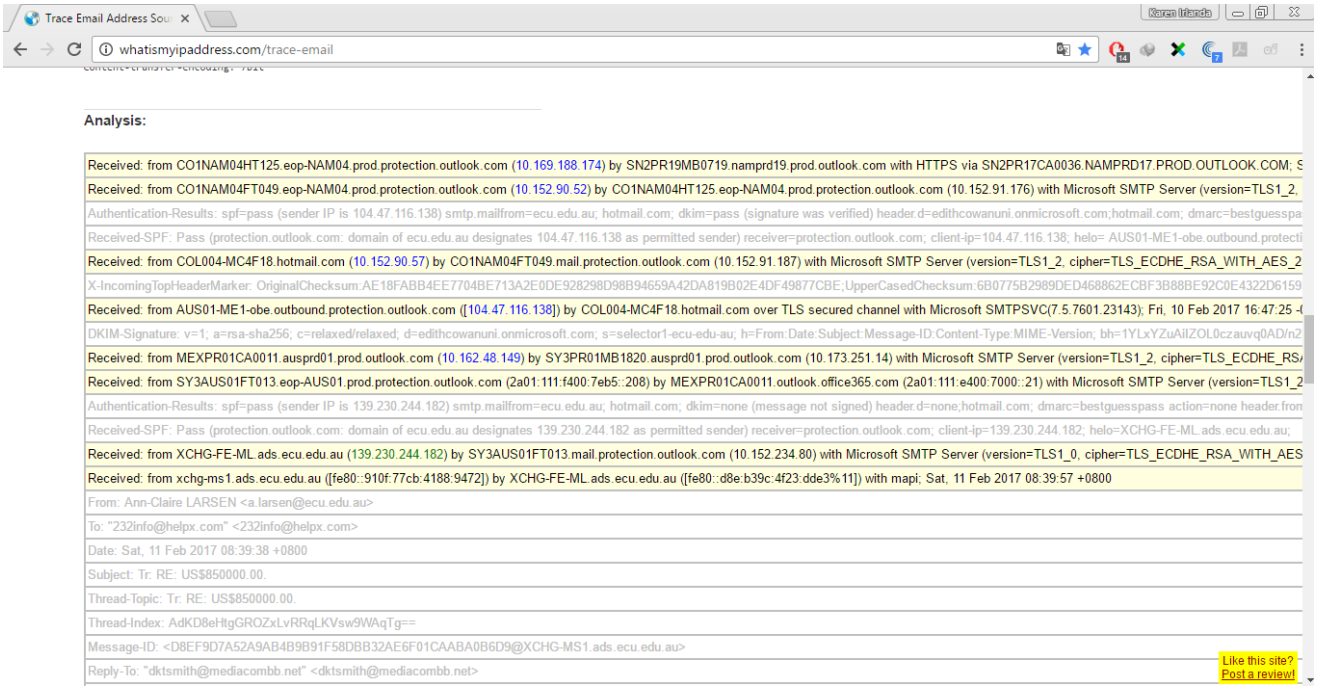


Ilustración 45 Análisis trace email.

Este sitio al obtener la dirección IP origen también obtiene la geolocalización la cual se puede observar en un pequeño mapa, como se muestra en la ilustración.

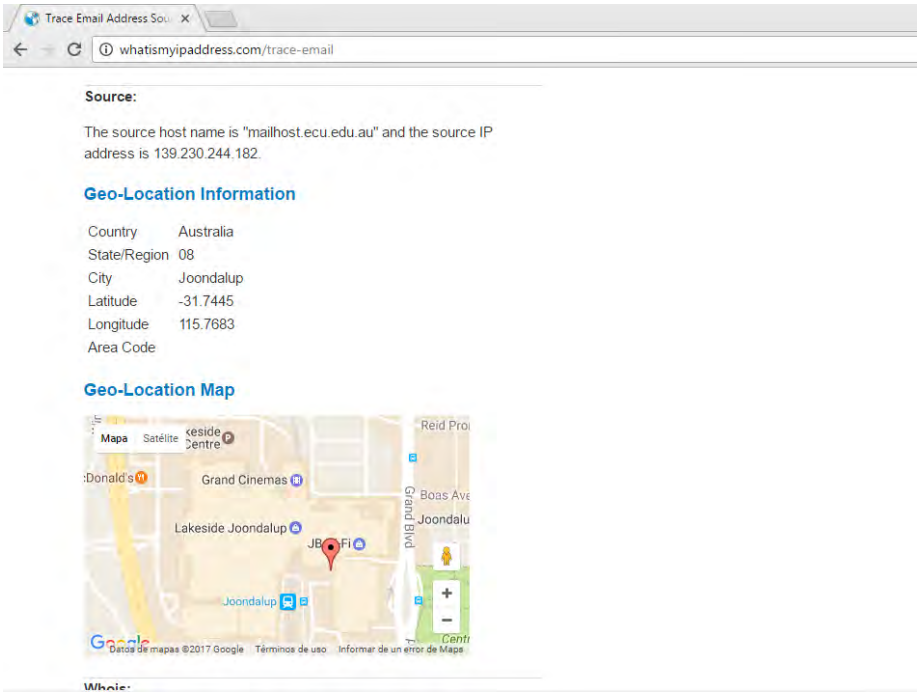


Ilustración 46 Resultado de análisis trace email.

Para tener una información completa del origen de nuestra dirección IP obtenida anteriormente es necesario el ISP, para obtenerla accedimos a la siguiente dirección: http://lacnic.net/cgi-bin/lacnic/whois?lg=EN, el cual obtuvimos la siguiente información.

```
% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% APNIC resource: whois.apnic.net

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '139.230.0.0 - 139.230.255.255'

inetnum:        139.230.0.0 - 139.230.255.255
netname:        EDITH-COWAN
descr:          Edith Cowan University
descr:          270 Joondalup Drive
descr:          Joondalup WA 6027
country:        AU
admin-c:        ECUA1-AP
tech-c:         ECUA1-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-AU-ECUNI
mnt-routes:     MAINT-AU-ECUNI
mnt-irt:        IRT-AU-ECUNI
changed:        hostmaster@arin.net 19960408
changed:        hm-changed@apnic.net 20040926
changed:        hm-changed@apnic.net 20170303
source:         APNIC
```

```
irt:          IRT-AU-ECUNI
address:       270 Joondalup Drive
address:       Joondalup WA 6027
phone:         +61 8 9304 2232
fax-no:        +61 8 9300 1257
e-mail:        d.hathaway@ecu.edu.au
abuse-mailbox:  abuse@ecu.edu.au
admin-c:       ECUA1-AP
tech-c:        ECUA1-AP
auth:          # Filtered
mnt-by:        MAINT-AU-ECUNI
changed:       hm-changed@apnic.net 20170302
source:        APNIC

role:          Edith Cowan University administrator
address:       270 Joondalup Drive
address:       Joondalup WA 6027
country:       AU
phone:         +61 8 9304 2232
fax-no:        +61 8 9300 1257
e-mail:        d.hathaway@ecu.edu.au
admin-c:       ECUA1-AP
tech-c:        ECUA1-AP
nic-hdl:       ECUA1-AP
mnt-by:        MAINT-AU-ECUNI
changed:       hm-changed@apnic.net 20170302
source:        APNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r0 (UNDEFINED)
```

Con la consulta anterior obtenemos información del contacto importante como lo es la dirección, el teléfono, el correo electrónico y el país.

4.1.5 RESULTADOS EMAIL TRACER

Para realizar el rastreo se necesita conocer la cabecera del correo electrónico que fue recibido. Con esta cabecera se puede utilizar la herramienta trace email analyzer para obtener la ip de origen donde fue enviado el correo electrónico. En este caso utilizamos el sitio web http://www.cyberforensics.in/OnlineEmailTracer/index.aspx que nos proporcionara la información deseada.

Para obtener la dirección IP es necesario copiar la cabecera del correo electrónico en el sitio web.

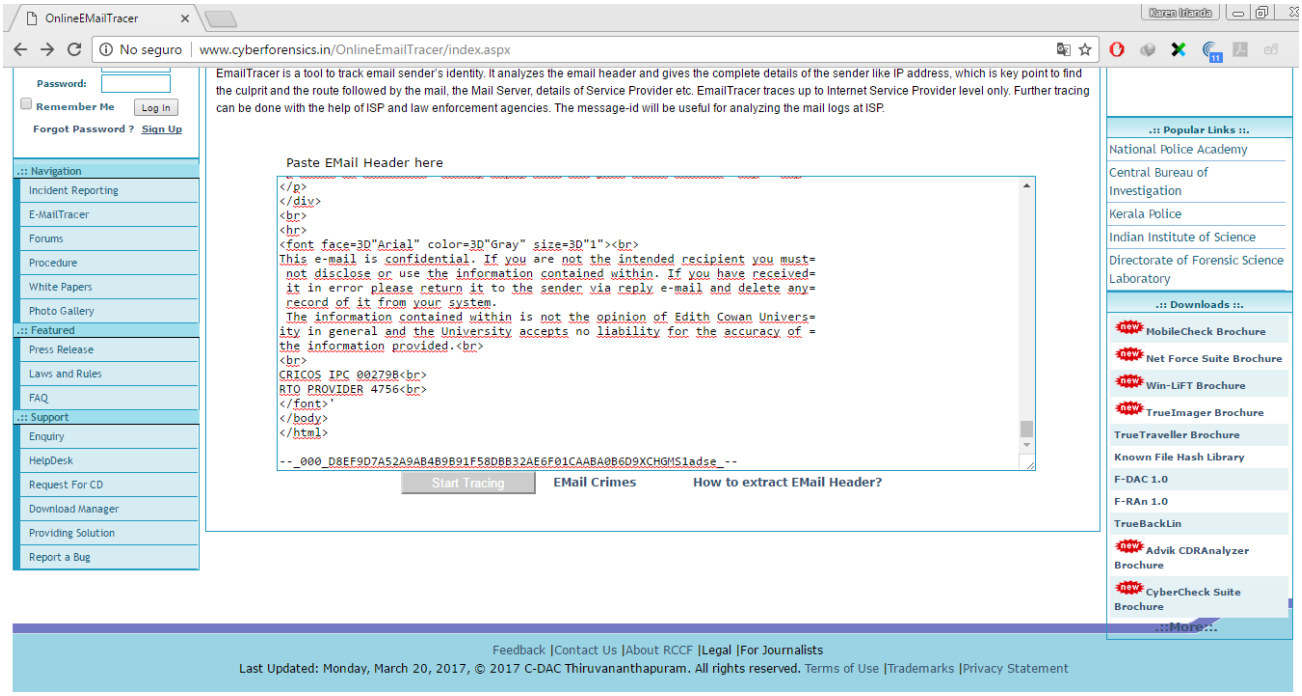


Ilustración 47 Encabezado en email tracer.

