Investigaciones vinculadas a

Redes Informáticas e Internet

1.- Traducción efectuada por ArCERT del documento “*Investigations Involving the Internet and Computer Networks “, desarrollado por el “Grupo Técnico de Tareas para la investigación de delitos de alta tecnología” de Estados Unidos.*

Indice de Contenidos

[Presentación 2](#_TOC_250008)

[Capítulo 2. Rastreo de una Dirección IP hasta su origen 3](#_TOC_250007)

[Capítulo 3. Investigaciones relacionadas con el correo electrónico (E-Mail) 15](#_TOC_250006)

[Capítulo 4. Investigaciones relacionadas con Sitios Web 24](#_TOC_250005)

[Capítulo 6. Investigaciones relacionadas con redes que comparten archivos 29](#_TOC_250004)

[Capítulo 7. Investigaciones sobre Intrusiones en la Red/Ataques de Denegación de Servicio. 34](#_TOC_250003)

[Apéndice A. Glosario 39](#_TOC_250002)

[Apéndice C. Acceso a Encabezados Detallados en los Mensajes de Correo Electrónico 42](#_TOC_250001)

[Apéndice D. Lista de Control Sugerida para la Investigación sobre Archivos Compartidos 44](#_TOC_250000)

# Presentación

Este documento es una **traducción del trabajo “Investigaciones que involucran Internet y otras redes informáticas”** ("*Investigations Involving the Internet and Computer Networks*"), desarrollado por el “Grupo Técnico de Tareas para la investigación de delitos de alta tecnología” (“Technical Working Group for the Investigation of High Technology Crimes”) y publicados por el Instituto Nacional de Justicia (National Institute of Justice) de los Estados Unidos de Norte América. El documento orginal se encuentra disponible para su descarga en el siguiente enlace: [*http://www.ncjrs.gov/pdffiles1/nij/210798.pdf*](http://www.ncjrs.gov/pdffiles1/nij/210798.pdf)

Este documento se encuentra orientado a usuarios con conocimientos técnicos o legales, que deseen tener una idea básica sobre cómo debe conducirse una investigación ante un incidente que involucre una red de computadoras.

El objetivo de este documento es introducir los distintos pasos que resultan útiles y necesarios a la hora de realizar una investigación que involucre a Internet o a redes de computadoras. Se presentan técnicas para realizar el rastreo de una dirección IP y para obtener información útil para la investigación, a partir de mensajes de correo electrónico, sitios web y redes para compartir archivos. Por último, se introduce la manera de proceder para realizar investigaciones sobre intrusiones en la red o ataques de denegación de servicio.

Cabe aclarar que se han traducido sólamente aquellos capítulos considerados relevantes o que contengan información útil para realizar investigaciones en la República Argentina. En particular, se omitió la traducción de los capítulos 5 y 9 y de algunas secciones dentro de los otros capítulos ya que hacían referencia a las normas legales vigentes en los Estados Unidos.

Adicionalmente, en algunos capítulos específicos se incluyeron notas de ArCERT con el fin de clarificar algunos puntos o bien, adaptar los contenidos a la realidad de nuestro país.

# Capítulo 2. Rastreo de una Dirección IP hasta su origen

Así como cualquier casa tiene una dirección, cada computadora conectada a Internet también tiene una dirección. A esta dirección se la denomina dirección de Protocolo de Internet (IP – Internet Protocol). Este capítulo explica cómo se asignan las direcciones IP y cómo rastrear las direcciones hasta su origen.

Al investigador también se le pueden presentar otros tipos de direcciones. Algunos ejemplos de estas direcciones son las de correo electrónico y las de World Wide Web (direcciones de sitio Web).

|  |  |
| --- | --- |
| Tipo | Ejemplo |
| Dirección E-mail | [alguien@nist.gov](mailto:alguien@nist.gov) |
| Dirección sitio Web | [www.nist.gov](http://www.nist.gov/) |
| Dirección Protocolo Internet | 129.6.13.23 |

Todas estas direcciones pueden ser rastreadas para obtener indicios de la investigación. Para mayor información sobre direcciones de correo electrónico y sitio Web, referirse a los capítulos específicos. Antes de rastrear una dirección IP, es importante comprender los siguientes conceptos.

## Dirección de Protocolo de Internet

Cada dispositivo[1](#_bookmark0) involucrado en una comunicación vía Internet requiere una dirección IP. Una dirección IP es una serie de cuatro números que van del 0 al 255, separados por puntos. La dirección identifica a la red y al dispositivo específico. El siguiente es un ejemplo de dirección IP:

129.6.13.23

Una analogía sería comparar una dirección IP con la dirección de un departamento. (Ver Figura 1)

1. Por ejemplo, los dispositivos pueden ser computadoras, routers, asistentes digitales personales (personal digital assistants - PDAs), etc.

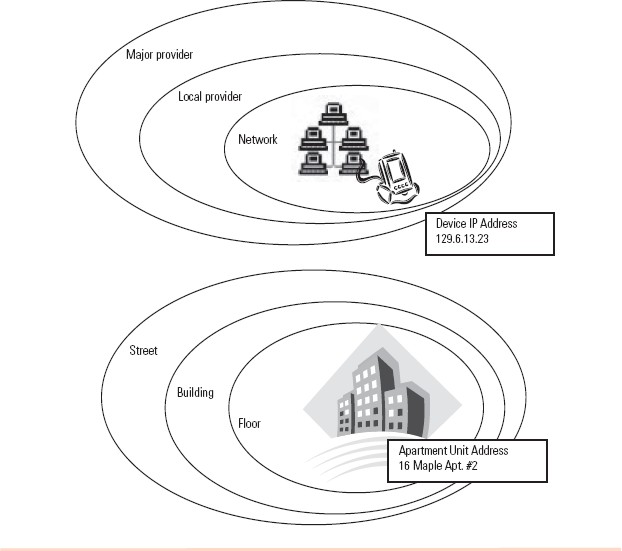


Figura 1. Dirección IP y dirección de un departamento

**Secuencia de la Figura**: Proveedor Mayorista, Proveedor Local, Red, Dirección IP del dispositivo: 129.6.13.23

Calle, Edificio, Piso, Dirección de Unidad de Departamento: 16 Maple Apt. #2

**ADVERTENCIA**: La dirección IP no denota una ubicación física del dispositivo al momento en que está conectado a Internet.

La asignación de dirección IP usa cuatro números separados por puntos que permiten un total de 2564 o 1.099.511.627.776 direcciones únicas. Este esquema de asignación de direcciones se está expandiendo para permitir un uso adicional de Internet. Independientemente del esquema de asignación de direcciones usado, el método de rastreo de dirección IP seguramente seguirá siendo el mismo.

## Dirección IP Privada

Hay tres grupos de direcciones IP específicamente reservados para el uso en redes privadas y que no se encuentran visibles en la Internet pública. La información para estas direcciones IP provienen del propietario de la red. Los rangos son:

|  |  |  |
| --- | --- | --- |
| 10.0.0.0 | a | 10.255.255.255 |
| 172.16.0.0 | a | 172.31.255.255 |
| 192.168.0.0 | a | 192.168.255.255 |

## Proveedores de Servicio de Internet

Los Proveedores de Servicio de Internet (ISPs) pueden ser proveedores comerciales u organizaciones, tales como una empresa o un organismo de gobierno. Ellos pueden reservar bloques de direcciones IP que pueden ser asignadas a sus usuarios.

Los ISPs pueden registrar fecha, hora, información de la cuenta de usuario e *Identificación Automática de Número (ANI - Automatic Number Identification)* o identificación de llamada entrante o la que inicia la llamada al momento de la conexión. Si se recuerdan los registros de eventos (*logs*), éstos se pueden mantener durante un tiempo limitado dependiendo de la política establecida del ISP. Actualmente, no existe ningún requerimiento legal general para la conservación de los registros de eventos; por lo tanto algunos ISPs no almacenan registros de eventos. En el caso que se requieran registros de eventos en particular para la investigación, es importante preparar y presentar una nota de solicitud de conservación como se describe en el Capítulo 9[2](#_bookmark1).

**Nota ArCERT**: En Argentina, en el caso que se requieran registros de eventos en el marco de una causa judicial, a petición de parte o de oficio, el juez solicitará al ISP, mediante el libramiento de un oficio, la información pertinente, no pudiendo el ISP negarse a proveerla.

## Direcciones de IP dinámicas y estáticas

Las direcciones de IP “Dinámicas” se asignan temporalmente desde un conjunto de direcciones disponibles registradas para un ISP. Estas direcciones son asignadas a un dispositivo cuando un usuario comienza una sesión online. Por este motivo, una dirección IP de un dispositivo puede variar de una sesión a la siguiente.

Las direcciones de IP “Estáticas” se asignan permanentemente a dispositivos configurados para que siempre tengan la misma dirección IP. Una persona, empresa u organización que mantiene una presencia constante en Internet, tal como un servidor Web, generalmente requiere una dirección IP estática.

1. Nota ArCERT: El Capítulo 9 no se traducirá ya que refleja las normas vigentes en Estados Unidos. Para completar, ArCERT incluye algunas notas referentes a las normas legales vigentes en la República Argentina.

**Nota**: Se debe determinar la fecha y la hora en que una dirección IP fue asignada, para relacionarla a un dispositivo específico o cuenta de usuario. El ISP puede mantener un historial de archivos de registros de eventos (*log files*) que relacionan estas direcciones IP asignadas dinámicamente con un suscriptor o un usuario en particular, en un momento en particular.

## Paquete

Los datos enviados por Internet están divididos en ***paquetes*** que son enrutados a través de Internet y rearmados en el destino. Cuando información tal como archivos, mensajes de correo electrónico, documentos HyperText Markup Language (HTML), o páginas Web se envían de un lugar a otro dentro de una red, su sistema operativo divide la información en “trozos” (*chunks*) de un tamaño eficiente para el ruteo. Cada uno de estos paquetes incluye la dirección de destino. Cada paquete puede viajar por diferentes rutas a través de una red. Cuando llegan todos los paquetes, son rearmados nuevamente en el archivo original.

**Nota**: Capturar paquetes está más allá del alcance de este informe especial. Sin embargo, los registros de transmisión de un paquete a través del dispositivo de red pueden ser retenidos en los registros de eventos (logs) de ese dispositivo. Puede ser necesario trabajar con el administrador de la red para obtener estos archivos de registros de eventos.

## Dispositivos y servicios de Red

Los dispositivos y servicios de red incluyen **routers**, ***firewalls****,* ***proxy servers/gateways****,*

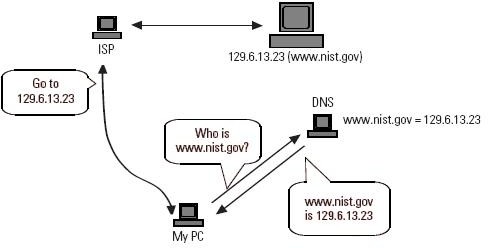
***Network Address Translation (NAT****),* y ***Dynamic Host Configuration Protocol (DHCP)****.*[*3*](#_bookmark2)Por diseño, estos dispositivos y servicios pueden tener o no una función *Logging* que captura información sobre las direcciones IP de la fuente y el destino, el nombre de *login* de usuario, y la fecha y hora de los *logins*. Algunos o todos estos dispositivos y servicios de red pueden alterar o enmascarar la verdadera dirección IP de origen o de destino. Puede ser necesario trabajar con el administrador de la red para determinar la verdadera dirección IP fuente o de destino.

## Servidores de Sistema de Nombre de Dominio (DNS servers)

Los servidores de Sistema de Nombre de Dominio (DNS) son las “guías telefónicas” de Internet. Mantienen los directorios que combinan las direcciones IP con los dominios registrados y descifran el texto que la gente comprende (el nombre de domino) en un formato que los dispositivos comprenden (la dirección IP).

En la Figura 2, My PC envía el pedido para la locación de “[www.nist.gov.](http://www.nist.gov/)” El servidor DNS responde con la dirección de IP asignada de “129.6.13.23”. My PC luego solicita que se muestren los datos desde la dirección IP 129.6.13.23, la computadora en Internet que alberga (*hosts*) el sitio web nist.gov.

1. Las definiciones de router, firewall, proxy server/gateway, Network Address Translation (NAT) y Dynamic Host Configuration Protocol(DHCP), se encuentran en el ANEXO A.

Figura 2. Sistema de Nombres de Dominio (Domain Name System) (DNS)

## Registro de nombres de dominio

Una persona u organización puede registrar un nombre de dominio siempre y cuando no esté ya registrado. Los nombres de dominio están registrados en la Internet Corporation for Assigned Names and Numbers (ICANN), una organización sin fines de lucro responsable de la asignación de la dirección de Internet y del manejo del servidor de nombre de dominio.

La información requerida para registrar un dominio consiste en: nombre, domicilio, número de teléfono, dirección de correo electrónico e información técnica y administrativa de contacto. Además de esta información, puede estar disponible en el registro la fecha en la que el dominio fue registrado. Aunque esta información puede suministrar indicios para la investigación, el investigador debería saber que la información es originada por la persona que registra el dominio y puede ser ficticia.

## Alteración con fines fraudulentos, enmascarado y redireccionado (spoofing, masking, and redirecting)

Los métodos avanzados para ocultar acciones en Internet incluyen esconder/ocultar la dirección IP, pretender ser otra persona y enviar tráfico a través de otra dirección IP.

Estos métodos comúnmente se denominan como masking (enmascarado) [4](#_bookmark3), spoofing (alteración con fines fraudulentos)[5](#_bookmark4) y redirecting (redireccionado) [6](#_bookmark5). Se requiere de un entrenamiento avanzado para investigar o identificar cuándo se practicaron estas acciones. Por lo tanto, aún luego de completar el proceso legal, todavía puede ser necesario usar los métodos de investigación tradicionales para identificar al usuario final. En algunos casos el “*masking*”, el

1. IP masking: el enmascaramiento de IP es un método para esconder u obstruir la fuente verdadera de la dirección IP.
2. IP spoofing: la alteración de IP es un método para personificar (hacerse pasar por) la dirección IP de otro sistema.

“*spoofing*” o el “*redirecting*” pueden impedir la identificación del usuario.

## Rastreo (Tracing) de una dirección IP o nombre de dominio

##### Escenario

Una persona hace un reclamo aduciendo que mientras estaba navegando por Internet, se encontró con un sitio Web que ella cree que debería ser revisado por una autoridad competente. La persona da el nombre del sitio Web d[e www.nist.gov.](http://www.nist.gov/)

##### Paso 1. Determinar el nombre de dominio

El primer paso es resolver el nombre de dominio de [www.nist.gov](http://www.nist.gov/) a una dirección IP. Se dispone de muchas herramientas de software comerciales para asistir al investigador en la tarea de resolver los nombres de dominio a direcciones IP. Además, muchos sitios Web disponibles públicamente descifrarán los nombres de dominio. Algunos de los sitios Web más comúnmente usados incluyen los siguientes:

[www.network-tools.com](http://www.network-tools.com/) [www.samspade.org](http://www.samspade.org/) [www.geektools.com](http://www.geektools.com/) [www.dnsstuff.com](http://www.dnsstuff.com/)

**Nota**: Los sitios de arriba contienen más de una herramienta.

Las características y el nivel de detalle disponible en los sitios de arriba mencionados pueden diferir. Las utilidades comunes de estos sitios Web incluyen las siguientes funciones:

|  |  |
| --- | --- |
| whois (quién es) | Una función que busca en una base de datos que incluye nombres de dominio, direcciones IP, y puntos de contacto, incluyendo nombres, direcciones postales, y números de teléfono. |
| nslookup (búsqueda NS) | Una función que busca un servidor de nombre de dominio para un nombre en particular y da direcciones IP para un dominio en particular. Precaución: Las direcciones IP pueden no ser devueltas desde una fuente validada y por lo tanto podrían ser erróneas. |
| traceroute (rastreo de ruta) | Una función que intenta rastrear el camino que un paquete toma cuando viaja desde un dispositivo a otro. Traceroute (rastreo de ruta) puede ayudar a focalizar la ubicación geográfica de un dispositivo en particular. |

**Nota**: Los investigadores deberían saber que las investigaciones realizadas sobre estos sitios podrían ser monitoreadas y registradas. Es importante conducir las investigaciones delicadas desde una computadora que no pueda ser rastreada de manera tal que permita identificar la agencia de investigación.

##### Paso 2. Determinar y registrar la inscripción/registración del nombre de dominio

1. IP redirecting: el redireccionamiento de IP es un método para enviar o rutear el tráfico de Internet a una dirección IP oculta.

El paso siguiente es determinar y registrar la información sobre inscripción/registro del nombre de dominio. Se pueden usar los siguientes recursos para obtener información sobre el registro:

[www.network-tools.com](http://www.network-tools.com/) [www.samspade.org](http://www.samspade.org/) [www.geektools.com](http://www.geektools.com/) [www.apnic.net](http://www.apnic.net/) (Asia) [www.checkdomain.com](http://www.checkdomain.com/) [www.lacnic.net](http://www.lacnic.net/) [www.ripe.net](http://www.ripe.net/) (Europa) [www.whois.com](http://www.whois.com/) [www.dnsstuff.com](http://www.dnsstuff.com/)



Figura 3. Registro del nombre de dominio

La Figura 3 muestra la información de inscripción/registro para [www.nist.gov](http://www.nist.gov/) y la descifra en la dirección IP 129.6.13.23. La información típica brindada incluye:

* + Nombre y dirección del propietario registrado.
  + Información sobre facturación.
  + Contacto administrativo.
  + Rango de direcciones IP asociadas con el dominio.
  + Información de contacto técnica.

Los contactos listados pueden brindar información adicional acerca de la computadora específica que se está buscando, incluyendo su ubicación y la persona designada, para iniciarle el proceso legal.

**Nota**: Se puede usar el mismo proceso para resolver una dirección IP hacia un nombre de dominio, para obtener la información de contacto.

##### ¿Dónde está la evidencia?

La información puede encontrarse en numerosos lugares, incluyendo:

* La computadora del usuario.
* El ISP del usuario.
* El ISP de la víctima y/o sospechoso.
* Los archivos de registro de eventos (logs) contenidos en los siguientes elementos de la víctima y/o sospechoso
  + — Routers.
  + — Firewalls.
  + — Servidores Web.
  + — Servidores de correo electrónico.
  + — Otros dispositivos conectados.

Ver la Figura 4 donde se muestra una representación del flujo de la información.

Dados una dirección IP y una fecha y hora (incluyendo la zona horaria), la mayoría de los ISPs pueden identificar al usuario registrado que fue asignado a la dirección IP en el momento especificado, permitiendo al investigador requerir información adicional. Sin embargo, el investigador puede necesitar el uso de métodos de investigación tradicionales para identificar a la persona que estaba usando la cuenta en ese momento.