Al hacer el análisis trace email nos muestra en la detección de direcciones IP en su análisis como lo muestra la siguiente ilustración.

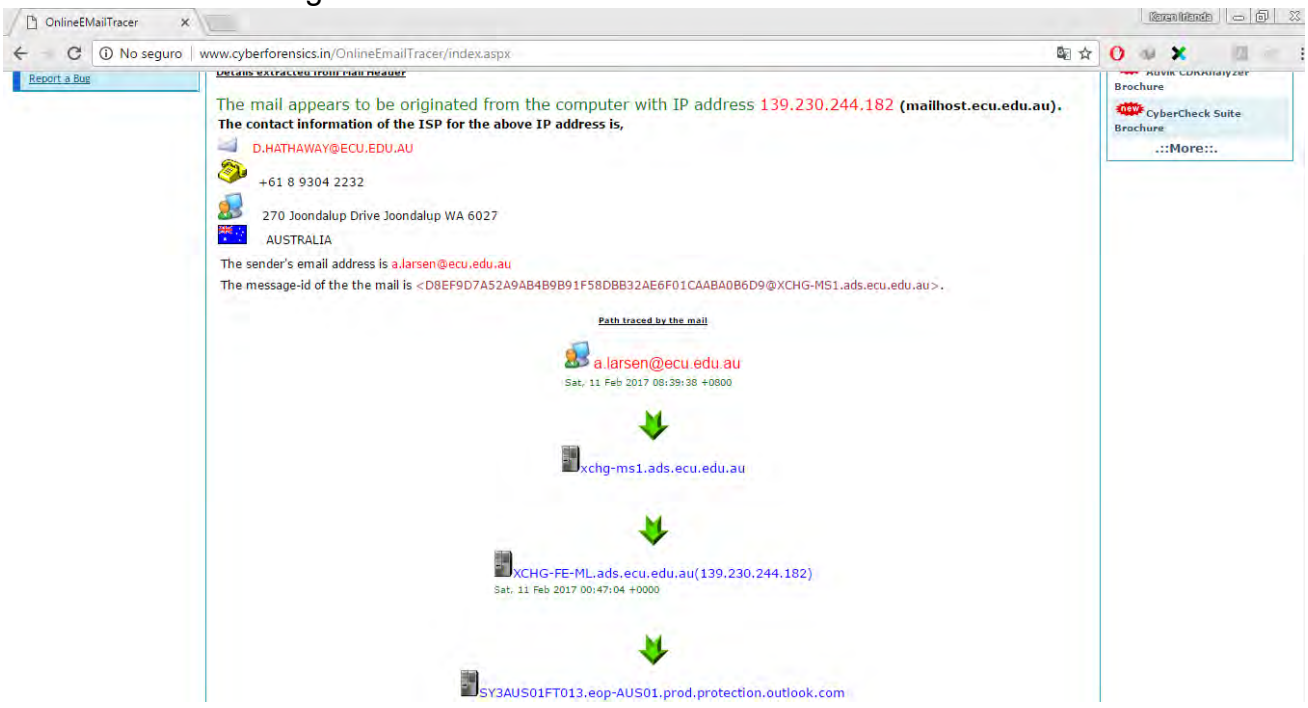


Ilustración 48 Resultados email tracer.

Al observar los resultados obtenidos por email tracer vemos el trazo de las direcciones ip de forma cronológica, empezando una ruta desde el origen del correo electrónico hasta el momento en que lo recibimos, esto se puede apreciar en la siguiente ilustración.

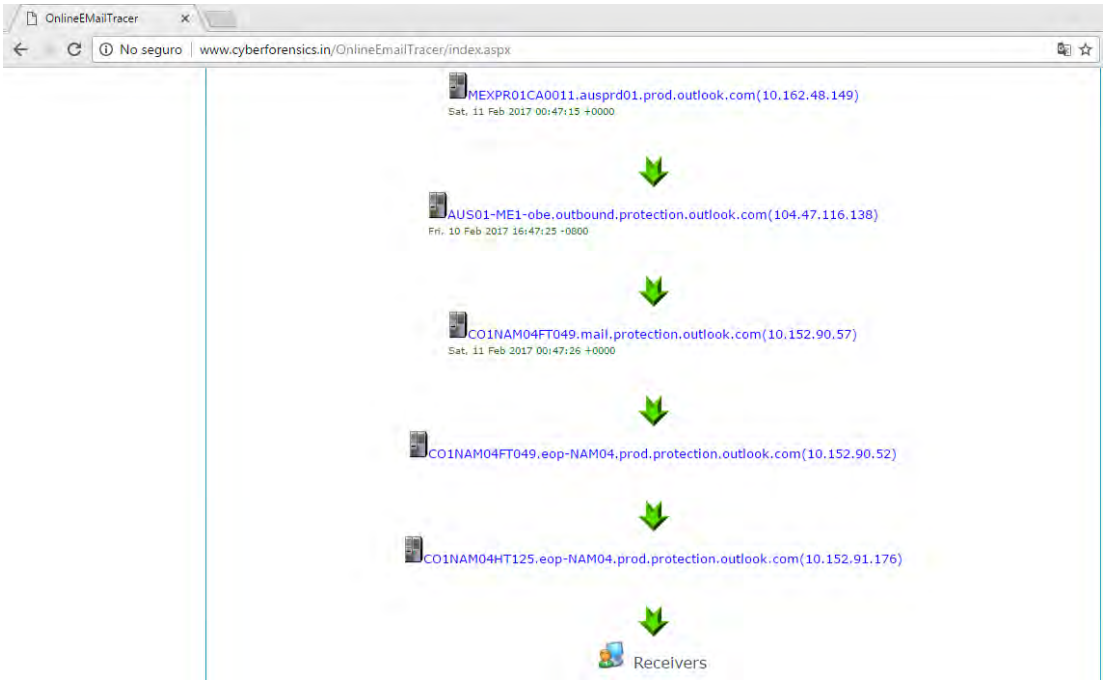


Ilustración 49 Trazo de ruta email tracer.

Una de las características que tiene email tracer es que nos proporciona una tabla con información de las cuentas o direcciones ip fueron remitente, las direcciones ip que fueron destinatarios, así como las fechas en la que fue recibido el correo eléctrico, la cual se puede observar en la siguiente ilustración.

Received By	Received From	Date
"232info@helpx.com" 232info@helpx.com	CO1NAM04HT125.eop-NAM04.prod.protection.outlook.com[10.152.91.176]	--
CO1NAM04HT125.eop-NAM04.prod.protection.outlook.com[10.152.91.176]	CO1NAM04FT049.eop-NAM04.prod.protection.outlook.com[10.152.90.52]	--
CO1NAM04FT049.eop-NAM04.prod.protection.outlook.com[10.152.90.52]	CO1NAM04FT049.mail.protection.outlook.com[10.152.90.57]	Sat, 11 Feb 2017 00:47:26 +0000
CO1NAM04FT049.mail.protection.outlook.com[10.152.90.57]	AUS01-ME1-obe.outbound.protection.outlook.com[104.47.116.138]	Fri, 10 Feb 2017 16:47:25 -0800
AUS01-ME1-obe.outbound.protection.outlook.com[104.47.116.138]	MEXPR01CA0011.ausprd01.prod.outlook.com[10.162.48.149]	Sat, 11 Feb 2017 00:47:15 +0000
MEXPR01CA0011.ausprd01.prod.outlook.com[10.162.48.149]	SY3AUS01FT013.eop-AUS01.prod.protection.outlook.com	Sat, 11 Feb 2017 00:47:16 +0000
SY3AUS01FT013.eop-AUS01.prod.protection.outlook.com	XCHG-FE-ML.ads.ecu.edu.au[139.230.244.182]	Sat, 11 Feb 2017 00:47:04 +0000
XCHG-FE-ML.ads.ecu.edu.au[139.230.244.182]	xchg-ms1.ads.ecu.edu.au	--
xchg-ms1.ads.ecu.edu.au	a.larsen@ecu.edu.au	Sat, 11 Feb 2017 08:39:38 +0800

Ilustración 50 Tabla de cuenta de correo y direcciones IP en email tracer

Otra de las opciones que nos ofrece email tracer es que nos proporciona una tabla con información detallada del nombre del dominio de donde proviene el correo electrónico, la dirección IP, el país, una dirección y el ISP; como se muestra en la siguiente ilustración.

Details obtained from Regional Internet Registry

Domain/Registrant	IP	Registry	Country	City/Address	ISP
CO1NAM04HT125.eop-NAM04.prod.protection.outlook.com	10.152.91.176	**	**	**	**
CO1NAM04FT049.eop-NAM04.prod.protection.outlook.com	10.152.90.52	**	**	**	**
CO1NAM04FT049.mail.protection.outlook.com	10.152.90.57	**	**	**	**
AUS01-ME1-obe.outbound.protection.outlook.com/mail-me1aus01on0138.outbound.protection.outlook.com	104.47.116.138/MICROSOFT CORPORATION	ARIN	UNITED STATES	REDMOND	MICROSOFT CORPORATION
MEXPR01CA0011.ausprd01.prod.outlook.com	10.162.48.149	**	**	**	**
XCHG-FE-ML.ads.ecu.edu.au/mailhost.ecu.edu.au	139.230.244.182/EDITH-COWAN	APNIC	AUSTRALIA	270 Joondalup Drive Joondalup WA 6027	EDITH COWAN UNIVERSITY

** Private IP address

Ilustración 51 Detalles obtenidos en email tracer.

A continuación, se muestra la información obtenida de cada una de las consultas que fueron enviadas a ARIN WHOIS por Email Tracer

104.47.116.138/MICROSOFT CORPORATION
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

#
Query terms are ambiguous. The query is assumed to be:
"n 104.47.116.138"
#
Use "?" to get help.
#

#
The following results may also be obtained via:
#
https://whois.arin.net/rest/nets;q=104.47.116.138?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2
#
NetRange: 104.40.0.0 - 104.47.255.255
CIDR: 104.40.0.0/13
NetName: MSFT
NetHandle: NET-104-40-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2014-05-07
Updated: 2014-05-07
Ref: https://whois.arin.net/rest/net/NET-104-40-0-0-1

OrgName: Microsoft Corporation
OrgId: MSFT
Address: One Microsoft Way

City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1998-07-09
Updated: 2017-01-28
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:
Comment: * https://cert.microsoft.com.
Comment:
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment: * abuse@microsoft.com.
Comment:
Comment: To report security vulnerabilities in Microsoft products and services, please contact:
Comment: * secure@microsoft.com.
Comment:
Comment: For legal and law enforcement-related requests, please contact:
Comment: * msndcc@microsoft.com
Comment:
Comment: For routing, peering or DNS issues, please
Comment: contact:
Comment: * IOC@microsoft.com
Ref: https://whois.arin.net/rest/org/MSFT

OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: https://whois.arin.net/rest/poc/MRPD-ARIN
OrgAbuseHandle: MAC74-ARIN
OrgAbuseName: Microsoft Abuse Contact
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@microsoft.com
OrgAbuseRef: https://whois.arin.net/rest/poc/MAC74-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

1

39.230.244.182/ASIA PACIFIC NETWORK INFORMATION CENTRE
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

#
Query terms are ambiguous. The query is assumed to be:
"n 139.230.244.182"
#

Use "?" to get help.
#

#
The following results may also be obtained via:
#
https://whois.arin.net/rest/nets;q=139.230.244.182?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2
#

NetRange: 139.230.0.0 - 139.230.255.255
CIDR: 139.230.0.0/16
NetName: APNIC-ERX-139-230-0-0
NetHandle: NET-139-230-0-0-1
Parent: NET139 (NET-139-0-0-0-0)
NetType: Early Registrations, Transferred to APNIC
OriginAS:
Organization: Asia Pacific Network Information Centre (APNIC)
RegDate: 2004-03-03
Updated: 2009-10-08
Comment: This IP address range is not registered in the ARIN database.
Comment: This range was transferred to the APNIC Whois Database as
Comment: part of the ERX (Early Registration Transfer) project.
Comment: For details, refer to the APNIC Whois Database via
Comment: WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment:
Comment: ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment: for the Asia Pacific region. APNIC does not operate networks
Comment: using this IP address range and is not able to investigate
Comment: spam or abuse reports relating to these addresses. For more
Comment: help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
Ref: https://whois.arin.net/rest/net/NET-139-230-0-0-1

ResourceLink: http://wq.apnic.net/whois-search/static/search.html
ResourceLink: whois.apnic.net

OrgName: Asia Pacific Network Information Centre
OrgId: APNIC
Address: PO Box 3646
City: South Brisbane
StateProv: QLD
PostalCode: 4101
Country: AU
RegDate:
Updated: 2012-01-24
Ref: https://whois.arin.net/rest/org/APNIC

ReferralServer: whois://whois.apnic.net
ResourceLink: http://wq.apnic.net/whois-search/static/search.html

OrgAbuseHandle: AWC12-ARIN
OrgAbuseName: APNIC Whois Contact
OrgAbusePhone: +61 7 3858 3188
OrgAbuseEmail: search-apnic-not-arin@apnic.net
OrgAbuseRef: https://whois.arin.net/rest/poc/AWC12-ARIN

OrgTechHandle: AWC12-ARIN
OrgTechName: APNIC Whois Contact

OrgTechPhone: +61 7 3858 3188
OrgTechEmail: search-apnic-not-arin@apnic.net
OrgTechRef: https://whois.arin.net/rest/poc/AWC12-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

CAPÍTULO 5 CONCLUSIONES

El crecimiento acelerado de las nuevas tecnologías de información y comunicación ha incrementado el número de usuarios conectados a internet, solo en el 2016 en México son 71.5 millones de usuarios conectados a internet, revelado por el Estudio de Consumo de Medios y Dispositivos en internautas mexicanos. Realizado por Kantar Millward Brown y patrocinado por Televisa Digital.

De acuerdo con el estudio, el 74% de la población en México cuenta con correo electrónico, es decir que en México son 52.91 millones de usuarios que están expuestos a ser atacados por diferentes tipos de ataques informáticos.

Desde el comienzo del uso generalizado de las tecnologías de la información han existido intentos por acceder a información confidencial o personal. Se ha enfocado el tema desde el punto de vista de unas herramientas indispensables que toda organización debe contemplar dentro de sus políticas de seguridad y enmarcada dentro del proceso de respuesta a incidentes en los sistemas informáticos.

Las herramientas que se describen en el presente documento son capaces de rastrear correos electrónicos desde el lugar donde se originó ciertas herramientas descritas en el capítulo 3 de este documento y son utilizadas en el análisis forense digital.

Se instalaron 2 herramientas de rastreo de correo electrónico (IPNetInfo y EmailtrackerPro), de igual forma se utilizaron 2 herramientas en línea para el rastreo de correo electrónico (Trace Email Analyzer y EmailTracer).

Se analizó un correo electrónico elegido al azar para analizar los diferentes resultados obtenidos de las 4 herramientas mencionadas anteriormente. El correo electrónico analizado resulto ser un ataque de spam, con esto podemos deducir que nuestro servicio de mensajería de Hotmail tiene algunas deficiencias en cuanto a sus políticas de seguridad.

En la siguiente tabla se muestra un comparativo en cual se puede apreciar las diferencias que se encuentran en cada una de las herramientas que fueron utilizadas para el rastreo de correo electrónico.

Herramientas de software para raestreo	IPNetInfo	EmailtrackerPro	Trace EmailAnalyzer	Email Tracer
Seguimiento del correo electrónico mediante el encabezado.	● Si	● Si	● Si	● Si
Geolocalización mediante un mapa mundial.	× No	● Si	● Si	× No
Traza de direcciones IP de forma cronológica.	× No	● Si	× No	● Si
Reporte de abuso.	× No	● Si	× No	× No
Filtro de spam.	× No	● Si	× No	× No
Red de datos de Whois "identifica los datos del emisor".	● Si	● Si	● Si	● Si
Data Domain Whois "identifica los detalles de contacto del dominio que se emplea".	● Si	● Si	● Si	● Si
Identifica la IP del remitente/emisor.	× No	● Si	× No	● Si
Identifica la IP del origen del correo electrónico.	● Si	● Si	● Si	● Si
Identificación del nombre del país/ estado del origen del correo electrónico.	● Si	● Si	● Si	● Si
Rango de direcciones IP.	● Si	× No	× No	× No
Información de contacto (dirección, teléfono, fax y correo electrónico).	● Si	● Si	× No	● Si

La propuesta de varias aplicaciones de software mencionada en los capítulos anteriores y en la tabla anterior sirve para el procedimiento de indagación y recopilación de evidencia informática ante un posible caso de delito informático.

Las 4 herramientas mencionadas anteriormente están diseñadas para el rastreo de correo electrónicos mediante los encabezados, direcciones IP o por medio de las cuentas de correo electrónico. No todas las herramientas cuentan con suficiente información como para ser tomadas en cuenta para la recopilación de evidencia informática ante un delito informático.

Los resultados obtenidos del análisis del rastreo de correos electrónicos mediante las herramientas mencionadas anteriormente en la tabla, se puede observar que la herramienta más completa es EmailtrackerPro al mostrar un informe más completo, adicionalmente se integra con Microsoft Outlook, y muy importante: detecta tácticas de ocultamiento de direcciones de personas o equipos, una táctica muy utilizada por los famosos “spams”. Por la que la considero como una de las herramientas más completas en rastreo de correos electrónicos y que todo usuario o administrador de red debe de tomar en cuenta para la decisión o reforzamiento de las políticas de seguridad.

En conclusión, he pretendido recoger una pequeña muestra de herramientas informáticas forense utilizadas en el análisis de rastreo de correo electrónicos para darle a conocer a los usuarios que existen herramientas que se pueden contemplar para las políticas de seguridad en las empresas.

.

Bibliografía

(s.f.).

Symantec Corporation . (02 de 03 de 2015). *Cómo atacan las Vulnerabilidades*. Obtenido de Norton Security: http://mx.norton.com/security_response/vulnerabilities.jsp

Abreu, F. (2006). *"Spoofing" en Fundamentos y aplicaciones de seguridad.* Barcelona: Marcombo S.A .

Apachefriends. (27 de Septiembre de 2015). Obtenido de https://www.apachefriends.org/es/index.html

Areitio, J. (2008). *Identificación de vulnerabilidades.* Madrid: Cengage Learning Parainfo, S.A.

Barceló Ordinas, J. M. (2008). *Correo Electrónico Internet.* Barcelona: UOC.

Benbunan, A. (29 de Septiembre de 2011). *Historia del Correo electrónico.* Barcelona: Centro de Libros PAPF, S.L. U. Obtenido de http://tomcat.apache.org/

BeyondTrust. (25 de Septiembre de 2015). *BeyondTrust*. Obtenido de http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/

Caprani, G. (2006). *Virus, antivirus y firewall.* Barcelona: Ediciones eni .

Carlos Miguel Pérez, J. A. (2003). *La Biblia del Hacker.* Anaya multimedia.

Castillo Sivianes, F. (2010). *Tipos de Spam.* Madrid: Parainfo, S.A.

Dean, T. (2009). *IMAP.* Boston: Cengage Course Technology.

Dean, T. (2009). *IMAP.* Boston: Cengage Course Technology.

Dean, T. (2009). *SMTP.* Boston: Cengage Course Technology.

Delisle, M. (2007). *Dominar phpMyAdmin para una administración efectiva de MySQL.* Packt publishing.

FileZilla. (28 de Septiembre de 2015). Obtenido de https://filezilla-project.org/client_features.php

Francisco Marciá Pérez, F. J., A Barca, V. D., & José Vicente Berná Martínez, J. H. (2009). *Administracíon de Servicios de Internet. De la teoria a la práctica.* Universidad de Alicante.

Gómez Andreu, J. (2010). *Formato de los mensajes de correo electrónico.* Madrid: Editex, S.A. .

Gómez Andreu, J. (2010). *Tipos MIME.* Madrid: Editex, S.A.

Harris, D. (28 de Septiembre de 2015). *Pegasus Mail*. Obtenido de http://www.pmail.com/overviews.htm

Huidobro Maya, J. M. (2007). *MIME.* Madrid: Parainfo, S.A. .

Izaskun Pallejero, F. A. (2006). *Fundamentos y aplicaciones de Seguridad en Redes WLAN: De la teoría a la practica.* Marcombo.

Linux Máxima Seguridad. (2000). Madrid: Pearson Educacion.

Maryann, B. M. (2001). *POP (Protocolo de Oficina Postal").* Miami: Pearsoneducacion.