##### Paso 3. Suministrar el servicio legal del proceso

El tercer paso es determinar las partes apropiadas para contactar y/o para cumplir con el proceso legal, dependiendo de los elementos de la investigación como se trata en los capítulos subsiguientes. Típicamente se requieran Autorizaciones Legales, Órdenes del Tribunal o Citaciones Legales para entregar a la autoridad información exacta sobre el usuario final. Muchos de estos requerimientos están gobernados por el Acta de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act - ECPA) y otras leyes Federales y Estatales aplicables. Una *solicitud de conservación de la información* puede ayudar a conservar la información hasta que se cumplan los requerimientos legales correspondientes. Estas solicitudes deberían especificar la dirección IP y la fecha y hora, incluyendo la zona horaria. Se deberá estar al tanto de la necesidad de un servicio expedito de solicitudes de conservación de la información bajo 18 USC § 2703(f) (apéndice G). Referirse al capítulo 9 para más detalles sobre los requerimientos legales y al apéndice H para un lenguaje de muestra.

**Nota ArCERT**: Se considera una buena práctica realizar todos los requerimientos por escrito, haciéndole firmar a la entidad requerida una copia que quedará en nuestro poder como constancia de dicha solicitud. Para el supuesto que la entidad no quiera suscribir copia alguna, se aconseja realizar el requerimiento mediante el envío de una Carta Documento.

Estos recaudos son necesarios ya que la documentación que uno vaya recabando en la investigación eventualmente será presentada en sede judicial, resultando por consiguiente

necesario acreditar el diligenciamiento adecuado.

Respecto a la forma en que deberá solicitarse la información, es importante que en la solicitud se especifique claramente la dirección IP y la fecha y hora en que se produjo el incidente, incluyendo la zona horaria. Ello a fin de obtener exactamente la información requerida. Para el supuesto que la investigación derive en la apertura de causa judicial, además de la información resultante de la investigación previa, el juez podrá solicitar todo tipo de información adicional pertinente, de oficio o a pedido de parte, en cuyo caso la entidad involucrada estará obligada a proveerla.

Es importante tener presente que el intercambio de información se encuentra regulado por diversas normas, en particular por la Ley de Protección de Datos Personales, pudiendo por tal motivo el ISP negarse a entregarla en la etapa extrajudicial, no así en la judicial mediando orden del juez competente.

La información que se puede obtener de un ISP incluye:

* **Información del suscriptor** tal como propietario registrado, domicilio y forma de pago.
* **Información de transacción** tal como horas de conexión, fechas y dirección IP usada.

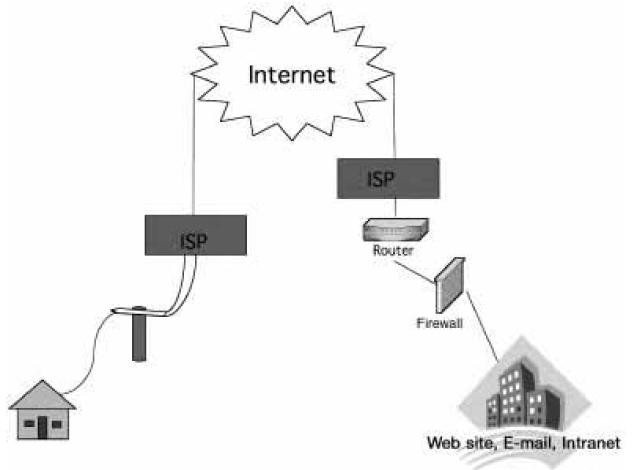


Figura 4. Dónde encontrar información

* **Contenido** tal como mensajes de correo electrónico, archivos de datos, y programas almacenados.

Parte de la información utilizada en el rastreo de una dirección IP o del usuario final puede ser obtenida de los ISPs o los administradores de red. Esta información típicamente incluye información sobre la cuenta, información sobre la dirección de correo electrónico, dirección IP, y nombre de dominio. Puede contener o no información acerca del propietario o usuario. En base a la información recibida, se puede requerir información adicional. Se pueden requerir citaciones legales, mandamientos, órdenes del tribunal y notas de conservación de información adicionales para cumplir con las entidades identificadas por el proceso legal previo. Por ejemplo, si la dirección IP original se descifra como “BIG-ISP.com,” se emiten procesos legales a BIG-ISP.com para identificar al usuario de una dirección IP en particular en una fecha y hora particular. La respuesta identifica “Medium-ISP.com” como el usuario de esa dirección IP. (Una práctica común entre ISPs más pequeños es ceder bloques de direcciones IP de ISPs más grandes.) En este punto, se deberá emitir un proceso legal adicional para “Medium-ISP.com.” Este proceso continúa hasta que la información identifica al usuario registrado (*logged in* ) en esa dirección IP en particular para una fecha y hora específica o hasta que todos los hilos de la investigación sean agotados.

**Nota ArCERT**: En el marco de una causa judicial, se puede requerir información mediante oficios, citaciones legales, mandamientos de secuestro de equipos y medidas cautelares que procuren la efectiva conservación de información adicional.

**Lenguaje de muestra.** Cuando se esté requiriendo información -extrajudicial o judicialmente-, el siguiente lenguaje de muestra puede ser útil. Sin embargo, el ISP puede requerir otro lenguaje específico

* + ■ **Información de cuentas de ISP**: (ISP account information) “Cualesquiera y toda información del suscriptor relacionada con la cuenta de (Nombre) incluyendo pero no limitado a la identificación del usuario, información de la cuenta del usuario, nombres de pantalla, estado de la cuenta, información de la cuenta de correo electrónico, registros de facturación detallada, identificación de llamada entrante (caller line identification - ANI), notas de historial de mantenimiento de la cuenta, e historial IP desde (Fecha) al presente.”



* + ■ **Información de la dirección de correo electrónico**: (E-mail address information) “Cualesquiera y toda información del suscriptor relacionada con el individuo que registró y mantiene la dirección de correo electrónico (JonDoe@Email.com) incluyendo pero no limitado a la identificación del usuario, información de la cuenta del usuario, nombres de pantalla, estado de la cuenta, información de la cuenta de correo electrónico, registros de facturación detallada, identificación de llamada entrante (caller line identification - ANI), notas de historial de mantenimiento de la cuenta, e historial IP desde (Fecha) al presente”
  + ■ **Información de dirección IP**: (IP address information) “Cualesquiera y toda información del suscriptor relacionada con la cuenta del individuo al que le fue asignada la dirección IP (Dirección IP) el (Fecha) a las (Hola y Zona Horaria) y la dirección IP de (Dirección IP) para (Fecha) a las (Hora y Zona Horaria) incluyendo pero no limitado a la

identificación del usuario, información de la cuenta del usuario, nombres de pantalla, estado de la cuenta, información de la cuenta de correo electrónico, registros de facturación detallada, identificación de llamada entrante (caller line identification - ANI), notas de historial de mantenimiento de la cuenta, e historial IP desde (Fecha) al presente.”



* + ■ **Información de nombre de Dominio**: (Domain name information) “Cualesquiera y toda información relacionada con la identidad de quien registró y mantiene los nombres de dominio de (www.xxxxxxxx.com) y (www.xxxxxxxx.org) incluyendo pero no limitado a la información completa de la cuenta, registros de facturación incluyendo nombre de tarjeta de crédito y otra información sobre el pago, identidad del usuario, historial IP, e identificación de la llamada entrante.”



* + ■ **Información de la página Web**: (Web page information) “Toda información sobre el individuo que creó y mantiene la página Web (nombre de la página Web) del (ISP) incluyendo pero no limitado a la identidad del usuario, información de la cuenta del usuario, registros de facturación, información sobre la cuenta de correo electrónico, identificación de llamada entrante, registros de eventos de uso, e historial IP.”



* + ■ **Proveedores de sesión Telnet**: (Telnet session providers) “Cualesquiera y todo historial IP relacionado con el tráfico de Internet (xxxxx.net) y registro de eventos de uso de sesiones ***Telnet*** de (xxxx.net) para (Fecha) y (Fecha) incluyendo pero no limitado a la identificación del usuario, nombre del usuario, comando de usuario emitido, y dirección de usuario.”



* + ■ **Información sobre Punto de Presencia** (Point of Presence (POP) information): “Cualesquiera y toda información relacionada con la ubicación del ***Punto de Presencia*** *(Point of Presence)* (ANS.NET y otro ISP) que emitió el IP (Dirección IP) el (Fecha/Hora) incluyendo pero no limitado a un número de telefónico para el acceso (*dial-in access phone number*), dirección física, y (Compañía Telefónica) a quién el número de teléfono para el acceso está suscripto.”



* + ■ **Registros telefónicos salientes**: (Outgoing telephon records) “Cualesquiera y toda información incluyendo pero no limitada a la información del suscriptor y a la información de facturación para la dirección de (Dirección del Suscriptor). Cualquier y toda información, pero no limitada a la información del suscriptor e información de facturación para el número de teléfono de (Número de Teléfono). Incluir un listado de cualquier llamada saliente local realizada desde la dirección de arriba. Incluir la información de arriba para cualesquiera y todos los números de teléfono listados para la dirección de arriba para el período de (Fecha/Hora).”

## Resumen

Todas las comunicaciones en Internet y a través de redes dependen de una dirección IP para alcanzar su destino. La clave para investigar los delitos relacionados con Internet y redes es identificar la dirección IP de origen y rastrearla a una fuente. Estas habilidades le permiten a un investigador localizar fuentes de evidencia adicionales, corroborar las declaraciones de las víctimas y testigos y potencialmente, localizar un sospechoso.