Microsoft TechNet. (29 de Septiembre de 2015). Obtenido de https://technet.microsoft.com/library/hh852345.aspx

Moro, M. (2010). *Historia del Correo Electrónico.* Madrid: Parainfo.

Pablo Gonzáles Pérez, G. J. (2013). *Pentesting con Kali.* 0xWORD Computing S.L .

Pacheco, F. G. (2012). *"Phishing" en Ethical Hacking.* Buenos Aires: Users.

Panda Security. (16 de Septiembre de 2015). Obtenido de http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/

Peláez, R. S. (2002). *Historia de las vulnerabilidades.* Madrid: O Reilly & Associates, Inc.

phpMyAdmin. (27 de Septiembre de 2015). Obtenido de https://www.phpmyadmin.net/

Rapid7. (15 de Septiembre de 2015). Obtenido de http://www.rapid7.com/es/products/nexpose/

Royer, J.-m. (2004). *Los Caballos de Troya.* Barcelona: Ediciones eni.

Saavedra Fernández, T. (2014). *Ventajas del protocolo IMAP.* Malaga: IC.

Saavedra Fernández, T. (2014). *Ventajas del protocolo POP.* Malaga: IC.

SAFETY-LAB. (23 de Septiembre de 2015). Obtenido de http://www.safety-lab.com/en/products/securityscanner.htm

Sergio, G. R. (02 de Febrero de 2017). *http://www.lcc.uma.es/~galvez/javamail.html.* Obtenido de http://www.lcc.uma.es/~galvez/javamail.html: http://www.lcc.uma.es/~galvez/javamail.html

Tanenbaum, A. S. (2003). *Arquitectura y servicios.* México: Pearson Educación de México, S.A de C.V. .

Tanenbaum, A. S. (2003). *Correo electrónico.* México: Pearson Educación de México, S.A de C.V.

Tanenbaum, A. S. (2003). *Correo electrónico.* México: Pearson Educación de México, S.A de C.V.

Tanenbaum, A. S. (2003). *Correo electrónico.* México: Pearson Educación de México, S.A de C.V.

Tenable Nessus. (15 de Septiembre de 2015). Obtenido de http://www.tenable.com/documentation/nessus/#/

ANEXOS

ANEXO A

HERRAMIENTAS DE INFORMÁTICA FORENSE DE CODIGO ABIERTO

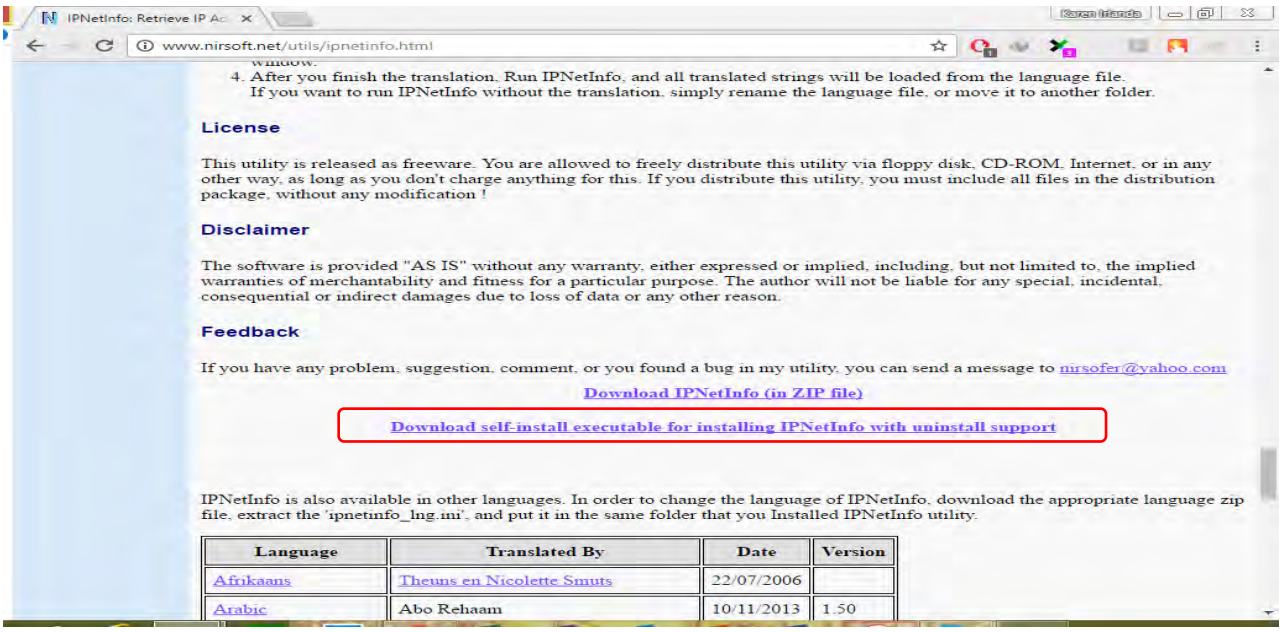
INSTALACIÓN IPNETINFO

Requisitos del sistema

El sistema operativo Windows: Windows 98/ME/2000/XP/2003/Vista/ Windows 8.1.
Conexión a Internet.
En un firewall, debe permitir conexiones salientes al puerto 43.

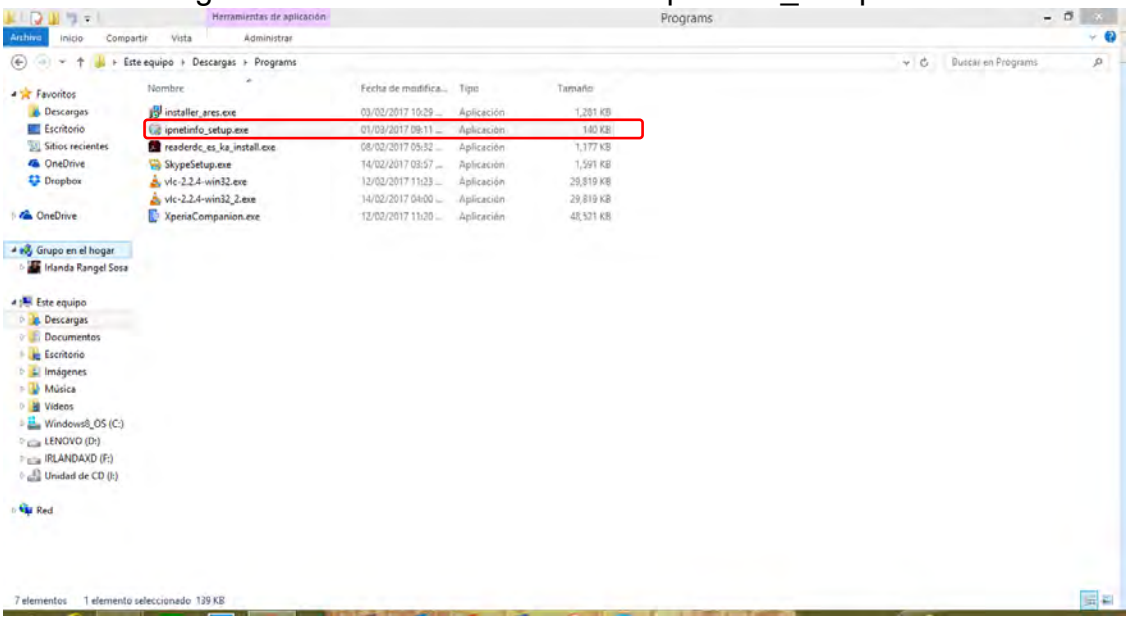
Instalación IPNetInfo

1. Ingresamos a la página web http://www.nirsoft.net/
2. En la sección Internet Related Utilities, elegimos IPNetInfo
3. En la página de IPNetInfo seleccionamos la opción download self-install executable for installing IPNetInfo with uninstall support como se muestra en la ilustración.