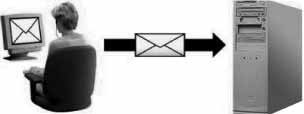
**Capítulo 3. Investigaciones relacionadas con el correo electrónico (E-Mail)**

Un e-mail puede ser el punto inicial o un elemento clave en muchas investigaciones. Un e-mail es el equivalente electrónico de una carta o un memo y puede incluir adjuntos. Al igual que el papel o un correo postal, un mensaje de correo electrónico puede representar una evidencia en muchos tipos de investigaciones. El correo electrónico ya no es exclusivo de las computadoras

/ordenadores de escritorio, dado que ahora se pueden intercambiar mensajes fácilmente usando muchos dispositivos portátiles tales como teléfonos celulares, asistentes digitales personales (PDA’s), y radio-localizadores (pagers).

## Cómo funciona el correo electrónico

Un mensaje de correo electrónico puede ser generado por medio de diferentes dispositivos y métodos, pero, en general, un usuario escribe un mensaje en su propia computadora y luego lo envía a su servidor de correo (mail-server). En este punto la computadora del usuario termina su trabajo, pero el servidor de correo aún tiene el mensaje para entregar. Un servidor de correo es como una oficina de correo postal envía y recibe correo electrónico. La mayor parte del tiempo, el servidor de correo está separado de la computadora donde se escribió el correo. (Ver Figura 5.)



Paso 1 Paso 2 Servidor de correo

Figura 5. Generación de un e-mail

El servidor de correo del emisor entrega el mensaje buscando el servidor de correo del receptor y envía el mensaje a ese sitio. El mensaje entonces, queda en ese segundo servidor de correo y está disponible para el receptor. Al software que se utiliza para redactar y leer el mensaje de correo electrónico se lo conoce como el ***cliente*** de correo electrónico. Dependiendo de cómo esté configurado el cliente de correo electrónico del receptor, se podría encontrar una copia del mensaje en la computadora del receptor, otro dispositivo electrónico como un Ayudante personal digital o PDA (***P****ersonal* ***D****igital* ***A****ssistant*) PDA, y/o en el servidor de correo o sus cintas de resguardo (backup). También se puede encontrar una copia del mensaje en la computadora del emisor (en la casilla de “enviados” o en la papelera), en el servidor del correo del emisor o en sus cintas de backup. (Ver figura 6.)

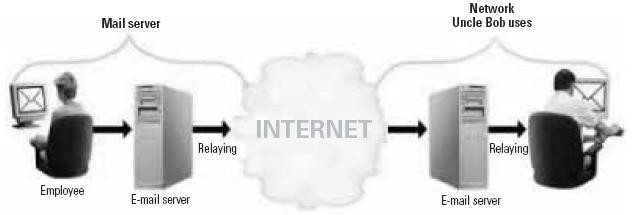


Figura 6. Entrega de un e-mail

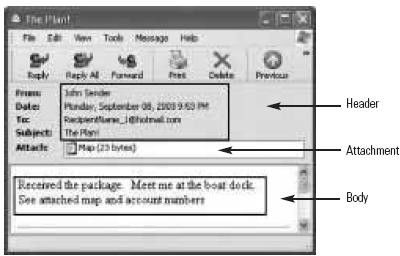
A medida que el mensaje de correo electrónico viaja a través de la red de comunicación, queda un registro abreviado del trayecto del mismo en un área del mensaje denominado el ***encabezamiento (header)****.* A medida que el mensaje es ruteado a través de uno o más servidores de correo, cada servidor agrega su propia información al encabezamiento del mensaje. **El investigador puede alcanzar a identificar las direcciones de Protocolo de Internet (IP) a partir del encabezamiento y usar esta información para determinar el emisor del mensaje usando técnicas tratadas en el Capítulo 2**.

## Componentes básicos de un mensaje de correo electrónico

Se utilizan varios métodos para crear y enviar un mensaje de correo electrónico. La apariencia de un mensaje de correo electrónico depende del dispositivo o del software utilizado. Sin embargo, típicamente, un mensaje tiene un encabezamiento (header) y un cuerpo (body) y también puede tener adjuntos (attachments).

El encabezamiento de un mensaje de correo electrónico contiene información sobre la dirección a la que se envía y la ruta que el mensaje toma desde el emisor hasta el receptor. El cuerpo contiene el contenido de la comunicación. Los adjuntos pueden ser cualquier tipo de archivo tales como fotos, documentos, sonidos, y video.

Inicialmente, cuando se visualiza un mensaje de correo electrónico, puede mostrarse sólo una pequeña porción del encabezamiento. Ésta generalmente es información puesta en el mensaje por el emisor, como se representa en la Figura 7.

Figura 7. Componentes de un e-mail

Sin embargo, el mensaje representado en la figura 7 no muestra toda la información disponible. Se puede obtener información adicional asociada con el mensaje mirando con más detalle el encabezamiento, lo cual se puede hacer de diversas formas dependiendo del software que se esté usando. Referirse al apéndice C para ver las instrucciones acerca de cómo revelar la información detallada del encabezamiento para los clientes de correo electrónico comunes. Tener en cuenta que no se han listado todos los clientes de correo electrónico y que las actualizaciones de los clientes pueden cambiar la forma de obtener la información detallada del encabezamiento.

El trayecto del mensaje generalmente se puede reconstruir leyendo el encabezamiento del mensaje desde la parte inferior a la superior. A medida que el mensaje pasa a través de servidores de correo adicionales, el servidor de correo agrega su información arriba de la información previa del encabezado. **Una de las informaciones más importantes que el investigador puede obtener del encabezado detallado es la dirección IP de origen**. En el ejemplo, en la figura 8, la dirección IP de origen es [165.247.94.223]

12. X-Message-Info: JGTYoYF78jEv6iDU7aTDV/xX2xdjzKcH

11. Received: from web11603.mail.yahoo.com ([216.136.172.55]) by mc4f4 with Microsoft SMTPSVC(5.0.2195.5600);

Mon, 8 Sep 2003 18:53:07 -0700

10. Message-ID: [20030909015303.27404.qmail@web11603.mail.yahoo.com](mailto:20030909015303.27404.qmail@web11603.mail.yahoo.com)

9. Received: from [165.247.94.223] by web11603.mail.yahoo.com viaHTTP; Mon, 08 Sep 2003 18:53:03 PDT

8. Date: Mon, 8 Sep 2003 18:53:03 -0700 (PDT)

7. From: John Sender [<sendersname2003@yahoo.com>](mailto:sendersname2003@yahoo.com)

6. Subject: The Plan!

5. To: [RecipientName\_1@hotmail.com](mailto:RecipientName_1@hotmail.com)

4. MIME-Version: 1.0Content-Type: multipart/mixed; boundary=“0- 20414130291063072383=:26811”

3. Return-Path: [sendersname2003@yahoo.com](mailto:sendersname2003@yahoo.com)

2. X-OriginalArrivalTime: 09 Sep 2003 01:53:07.0873 (UTC)FILETIME=[1DBDB910:01C37675] 1. --0-2041413029-1063072383=:26811Content-Type: multipart/alternative; boundary="0-

8714595721063072383=:26811"

--0-871459572-1063072383=:26811Content-Type: text/plain; charset=us-ascii Recibí el paquete. Encontrame en el muelle del barco. Ver mapa adjunto y

números de cuenta.

Figura 8. Encabezado del e-mail

Para comprender las partes del encabezado del mensaje de correo electrónico de la figura 8, dicho encabezado se ha reproducido más abajo con una descripción línea por línea. Observar que el encabezado del mensaje está compuesto por dos áreas generales, el *encabezado del sobre* y el *encabezado del mensaje.*

El *encabezado del sobre* contiene información agregada al mismo por los servidores de correo que reciben el mensaje durante su trayecto. Las líneas de “Recibido:” y la línea del Message-ID son los componentes más importantes del encabezado del sobre y generalmente, son los más difíciles de *alterar (spoof).* En el siguiente ejemplo, las líneas del 9 al 12 son parte del encabezado del sobre.

El *encabezado del mensaje* contiene información agregada al encabezado por el cliente de correo electrónico del usuario. Generalmente, ésta es una información creada por el usuario y es la más fácil de alterar (spoof). Contiene el Para:, De:, Camino de Retorno:, Tema:, Tipo de Contenido:, y la primera mención de la Fecha y hora. En el ejemplo siguiente, las líneas del 2 al 8 son parte del encabezado del mensaje.

##### 12. X-Message-Info: JGTYoYF78jEv6iDU7aTDV/xX2xdjzKcH

*Los encabezados X no son estándar ni son esenciales para la entrega del correo. La utilidad del encabezamiento X necesita ser explorada con el Proveedor del Servicio de Internet (ISP).*

##### 11. Received: from web11603.mail.yahoo.com ([216.136.172.55]) by mc4-f4 with Microsoft SMTPSVC(5.0.2195.5600);

##### Mon, 8 Sep 2003 18:53:07 -0700

*Received: (Recibido:)*

*Esta línea de “Recibido” es la última información colocada en el encabezado. Es colocada por*

*el último servidor de correo en recibir el mensaje e identificará al servidor de correo desde el cual fue recibido. Observar que la información de fecha y hora está generada por el servidor de correo de recepción e indica su salida desde* ***UTC*** *(-0700). En este ejemplo, el nombre del servidor de correo está indicado. Esto puede lograrse ya fuere por el servidor de recepción resolviendo la dirección IP del último servidor de correo, o por el servidor de correo previo que difunde su nombre.*

##### 10. Message-ID: [20030909015303.27404.qmail@web11603.mail.yahoo.com](mailto:20030909015303.27404.qmail@web11603.mail.yahoo.com)

*Message-ID (Identificación del Mensaje:)*

*Es un identificador único asignado a cada mensaje. Generalmente es asignado por el primer servidor de correo y es una información clave para el investigador. Contrariamente a la dirección IP de origen (ver más abajo), que puede dar información del suscriptor, la identificación del mensaje puede vincular el mensaje al emisor si se mantienen los registros (logs) apropiados.*