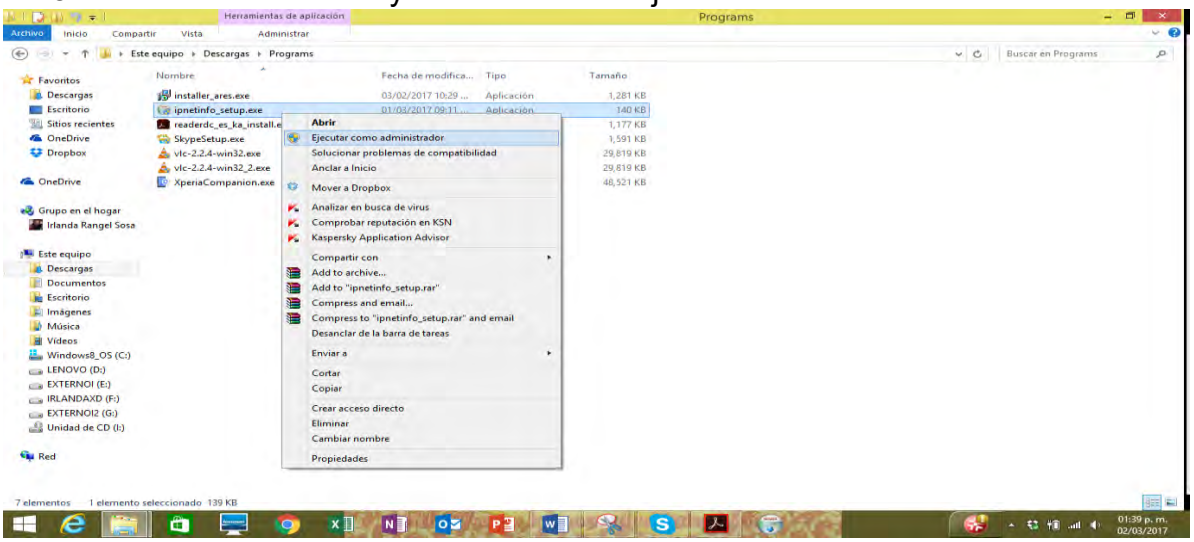
Opción de descarga IPNetInfo

4. descargamos el instalador con nombre ipnetinfo_setup.exe



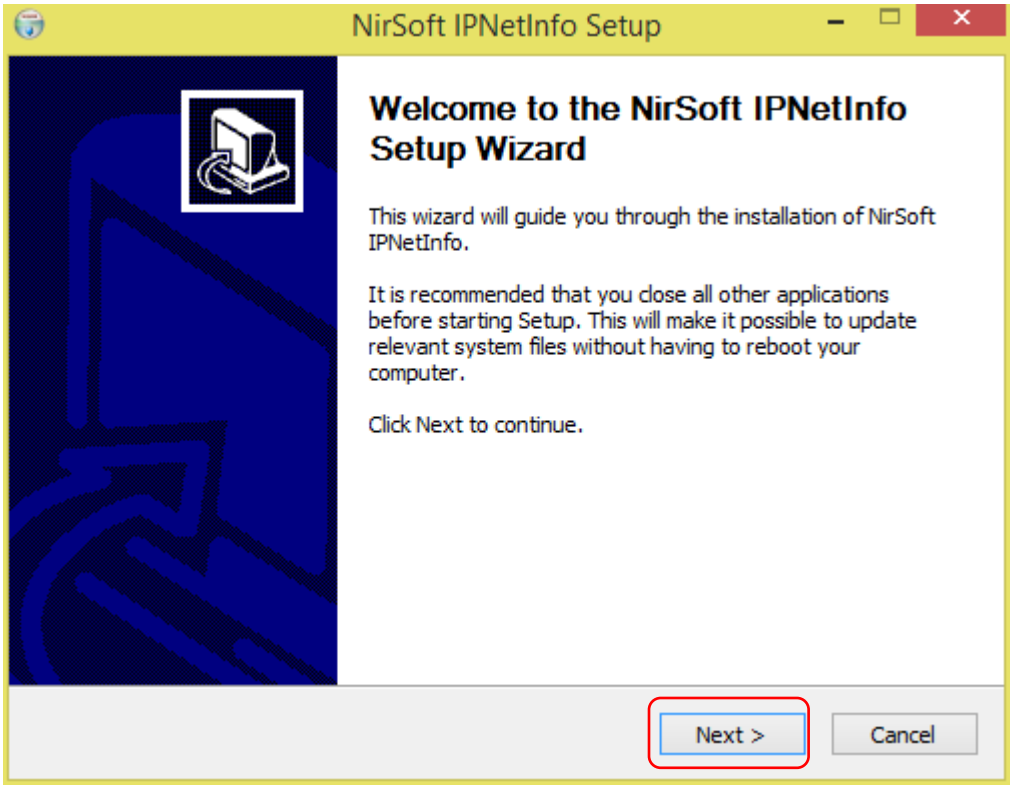
Instalador IPNetInfo

5. Damos clic derecho y seleccionamos ejecutar como administrador



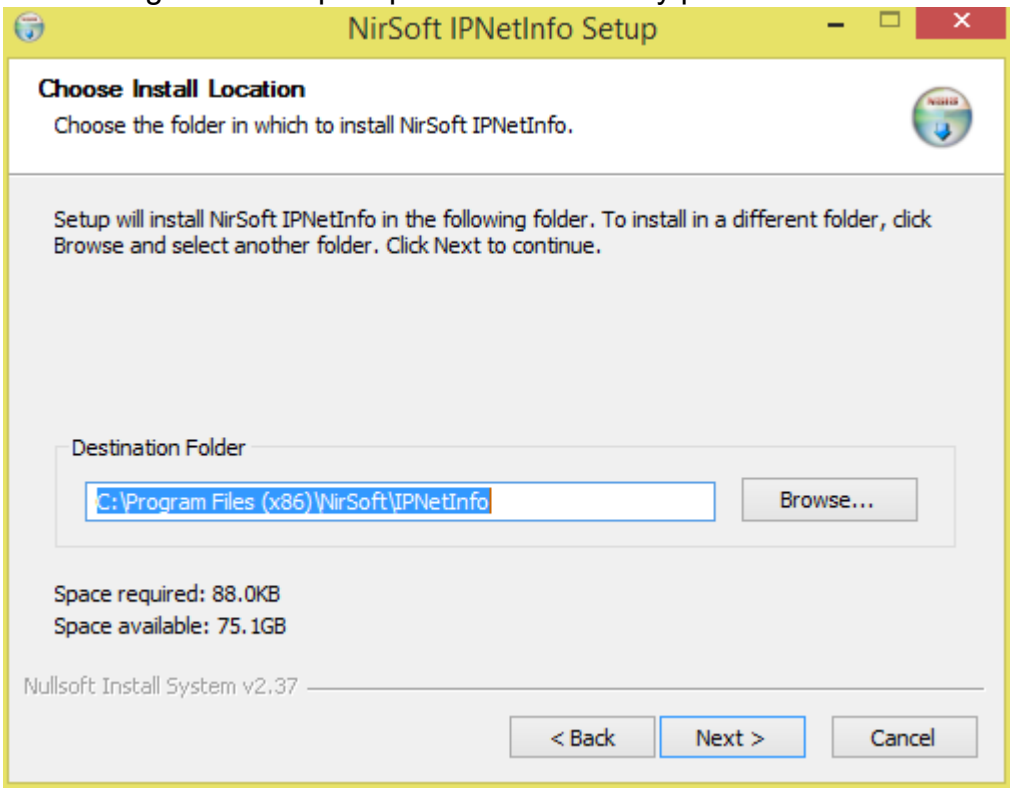
Inicio de instalación IPNetInfo

6. Enseguida se abre la ventana del asistente de instalación, pulsamos en **Next**.



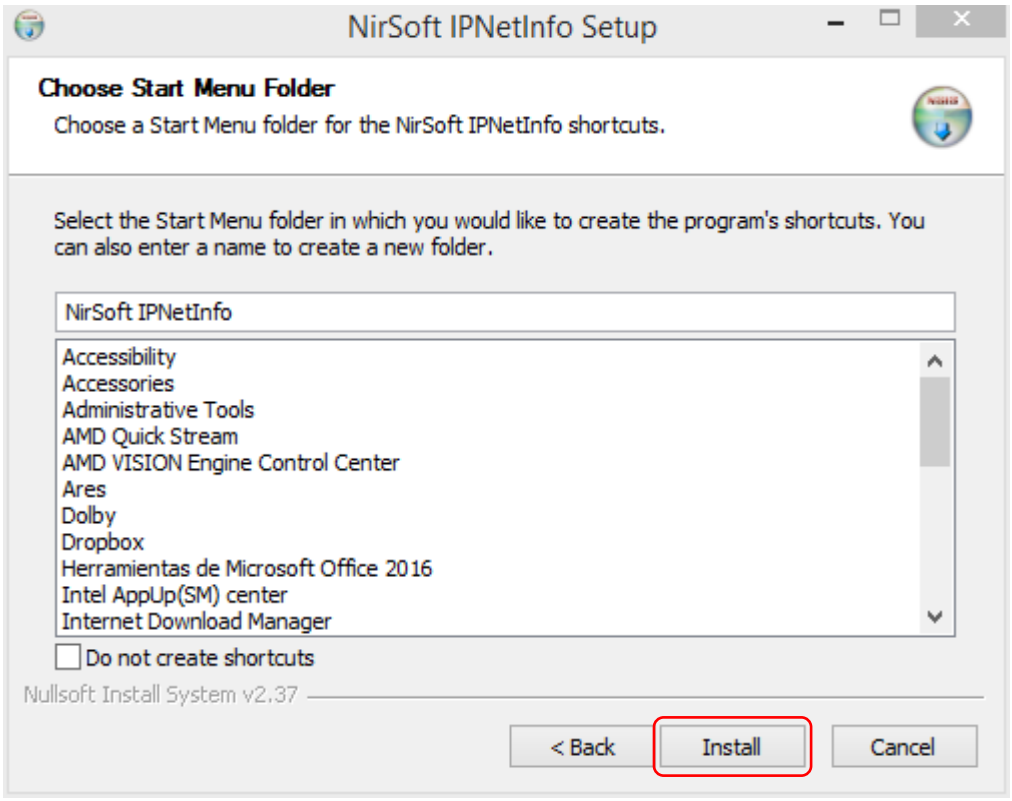
Asistente de instalación IPNetInfo

7. Elegimos la carpeta para la instalación y pulsamos en **Next.**



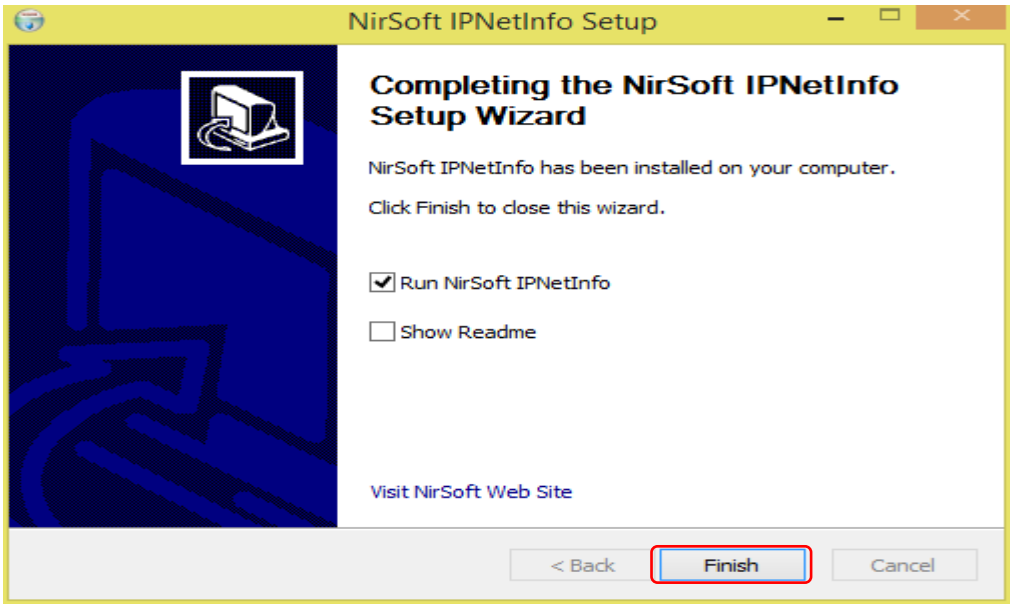
Ventana NirsSoft IPNetInfo Setup

8. Seleccionamos la carpeta del menú de inicio para crear los accesos directos del programa y pulsamos **Install.**



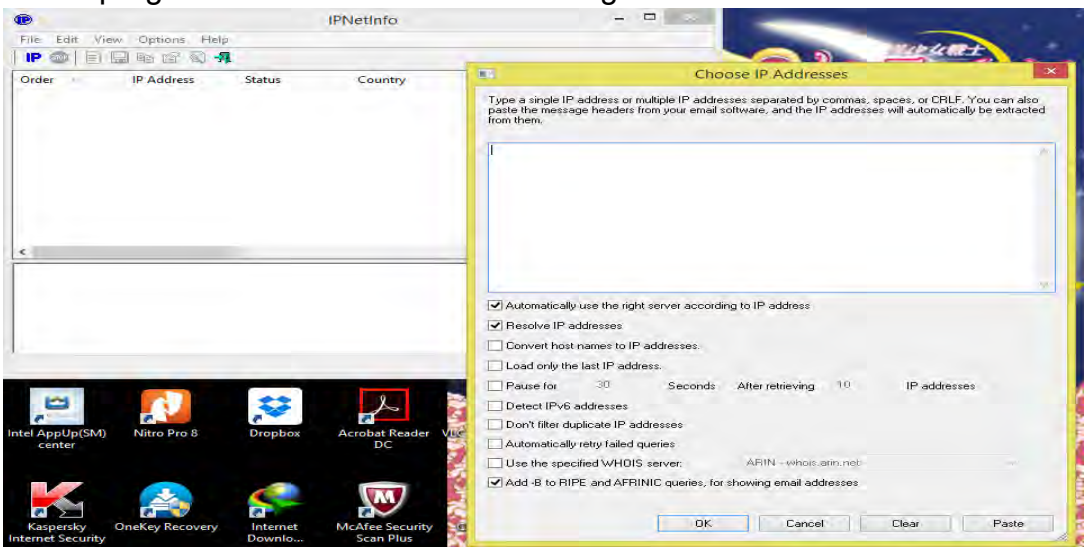
Ventana de selección de menú principal

9. Una vez que la instalación esté completada pulsamos **Finish.**



Ventana de instalación completa IPNetInfo