##### 9. Received: from [165.247.94.223] by web11603.mail.yahoo.com via HTTP; Mon, 08 Sep 2003 18:53:03 PDT

*Received: (Recibido:)*

*La última línea en “Recibido” identifica la dirección IP del servidor de correo originario. Podría*

*indicar el nombre del servidor, el protocolo utilizado, y la fecha y hora programados (settings) en el servidor. Observar los datos de zona horaria que se informan.*

*PRECAUCIÓN: Si la fecha y hora asociados al e-mail son importantes para la investigación, considerar que esta hora de “Recibido” registrada en el encabezamiento del e-mail proviene del servidor de e-mail y puede no ser precisa.*

##### 8. Date: Mon, 8 Sep 2003 18:53:03 -0700 (PDT)

*Date: (Fecha:)*

*Esta fecha está asignada por la máquina del emisor y puede no concordar con la fecha y hora del servidor de correo. Si la fecha y hora de creación del mensaje son importantes para la investigación, considerar que el tiempo registrado en el encabezado del mensaje proviene de la máquina del emisor y pude no ser preciso.*

##### 7. From: John Sender [<sendersname2003@](mailto:sendersname2003@yahoo.com)y[ahoo.com>](mailto:sendersname2003@yahoo.com)

*From: (De:)*

*Esta información generalmente está configurada por el usuario en el cliente de correo electrónico y puede no ser confiable.*

##### 6. Subject:The Plan!

*Subject: (Tema:)*

*Ésta es información ingresada por el usuario.*

##### 5. To: [RecipientName\_1@hotmail.com](mailto:RecipientName_1@hotmail.com)

*To: (A):*

*Ésta es información ingresada por el usuario.*

##### 4. MIME-Version: 1.0

##### Content-Type: multipart/mixed; boundary=”0-2041413029-1063072383=:26811”

*El propósito de estas dos líneas es darle al cliente de correo del receptor información acerca de cómo interpretar el contenido del mensaje.*

##### 3. Return-Path: [sendersname2003@yahoo.com](mailto:sendersname2003@yahoo.com)

*Return-Path: (Camino de Retorno:)*

*Ésta es información generalmente configurada por el usuario en el cliente de correo y puede no*

*ser confiable.*

##### X-OriginalArrivalTime: 09 Sep 2003 01:53:07.0873 (UTC) FILETIME=[1DBDB910:01C37675]

*Los encabezados X no son estándar y no son esenciales para la entrega del correo. La utilidad del encabezado X requiere ser explorada con el Proveedor del Servicio de Internet (ISP).!*

##### 1. --0-2041413029-1063072383=:26811

*Información del cliente de correo, no relevante para la investigación.*

##### Una vez que las direcciones IP están identificadas en el encabezado se pueden utilizar los procedimientos descriptos en el capítulo 2 para rastrear el trayecto del mensaje. Tener en cuenta que las direcciones IP pueden ser creadas o alteradas (spoofed) en un intento de ocultar la verdadera identidad del emisor.

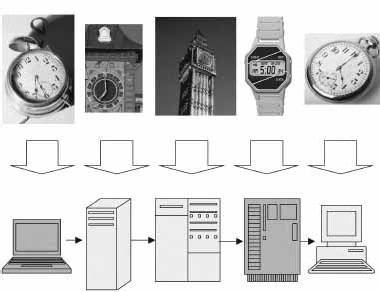
## Time stamping (Sello de Tiempo)

Los investigadores deben tener en cuenta que, cuando examinan los encabezamientos de los e- mails, las horas pueden no ser consistentes. Se deben examinar los sellos de fecha y hora relacionados con el encabezado debido a que esta información puede ser agregada por diferentes servidores en distintas partes del mundo y en variadas zonas horarias y pueden no ser

consistentes. Además, los relojes incorporados dentro de los equipos y que funcionan con pilas

—especialmente aquellos dentro de las computadoras personales—pueden no estar siempre programados con precisión o pueden no mantener la hora correctamente, mostrando así una hora incorrecta. Se debería dar consideración especial a la búsqueda de información sobre la zona horaria relacionada con la hora del mensaje.

La Figura 9 muestra una secuencia cronológica de acciones con diferentes horas de relojes involucrados en la transmisión de un e-mail.



Hora errónea Hora Standard

UTC

Hora Estándar Hora Standard

Oriental

de la Montaña

Pacífico

**Laptop del**

**Servidor del Servidor de**

**Servidor de mail Computadora de**

**emisor**

**emisor**

**mail del proveedor**

**local**

**escritorio del**

**del servicio Internet**

**receptor**

Figura 9. Secuencia de hora de un e-mail

## Temas a los que se debe prestar atención

**Encabezamientos de e-mail alterados** (spoofed). Todo lo que haya hasta la línea superior de “Recibido:” en el encabezado del mensaje puede ser alterado (spoofed), o falsificado (faked). Compare la información del encabezado del mensaje con aquella del encabezado del sobre. Si no concuerdan, existe la posibilidad de que el mensaje haya sido alterado.

**Anonimizadores (Anonymizers)** (métodos para lograr anonimato). Los anonimizadores son servidores de correo electrónico que eliminan información de identificación del mensaje antes de reenviarlo. Aunque existen razones valederas para usar un servicio anonimizador, muchas personas utilizan este servicio para ocultar su identidad. Si se utiliza un anonimizador, el investigador tal vez no pueda rastrear el mensaje de correo electrónico hasta su origen debido a que estos servicios generalmente no mantienen registros de eventos (logs).

**Lugares remotos (Remote Location)**. Tener en cuenta que existen muchos lugares públicos donde se dispone de acceso a Internet, tales como bibliotecas, colegios, aeropuertos, hoteles y *cybers*. Si se envía un mensaje de correo electrónico desde uno de estos lugares, puede resultar difícil determinar el emisor real.

**Envío demorado**. Muchos proveedores y clientes e-mail tienen la habilidad de permitir al emisor programar la hora de envío de un mensaje de correo electrónico. También, algunos servidores envían mensajes a cierta hora pre-programada. Cualquiera de estas situaciones podría permitir a una persona estar en otro lugar en el momento en que el mensaje es realmente enviado.

**Ubicación del mensaje de correo electrónico**. Independientemente del tipo de cliente de correo que se esté utilizando, el mensaje puede ser almacenado en múltiples lugares. Considere obtenerlo de todas las fuentes posibles. Por ejemplo, si el mensaje está almacenado en la Web

®

por un proveedor de servicio (por ej., Hotmail , Yahoo!®), el tiempo es esencial dado que muchas

de estas empresas tienen la política de purgar información luego de un cierto período de tiempo. Una carta de preservación emitida al proveedor podría ser una medida necesaria para prevenir la purga de datos. En el capítulo 9 puede encontrarse mayor información acerca de los pedidos de preservación de la información.

## Investigación forense

### ¡STOP!

Un investigador no debería intentar examinar un equipo o sistema si no ha recibido una capacitación especial en investigación forense de computadoras.

El investigador debe seguir la política del organismo o contactar a un organismo con capacidad de realizar una investigación forense.

Una investigación forense de un sistema informático debería revelar información adicional, tal como:

* + Otros mensajes de correo electrónico relacionados con la investigación.
  + Otras direcciones de correo electrónico.
  + Información del emisor.
  + Contenido de las comunicaciones.
  + Direcciones IP.
  + Fecha y hora de la información.
  + Información del usuario.
  + Adjuntos.
  + Contraseñas (Passwords).
  + Registros de aplicación que muestren evidencia de alteración (spoofing).

## Consideraciones legales

**Nota de Traducción**: Esta sección no fue traducida debido a que hace referencia a normas legales de EEUU y no posee aplicaciones prácticas en la República Argentina.

## Resumen

La información obtenida de un mensaje de correo electrónico puede ser una evidencia valiosa. Este capítulo muestra técnicas para obtener una pieza del rompe cabezas de la investigación. Sin embargo, una vez que se identifica al suscriptor de una cuenta de correo electrónico, se deben usar otras técnicas de investigación para localizar al individuo en el teclado al momento que el mensaje fue enviado. Tener presente los procedimientos legales que se deben seguir para asegurarse que la evidencia reunida pueda ser usada en un Tribunal.

# Capítulo 4. Investigaciones relacionadas con Sitios Web

Este capítulo es una guía sobre los métodos y prácticas para llevar adelante investigaciones vinculadas a sitios Web. El investigador debería saber que el acceso a un sitio Web puede estar monitoreado por el sujeto investigado. Este monitoreo puede revelar la identidad del investigador, y de este modo comprometer la investigación. Debería considerarse el uso de una computadora y una cuenta confidencial/secreta de un Proveedor de Servicio de Internet (ISP) u otros métodos secretos.

**ATENCIÓN**: Las investigaciones no se deberían llevar a cabo usando la computadora del sospechoso o de la víctima a menos que existan circunstancias que lo exijan, debido a que se puede afectar la integridad de la evidencia.

Generalmente, un sitio Web es una colección de páginas Web o archivos relacionados (tales como fotos, sonidos o texto) que está almacenada en un servidor Web. El lenguaje típico de estas páginas está escrito en HyperText Markup Language (HTML). Este lenguaje permite a los usuarios navegar fácilmente entre páginas o archivos relacionados dentro de esa colección. También permite que una colección de páginas relacionadas se vincule a otra colección de páginas relacionada. Dicho en forma simple, HTML permite vínculos entre sitios Web.

Un servidor Web es una computadora con un software especial que provee páginas Web a los clientes a través de Internet o una intranet. Un servidor Web puede alojar múltiples sitios Web, muchos de los cuales pueden no estar relacionados con la investigación que se lleva a cabo. Además, los archivos que conforman un único sitio Web pueden existir en más de un servidor Web.

Se accede a una página Web tipeando un “Uniform Resource Locator” (URL) dentro de un navegador de Internet tal como Internet Explorer®, Netscape® Navigator, o Mozilla. El URL es la dirección de un recurso o archivo, disponible en Internet. El URL contiene el *protocolo* del recurso (por ej., http://, https://), el nombre del dominio (domain) para el recurso y el nombre jerárquico para el archivo (dirección o address). Por ejemplo, una página en Internet puede estar en el URL [http://www.nist.gov.](http://www.nist.gov/) La parte inicial, http://, provee el protocolo, la siguiente, www, es un puntero (pointer) hacia un servidor Web y nist.gov es el dominio. Ver el capítulo 2 para mayor información sobre nombres de dominio y las direcciones IP asociadas con ellos.

Los hipervínculos o enlaces (Hyperlinks o simplemente links) son atajos que permiten a los usuarios navegar desde una página Web a otra página Web o a un archivo sin ingresar manualmente la dirección URL completa. Los enlaces pueden estar ocultos en las páginas Web, de forma tal que probablemente sólo los usuarios que conocen dónde mirar encuentren los enlaces. Los enlaces también pueden re-direccionar automáticamente al navegador de Internet a un sitio Web diferente.

Los investigadores deberían saber que a pesar de que las páginas Web típicamente están escritas en HTML, también pueden estar escritas en lenguajes *script*. Estos lenguajes permiten que la página Web muestre un contenido individualizado para cada usuario. El contenido puede

estar hecho a medida de acuerdo con la dirección de Procotolo de Internet (IP), los sitios Web visitados previamente, los cookies almacenados u otros criterios. Por lo tanto, puede ocurrir que dos personas que navegan simultáneamente hacia el mismo URL vean contenidos diferentes.

## Vista de la fuente HTML (HTML source) de una página Web

El código fuente HTML de una página Web es el texto que define el contenido y formato de una página. Además de la representación gráfica que se brinda al visualizador, la página puede contener información adicional relacionada con su autor, código de programación, metadatos (\*) y otra información de identificación que puede no ser mostrada en la vista de la página Web. Los navegadores de Internet (más comunes permiten a los usuarios ver el código fuente HTML de la página Web. La Figura 10 muestra la captura de una pantalla para el sitio Web [www.nist.gov,](http://www.nist.gov/) seguido por la información del código fuente HTML. Para ver el código fuente usando Internet Explorer®, seleccionar “view” en la barra de herramientas y luego “source” en el menú que se despliega.

**Nota**: Existen técnicas que pueden ocultar el código fuente HTML mientras que al mismo tiempo permiten ver la página Web en un navegador.

(\*) Metadatos en este contexto es la información que describe los atributos o palabras claves que han sido insertadas en el código fuente de una página Web.

## Captura de los datos de una página Web

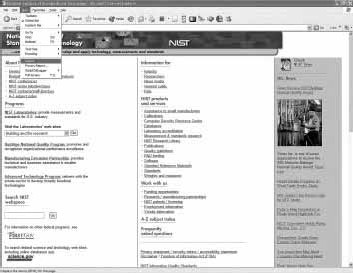
Dependiendo de la naturaleza y alcance de la investigación, puede resultar útil capturar información de una sola página Web o todos los contenidos de un sitio Web. Las técnicas para obtener esta información pueden incluir capturas de pantalla, el comando “save as”, herramientas de captura del sitio Web, o la localización e incautación (seizing) del servidor Web.

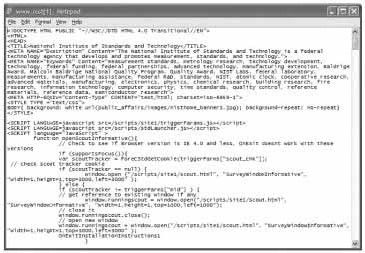
##### Captura de la pantalla

Existen varios métodos para capturar una imagen de pantalla de una página Web. Un método es una función Windows® [Ctrl]+[PrntScrn], que capturará la pantalla completa copiándola al *portapapeles (clipboard)* Windows®*.* Para preservar la imagen luego se la puede copiar ([Ctrl]+[v] or Edit > Paste) dentro de otra aplicación, tal como un programa de procesamiento de texto o un editor de gráficos. Otro método es usar una aplicación de software de terceros específicamente diseñada para capturar imágenes de pantallas o ventanas activas. Estos métodos pueden capturar sólo el contenido mostrado en la ventana activa pero pueden no capturar el que está fuera de la vista de la ventana activa. La fuente HTML no se podrá capturar a menos que esté expuesta (displayed).

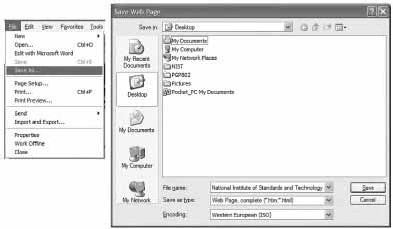
##### Comando “Save as”

Un método simple para capturar información de una página Web que puede incluir el código fuente y los archivos insertados, es usar el comando “save as” dentro del navegador de Internet. Este comando guardará la página Web en un lugar especificado de la computadora que el investigador está usando. En la Figura 11, el comando “save as” se muestra a la izquierda, y el destino de la captura de la página Web se muestra a la derecha.



Figura 10. Captura de Pantalla y fuente HTML para el sitio Web NIST

Observar que, dependiendo del navegador de Internet utilizado, se pueden usar varias opciones “Save as type” para capturar la página completa y todos sus archivos insertados. En la Figura 11, la opción “Save as type” dará por resultado que la página Web completa con todos los archivos insertados sean guardados en una carpeta ubicada en el mismo directorio. Se recomienda como buena práctica, probar y verificar la información que es capturada usando las distintas opciones “save as” antes de usar esta técnica de investigación. Una vez que se finaliza con la captura, se la debería verificar inmediatamente para asegurar que toda la información buscada quedó guardada.

Figura 11. Comando “Save as” y captura de página Web

## Herramientas de captura de sitio Web

Una forma de automatizar la captura de una colección de páginas dentro de un sitio Web es a través del uso de aplicaciones de terceros. Llevaría mucho tiempo navegar y guardar manualmente cada página Web en un sitio de gran tamaño. Existen muchas herramientas comerciales y gratuitas para capturar sitios Web. El uso de las herramientas específicas está más allá del alcance de este documento. En general, estos programas están diseñados para navegar hacia cada enlace en una página Web y capturar todos los contenidos, incluyendo archivos insertados y códigos fuente, de esos enlaces.

Es importante para el investigador saber que el contenido del sitio Web actual pudo haber cambiado desde el inicio de la investigación. Por lo tanto, la fecha y hora de las capturas del sitio Web deben quedar documentadas. Se puede determinar el contenido previo de muchos sitios Web usando sitios de archivo Web (por ej., la herramienta de búsqueda ***Wayback Machine***, http://www.archive.org) o sitios similares. Para obtener detalles sobre la forma en que trabajan estos sitios, visitar y leer la documentación del sitio.

**Nota**: Para sitios Web escritos en lenguajes de scripting (scripting languages), puede no ser posible la captura de todo el contenido específico de interés usando las herramientas de captura de sitio Web.

## Localización e incautación del servidor Web

En algunas investigaciones en las cuales el sitio Web está siendo utilizado para perpetrar un delito (por ej., distribución de pornografía infantil), se debe considerar la localización e incautación del servidor Web. El servidor Web puede contener el contenido y los códigos fuente, como así también los registros de transacción que muestran las direcciones IP de los usuarios que se conectan y bajan material del sitio Web. El servidor también puede almacenar nombres, contraseñas, formas de pago y otra información pertinente para la investigación. Para localizar e identificar al servidor Web, será necesario obtener la dirección IP y otra información de identificación y establecer la base legal necesaria para capturar y revisar el servidor Web. Ver el capítulo 2 para los detalles de cómo determinar la dirección IP para los sitios Web a través del dominio.

## Resumen

Durante el curso de una investigación, el investigador puede necesitar determinar y preservar los contenidos de un sitio Web. Preservar esta información puede ser tan simple como capturar la imagen de una pantalla del material relevante, pero también se explican técnicas para capturar el código fuente subyacente y los contenidos completos de una página Web. El investigador debería saber que el contenido de una página es dinámico y puede cambiar frecuentemente. Este capítulo ofrece una fuente potencial para ver el contenido histórico de una página Web.

# Capítulo 6. Investigaciones relacionadas con redes que comparten archivos

Los investigadores progresivamente van encontrando nuevos métodos que se utilizan para compartir archivos que contienen datos obtenidos de forma ilegal. Un método que va creciendo a paso acelerado utilizado para cometer delitos en Internet son las redes que comparten archivos. Los procesos más populares para compartir archivos son los Protocolos de Transferencia de Archivos [File Transfer Protocol (FTP)] y las redes entre pares [Peer-to-Peer (P2P)]. Este capítulo brinda una visión general de estas tecnologías. Para consejos sobre la investigación, ver el apéndice D.

## Protocolo de Transferencia de Archivo (File Transfer Protocol - FTP)

FTP está basado en un modelo cliente-servidor que permite al usuario transferir archivos hacia y desde otra computadora. Cualquier computadora puede actuar como cliente o como servidor. Los sitios FTP se pueden configurar para permitir una conexión anónima o para requerir un nombre de usuario y contraseña. Algunos programas comunes de FTP cliente incluyen navegadores de Internet, WS-FTP (Light Edition & Pro), War FTP Daemon, CuteFTP, BulletProof FTP, y FTP Voyager. El modelo cliente-servidor es similar a un gabinete central de archivos en una oficina donde la gente puede acceder a documentos. (Ver Figura 20.)