10. Al finalizar la instalación de IPNetInfo aparecerá la pantalla para empezar a utilizar el programa como se muestra en la siguiente ilustración.



Pantalla de inicio IPNetInfo

INSTALACIÓN DE EMAILTRACKERPRO

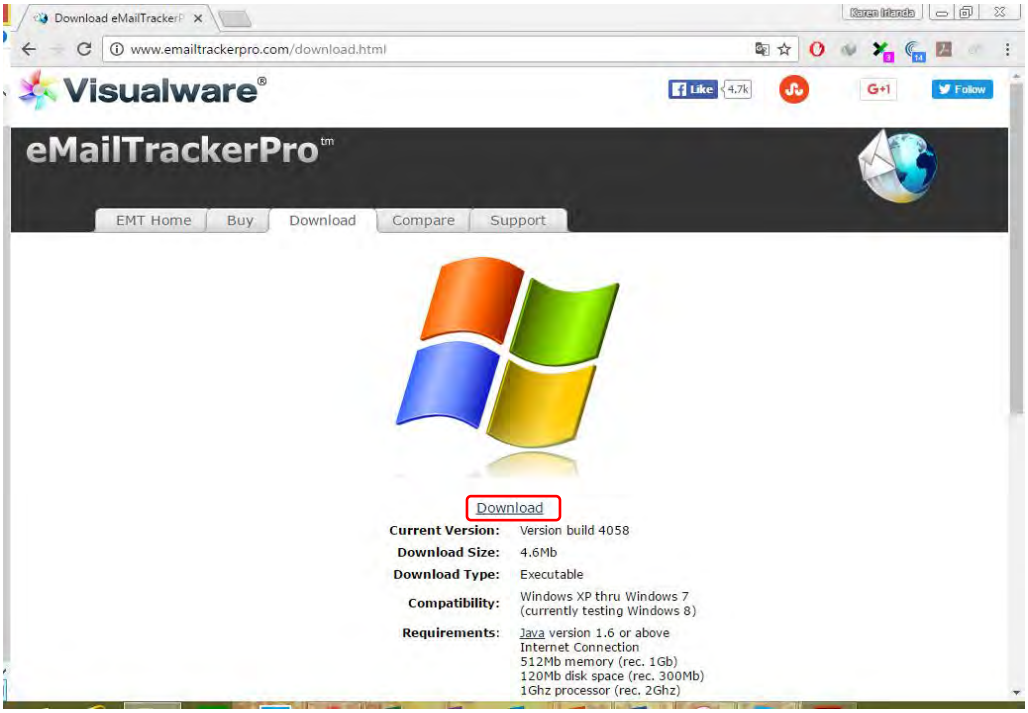
Requisitos del sistema

Sistema Operativo Windows 2000/XP/2003/Vista/7/8
Requerimientos adicionales Java 1.6 o superior.

1. Ingresamos a la página web http://www.emailtrackerpro.com/, seleccionamos la pestaña Download como aparece en la siguiente ilustración.

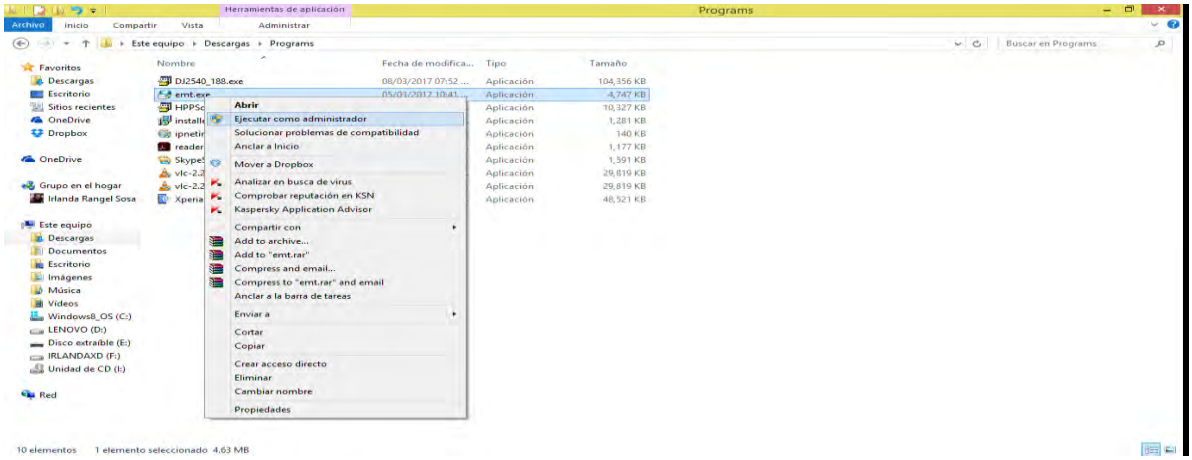
Página oficial EmailtrackerPro

2. Una vez que estemos en la pestaña de **Download**, seleccionamos **Download** para descargar el instalador de EmailtrackerPro. Como se muestra en la siguiente ilustración.



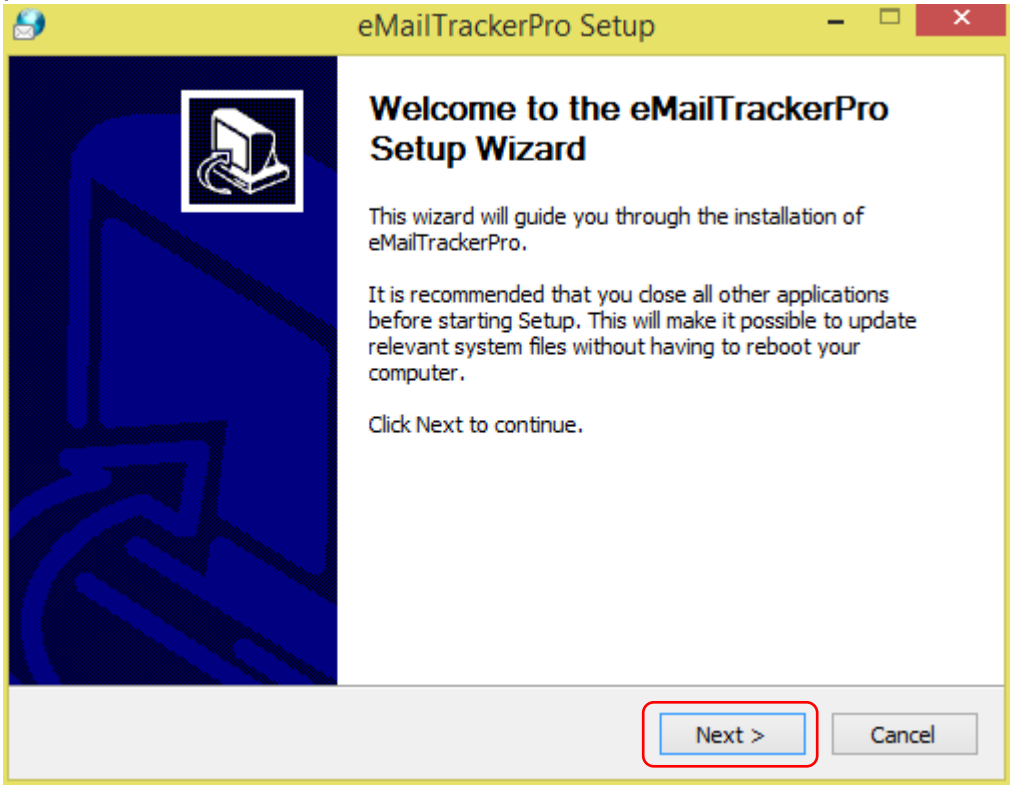
Opción de descarga Emailtrackerpro

3. una vez descargado el programa de instalación de EmailtrackerPro lo ejecutamos como administrador como se muestra en la siguiente ilustración.