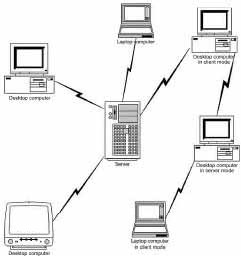


Figura 20. FTP

##### Escenario FTP

Alfredo busca en los canales de chat y en grupos de noticias para encontrar las direcciones de los servidores FTP que están compartiendo música. Usa un programa cliente FTP para conectarse a la dirección de servidor FTP que encontró. Hace un repaso de la música disponible y si encuentra la canción que le gusta, baja la canción.

## Redes Entre Pares(Peer-to-Peer - P2P)

Una verdadera red P2P comparte información directamente entre las computadoras y no requiere un servidor. En las redes P2P que comparten archivos tales como Kazaa, Grokster, Morpheus™, o Blubster™, los usuarios que están buscando el archivo deseado hacen la búsqueda en un directorio que está almacenado en un servidor. (**Nota:** El servidor generalmente no mantiene registros de auditoria de la actividad de transferencia de archivos.) El directorio dirige al usuario a la computadora o múltiples computadoras donde está almacenado el archivo real. El usuario luego baja el archivo directamente desde una o más computadoras en una red P2P que contiene el archivo. La estructura de una red P2P cambia cuando las computadoras entran y salen de la red, por lo tanto una red P2P está en un estado de cambio constante. (Ver Figura 21.)

Existen muchas aplicaciones P2P; algunas de las aplicaciones más populares incluyen Kazaa, Grokster, Morpheus™, Blubster™, WinMX™, iMesh, Filetopia, eDonkey, y Freenet.

**Nota ArCERT**: Actualmente, las redes más utilizadas son edonkey y Bittorrent, y dentro de los clientes, se destacan por su popularidad el emule, utorrent, azureus y shareaza.

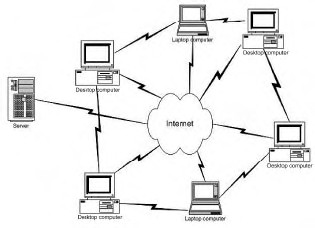


Figura 21. Red P2P

##### Escenario P2P simple

Alfredo quiere obtener pornografía infantil. Comienza la sesión de compartir un archivo Kazaa y busca otros usuarios Kazaa para encontrar el término común de pornografía infantil “Lolita.” Los usuarios en la red Kazaa normalmente tienen un directorio de ítems que comparten con la red.

Alfredo encuentra numerosos archivos que se corresponden con su búsqueda y los transfiere a su computadora directamente desde la(s) fuente(s).

## Consideraciones investigativas para las redes que comparten archivos

Las redes que comparten archivos FTP y P2P tienen usos válidos, pero también permiten que los usuarios busquen, obtengan, posean y/o distribuyan muy fácilmente una variedad de contenido ilegal. Un individuo que usa FTP o P2P puede tener una combinación de material ilegal y de datos obtenidos ilegalmente, tales como:

* Pornografía infantil.
* Material con derecho de autor (música, películas, video juegos, fotografías, software).
* Propiedades intelectual/secretos comerciales.
* Información financiera (números de tarjetas de crédito, información de cuentas bancarias).
* Información de identificación personal (número de seguridad social, fecha de nacimiento, licencia de conducir).

A medida que los usuarios se van haciendo más sofisticados, pueden desarrollar técnicas para enmascarar su verdadera identidad. Entre estas técnicas está el uso de servidores proxy.

##### Escenario P2P complejo – servidor proxy

Alfredo, que no quiere ser rastreado hasta su computadora de trabajo, busca en Internet servicios proxy gratuitos. Inicia un programa Kazza, lo configura para usar una dirección de Protocolo de Internet (IP) de servicio proxy gratuito, luego busca la palabra “Lolita” y comienza a transferir los archivos a su computadora vía el servidor proxy. Si un investigador trata de encontrar a Alfredo rastreando la dirección IP de él, sólo podrá rastrear la dirección IP del servidor proxy. Sin embargo, si el servidor proxy mantiene los registros de eventos (logs), hay posibilidad de que el investigador obtenga información con la que pueda identificar la verdadera dirección IP de Alfredo. A veces, sin embargo, el servidor proxy puede estar ubicado en otro país, o los registros de eventos (logs) pueden no estar disponibles. (Ver Figura 22.)

Las investigaciones de delitos relacionados con las redes que comparten archivos pueden ser complejas y requerir recursos y experiencia adicionales. El primer paso en estas investigaciones es determinar la dirección IP de la computadora bajo sospecha. Esta dirección IP se puede obtener a partir del Proveedor de Servicio de Internet (ISP) del demandante, a través de una investigación forense de la computadora del demandante o a través del uso de técnicas proactivas confidenciales. Las técnicas confidenciales están más allá del alcance de este informe especial. Algunas aplicaciones de archivos compartidos proveen anonimato por medio del uso de ***redirectores*** *(redirectors)* y servidores proxy y pueden encubrir la ubicación del usuario con respecto a otros usuarios e investigadores.

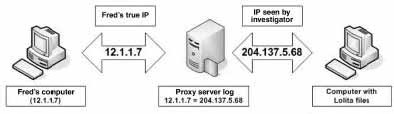


Figura 22. Escenario de servidor proxy

## Evidencia de examen forense

La evidencia que el investigador puede obtener a partir de un examen forense de una computadora incluye:

* + Archivos que son obtenidos ilegalmente.
  + Archivos de configuración que muestran información del servidor o del usuario, historial de conexión, *drives* compartidos en una red, o sitios de Internet que ofrecen un espacio remotos para el almacenamiento de datos (por ej., X-Drive, Yahoo!® Briefcase, .Mac, etc.).
  + Archivos de datos que muestran ubicaciones de archivos compartidos con los nombres de usuarios, contraseñas, palabras de búsqueda, listados de archivo, e información de fecha y hora (.db, .dbb).
  + Archivos de registros de eventos (logs) que muestran transferencias y actividad en la red.
  + Correo electrónico almacenado que muestre una actividad importante del usuario.
  + Programas de transferencia de archivos.

## Evidencia ISP

Evidencia que el investigador puede obtener a partir del ISP del sospechoso:

* Firewall, Dynamic Host Configuration Protocol (DHCP), y ***RADIUS logs****,* que pueden ayudar a vincular al sospechoso con la actividad ilegal.
* Registros de eventos del servidor de correo electrónico, registros de pagos e información del suscriptor, que puede ayudar para la identificación del sospechoso y para vincular al sospechoso con la actividad ilegal.

## Temas legales

**Nota de Traducción**: Esta sección no fue traducida debido a que hace referencia a normas

legales de EEUU y no posee aplicaciones prácticas en la República Argentina.

## Resumen

Este capítulo introduce el concepto de redes que comparten archivos. Las redes FTP y P2P permiten a los usuarios compartir archivos. Los programas de cliente FTP permiten a los usuarios bajar archivos de un servidor central, mientras que los programas de cliente P2P permiten a los usuarios intercambiar archivos directamente entre computadoras. Los usuarios de red FTP y P2P pueden ocultar sus verdaderas direcciones IP a través del uso de servidores proxy, lo que significa que deben obtenerse oportunamente aquellos registros de eventos del servidor.

# Capítulo 7. Investigaciones sobre Intrusiones en la Red/Ataques de Denegación de Servicio.

Este capítulo tiene por objetivo ser un recurso para la investigación de una intrusión en la red o un ataque de Denegación de Servicio [Denial of Service (DoS)]. Dado que las intrusiones y los ataques DoS son frecuentemente implementados por medio del uso de un ***virus, gusanos (worm), Troyanos (Trojan)*** o *scripst*, se incluye una breve discusión acerca de estos programas. Las investigaciones de una red pueden ser muy complejas y pueden requerir una experiencia adicional que está más allá del alcance de este informe especial. Previo a encausar una investigación es muy conveniente obtener información del contacto para tales recursos. Sin embargo, hay algunos pasos básicos que se pueden tomar para identificar qué ocurrió y para preservar la evidencia para una posterior investigación.

## ¿Qué es una red?

Una red en su nivel más básico son dos o más dispositivos conectados de forma tal que usen hardware y software para permitir que los dispositivos se comuniquen. Los dispositivos tales como (pero no limitados a) computadoras, impresoras, routers, switches, dispositivos inalámbricos, puntos de acceso, laptops, y asistentes digitales personales pueden ser nodos de una o más redes. Un nodo es un componente de una red que realiza funciones relacionadas con ésta y se lo trata como a una entidad independiente. Los medios de conexión entre nodos pueden incluir cables (par trenzado, par no trenzado, coaxil), fibra óptica, inalámbrico, microondas, infrarrojo o satélite. La forma en que está configurada una red en términos de nodos y conexiones es su arquitectura. La arquitectura de la red puede variar desde dos dispositivos conectados entre sí en un lugar o cientos de miles de dispositivos conectados, que se encuentran en localidades geográficamente dispersas. Cualquier nodo en una red puede ser una fuente importante de evidencia cuando se investiga un delito basado en una intrusión en la red o un ataque de DoS.