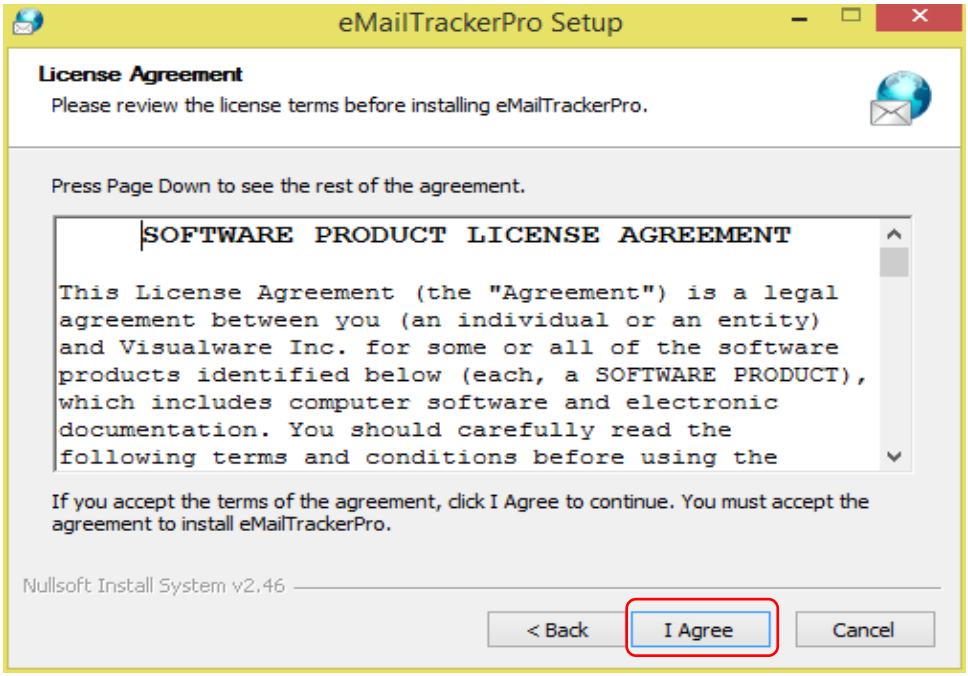
Inicio de instalación EmailtrackerPro

4. Al ejecutarlo nos mostrará el asistente de instalación como se muestra en la ilustración; pulsamos **Next**.



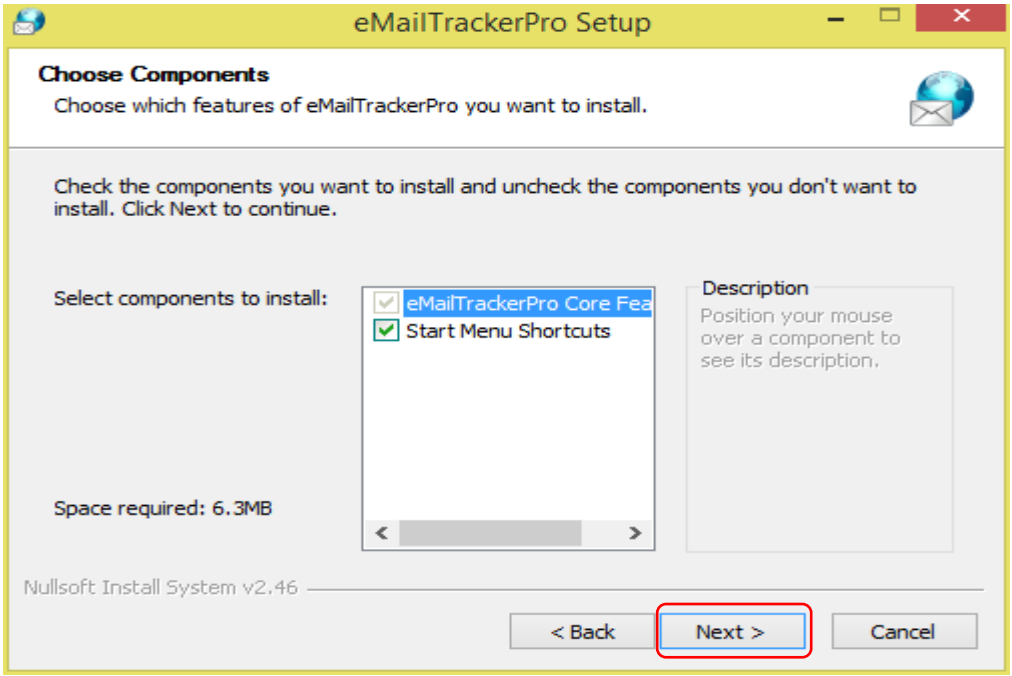
Asistente de instalación de EmailtrackerPro

5. Nos mostrará en pantalla los términos de la licencia, para aceptar los términos de la licencia, pulsamos en **I Agree**, como se muestra en la siguiente ilustración.



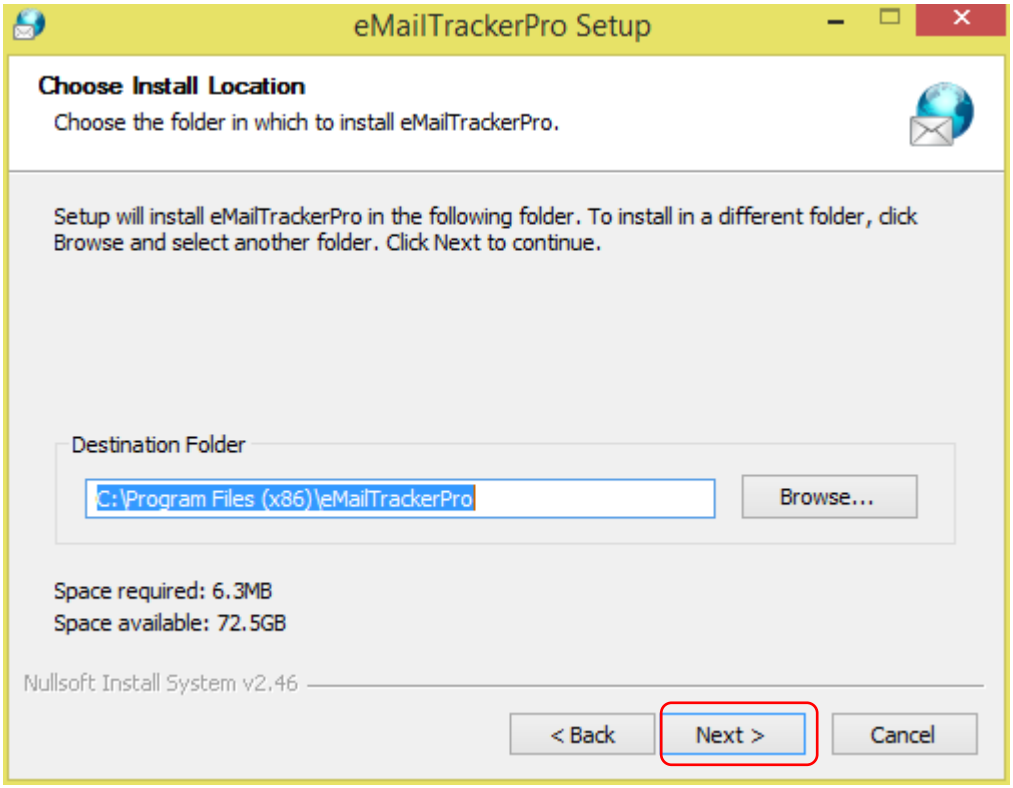
Términos de licencia EmailtrackerPro

6. Seleccionamos las utilidades a instalar y seleccionamos **Next**, como se muestra en la ilustración.



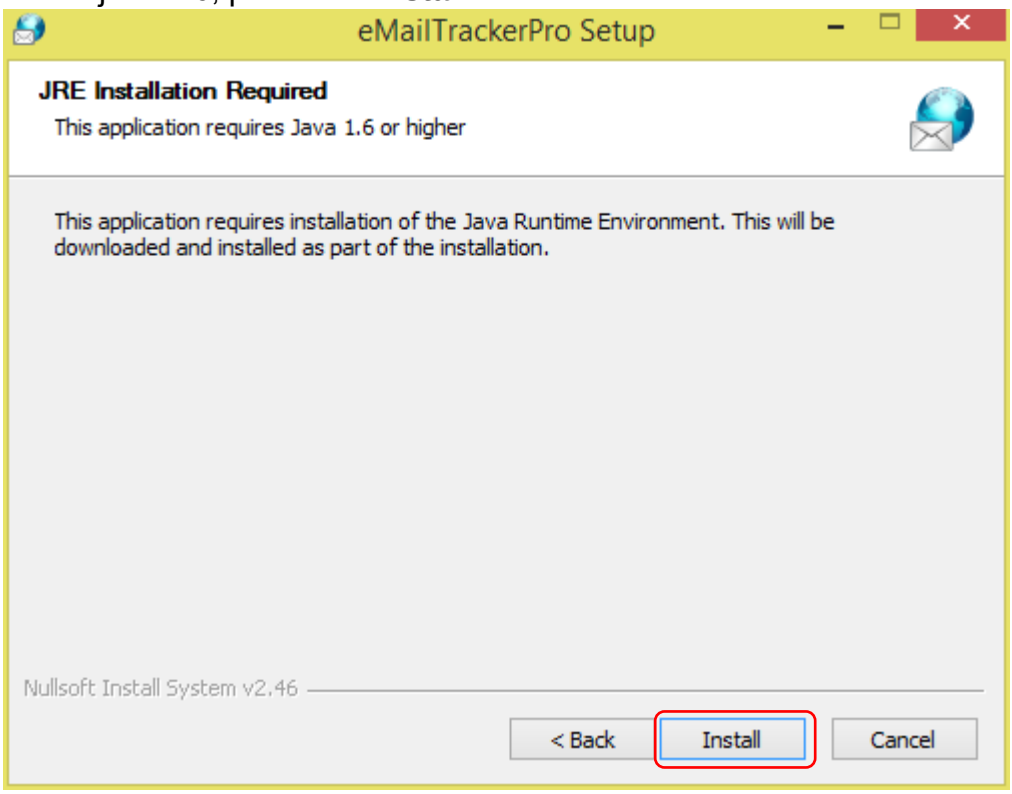
Selección de utilidades de EmailtrackerPro

7. Elegimos la carpeta para la instalación y pulsamos en **Next.**



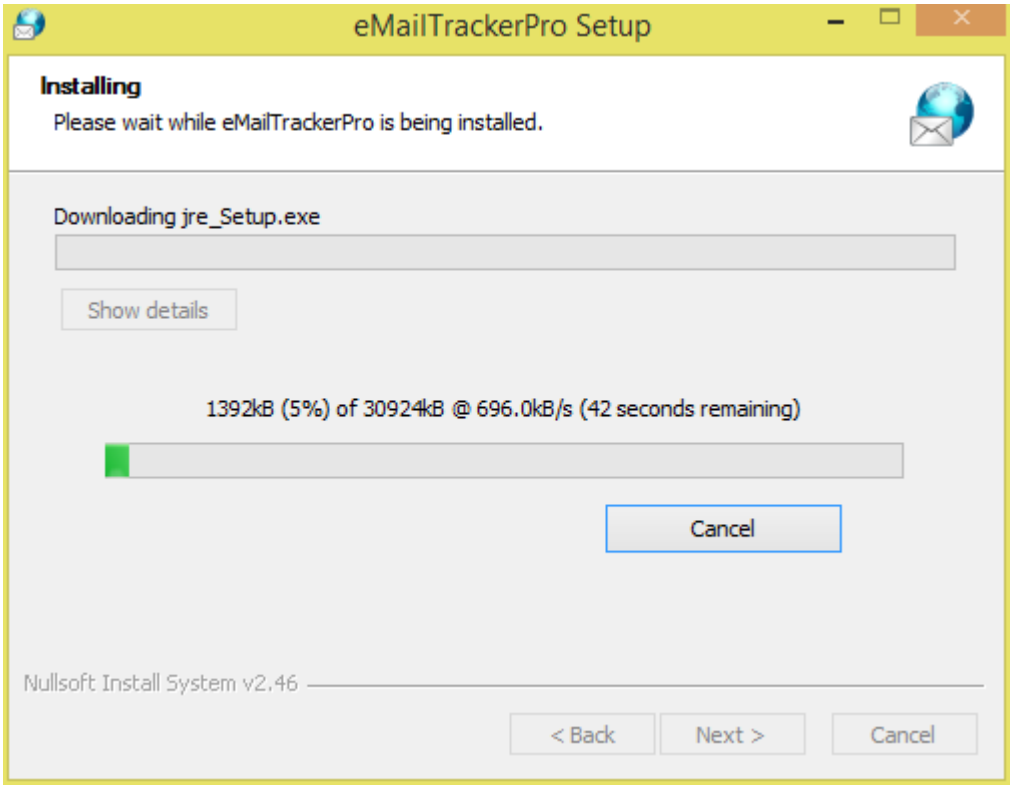
Ubicación de la carpeta de EmailtrackerPro

8. Esta aplicación requiere java 1.6 o superior para el mejor funcionamiento, para instalar java 1.6, pulsamos **Instal**l como se muestra en la ilustración.



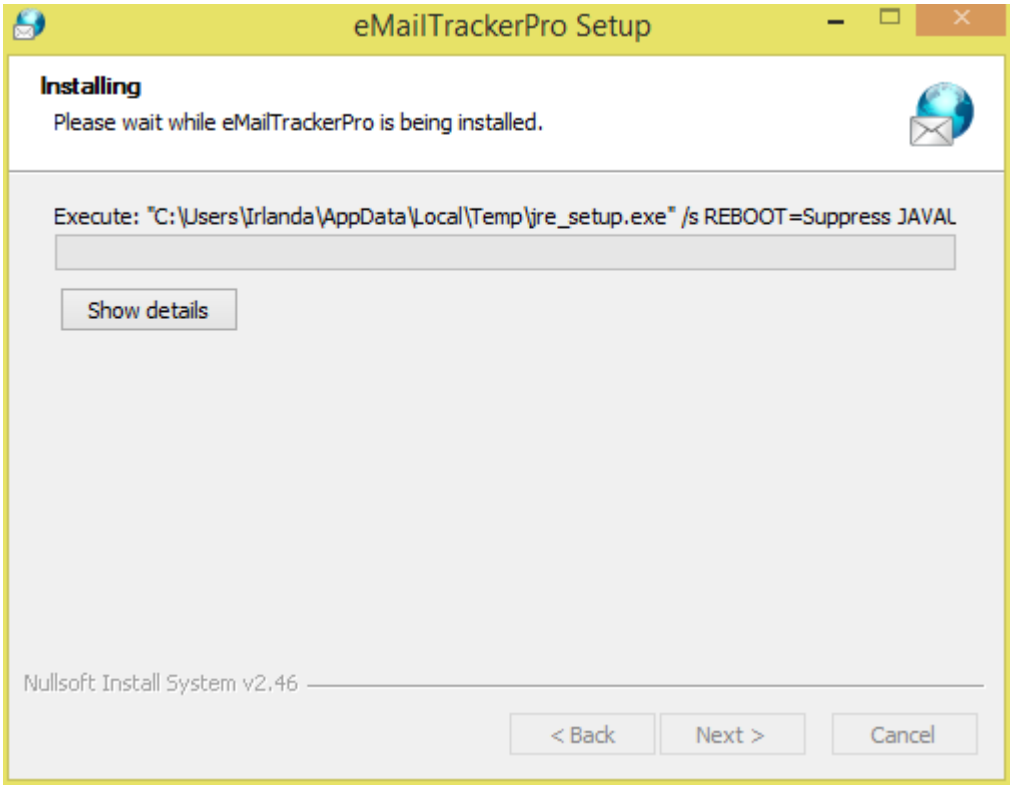
Instalación java en EmailtrackerPro

9. Enseguida nos muestra el proceso de instalación de java como se muestra en la ilustración.



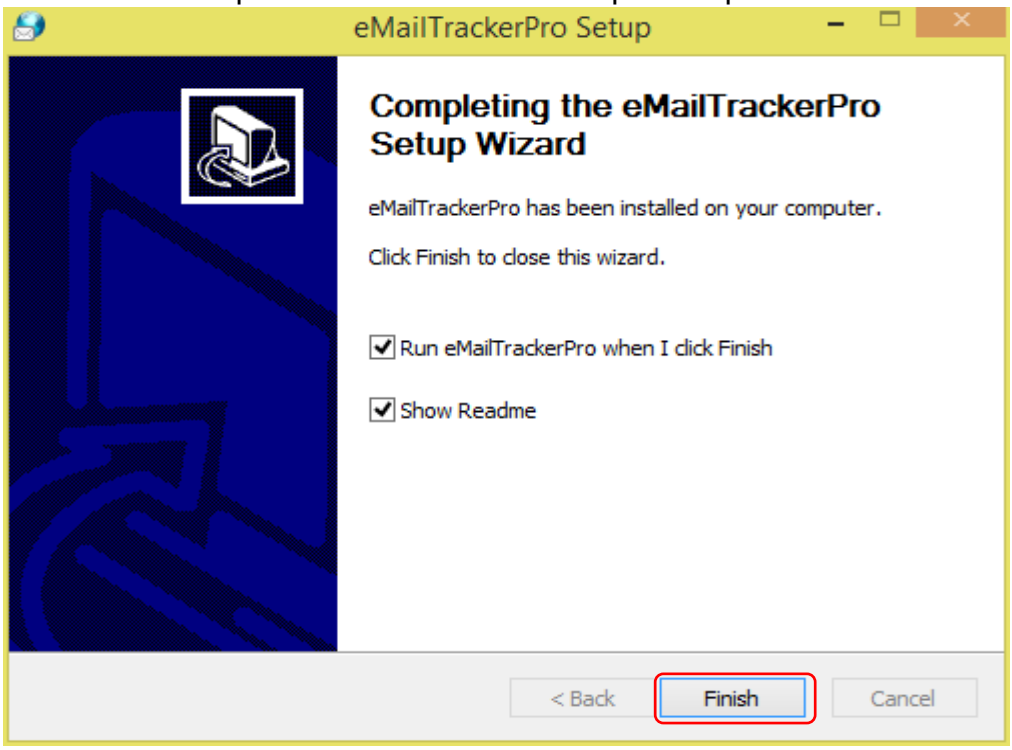
Proceso de instalación de java

10. Una vez que se termina la instalación de java, comienza el proceso de instalación de EmailtrackerPro como se muestra en la ilustración.



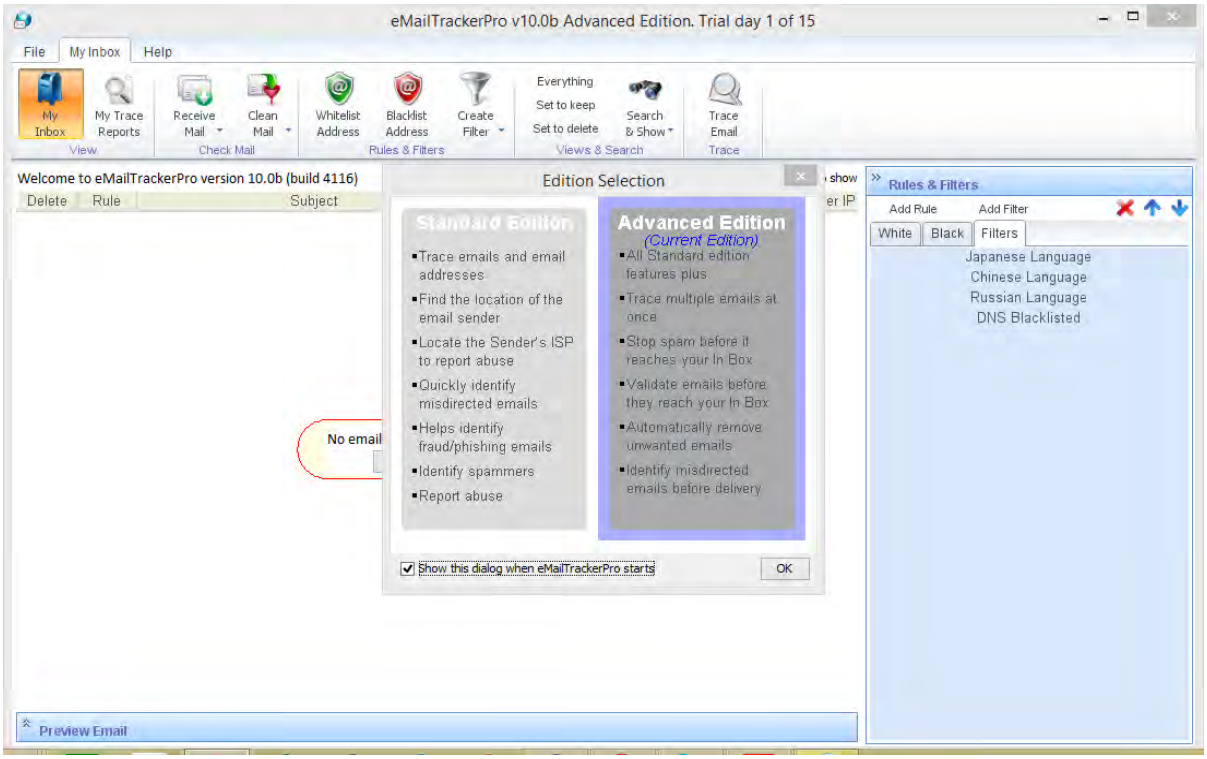
Proceso de instalación de EmailtrackerPro.

11. Una vez que la instalación esté completada pulsamos **Finish**



Ventana de instalación completa

12. Al finalizar la instalación de EmailtrackerPro aparecerá la pantalla para empezar a utilizar el programa como se muestra en la siguiente ilustración.



Pantalla de inicio EmailtrackerPro