## Virus, gusanos, y Troyanos

Los virus, gusanos y Troyanos generalmente son programas malignos *(****malware****)* que provocan una acción inesperada y frecuentemente no deseada sobre el sistema de la víctima. Un virus es un archivo ejecutable diseñado para extenderse a otras computadoras sin ser detectado. Puede ser transmitido como un adjunto a un correo electrónico, como una descarga (download), o estar presente en un diskette o CD. Un gusano es un tipo de virus que se auto-replica a través de una red, consumiendo los recursos del sistema y desacelerando o deteniendo el sistema. Un Troyano es un código maligno escondido dentro un programa aparentemente inofensivo que oculta su verdadera función.

## Scripts

Un script es un archivo que automatiza la ejecución de una serie de comandos. Los administradores de la red, a menudo, usan scripts para facilitar el cumplimiento de tareas tales como la creación de cuentas de usurario o la implementación de actualizaciones de seguridad. Los scripts se obtienen fácilmente, a menudo compartidos vía Internet, y pueden ser usados por personas con un conocimiento de computación limitado. Los scripts pueden usarse para descubrir y explotar las vulnerabilidades de una red.

## Intrusión en la red

Una intrusión es el acceso no autorizado o el acceso con exceso de privilegios de un usuario en una red. Una intrusión generalmente se lleva a cabo tomando ventaja de un sistema que no está correctamente configurado, una vulnerabilidad conocida que no fue enmendada (patched), o una implementación de seguridad débil, tal como una contraseña en blanco o fácilmente adivinable. Una vez que se logró el acceso a la red, el(los) intruso(s) pueden explotar el sistema de varias formas. Algunos ejemplos incluyen:

* + Recolección de información sobre inteligencia del sistema.
  + Determinación de cuentas y contraseñas de usuario.
  + Mapeo de la red.
  + Creación de cuentas o puertas traseras *(****backdoors****)* para ser usados más tarde.
  + Aumento de privilegios del usuario.
  + Uso de software ***sniffer*** para monitorear el tráfico de la red.
  + Uso de recursos de la red para almacenar y/o compartir archivos.
  + Acceso a datos propietarios o confidenciales.
  + Hurto o destrucción de datos.
  + Uso de recursos para identificar y explotar otros sistemas vulnerables.

## Denegación de Servicio (DoS)

Un ataque de Denegación de Servicio es una acción (o acciones) diseñada/s para desestabilizar la capacidad del sistema objeto del ataque, de brindar servicios de red e impedir que los usuarios accedan a los recursos. Un ataque DoS común genera un flujo de datos, imponiendo una demanda abrumadora sobre los recursos de un sistema, de forma tal que éste no puede responder a los pedidos legítimos. Aunque un DoS frecuentemente es intencional, también puede ocurrir en forma no intencional a través de un sistema mal configurado.

## Investigación de las intrusiones y ataques DoS

Uno de los primeros pasos que se toman en una investigación es identificar los individuos que tienen información relacionada con el incidente. En una investigación de una red, estos individuos pueden incluir:

* Administradores de la red.
* Empleados, actuales y anteriores.
* Usuarios de la red.
* Proveedores de Servicio de Internet (ISP).
* Consultores.
* Administrador(es) de tecnología de la información.
* Recursos humanos.
* Administradores de cuentas.

**Atención:** Tener en cuenta que cualquiera de los individuos listados arriba puede ser un sospechoso potencial o puede no estar abierto o ser sincero en cuanto a brindar información precisa.

La información adicional a recoger de una víctima incluye:

* Impacto económico del incidente.
* Medidas de seguridad de la red implementadas en el momento del incidente.

1. La identificación de la arquitectura de red es también importante. Generalmente, el administrador de la red también podrá brindar información sobre los dispositivos conectados a la red, su ubicación física y la forma en que están conectados. Otros recursos de la evidencia a considerar incluyen:

23.

* Computadoras y servidores conectados localmente.
* Usuarios y dispositivos remotos
* Proveedores de servicio de red externos:
  1. — Almacenamiento remoto.
  2. — Proveedores de servicios de aplicaciones.
  3. — Proveedores de servicios de backup remoto.

**Nota**: Tener en cuenta que los dispositivos que contienen evidencia pueden estar en diferentes edificios, estados o países.

El administrador del sistema debería poder brindar información sobre cualquier herramienta de administración del sistema o de las medidas de seguridad que estaban implementadas al momento del incidente o de los tipos de registros de eventos (logs) que se conservaban, y de los registros de backup desde el momento del incidente. Ejemplos de información que se puede obtener de los registros de eventos incluyen si:

* Se agregaron cuentas.
* Se agregaron, modificaron, copiaron o eliminaron archivos.
* Se configuraron acciones de seguridad o se agregaron **backdoors (puertas traseras)**.
* Se indica actividad de virus o Troyanos.
* Se copiaron herramientas de intrusión y **sniffer** a la red.
* Se registraron direcciones de Protocolo de Internet (IP) de los responsables aparentes del ataque.
* Se detuvieron o iniciaron servicios.
* Se cerraron o abrieron puertos.
* Ocurrió otra actividad relevante.

**Atención:** Si el registro de eventos no estaba conectado/habilitado, sugerir a la víctima que lo habilite para recopilar cualquier evidencia potencial de hechos futuros.

**Atención:** En muchas investigaciones sobre una red, la entidad que informa es la víctima. El investigador debería conocer las repercusiones de cualquier acción tomada en la recolección de la evidencia. Dependiendo de la situación, la respuesta de la investigación podría ser tan simple como reunir y examinar los archivos de registro de eventos, o tan compleja como incorporar un experto forense en redes de computación. Tener en cuenta que cerrar la red podría provocar la pérdida de ingresos.

## Redes inalámbricas

Mientras que muchas redes usan algún tipo de conexión física para la comunicación, se han tornado muy populares las redes inalámbricas que usan señales de radio para comunicarse. Una red inalámbrica es un método simple y económico de compartir recursos que no requieren una conexión de cableado directo. Sin embargo, el uso de una red inalámbrica requiere que el usuario esté próximo al punto de acceso inalámbrico. La fortaleza de la señal inalámbrica que está siendo transmitida determinará la distancia máxima a la que el usuario debe estar para usar los recursos de la red.

Dependiendo de la configuración, los usuarios deben poder conectarse a la red inalámbrica sin conocimiento del propietario de la red simplemente estando lo suficientemente cerca de la señal. Por ejemplo, “war driving” se refiere a la acción de buscar redes inalámbricas, utilizando un dispositivo inalámbrico para detectar los puntos de acceso a dichas redes. Ahora hay “hot spots” inalámbricos disponibles en muchos lugares públicos tales como aeropuertos, bares, bibliotecas y restaurantes de comidas rápidas.

La información a reunir durante una investigación de una red inalámbrica puede incluir si:

* El Identificador de Servicio [Service Set Identifier (SSID)] estaba siendo difundido/transmitido. El SSID es un identificador incluido en los paquetes para permitir la diferenciación entre redes inalámbricas múltiples. Todos los puntos de acceso y todos los dispositivos que usan una red inalámbrica específica deben usar el mismo SSID.
* La Wired Equivalent Privacy (WEP) estaba habilitada. WEP es una forma de cifrado que se usa para proteger la comunicación inalámbrica de escuchas secretas y para prevenir el acceso no autorizado a la red inalámbrica.

**Nota ArCERT**: WEP no es considerado un mecanismo robusto, en lo posible se debe utilizar WPA2.

* El Protocolo de Configuración Dinámica de Equipos [Dynamic Host Configuration Protocol (DHCP)] estaba habilitado y si los registros de eventos (logs) están disponibles. Cuando el DHCP está habilitado, automáticamente se configura y habilita un sistema para conectarse a la red.
* Se conservaron los registros de eventos (logs) de las conexiones inalámbricas establecidas.

Esta información ayudará a determinar el grado de vulnerabilidad que tenía la red para una intrusión. Si las medidas de seguridad arriba mencionadas estaban implementadas, un usuario no autorizado hubiera requerido conocimiento y/o herramientas especiales para poder acceder.

**Nota**: Este capítulo ofrece una introducción para las investigaciones de redes. Por naturaleza, este tipo de investigación es técnicamente compleja y hay probabilidad de que se requiera la asistencia de expertos especializados en esta área. Permanentemente se descubren vulnerabilidades y abusos y la información sobre estos temas es divulgada por varias organizaciones que incluyen a SANS (www.sans.org) y CERT (www.cert.org). Los productores de software antivirus brindan información relacionada con virus, Troyanos y gusanos, tales como Symantec (www.symantec.com), Computer Associates (www.ca.com), y F-Secure (www.f- secure.com).

## Temas legales

**Nota de Traducción**: Esta sección no fue traducida debido a que hace referencia a normas legales de EEUU y no posee aplicaciones prácticas en la República Argentina.

## Resumen

Este capítulo brinda detalles con respecto a los métodos usados para llevar a cabo intrusiones en la red y un ataque de Denegación de Servicios (DoS). El concepto de redes que comparten archivos cubre las redes de Protocolo de Transferencia de Archivo [File Transfer Protocol (FTP)] y las redes Punto a punto (P2P). Los virus, gusanos y Troyanos generalmente son programas maliciosos que pueden provocar una acción no esperada y frecuentemente no deseada sobre un sistema. Un script es un archivo que automatiza la ejecución de una serie de comandos y una intrusión es el acceso no autorizado o el acceso con exceso de privilegios de un usuario en la red. Se ofrecen consideraciones sobre las investigaciones de una red y se incluye información sobre conexión con cable físico y también sobre conexiones inalámbricas para comunicación. Uno de los primeros pasos a tomar en cualquier investigación es identificar a los individuos que tienen información relacionada con el incidente.

Apéndice A. Glosario

**ANI**: Ver **Automatic Number Identification** (Identificación Automática de Número).

**Automatic Number Identification** - Identificación Automática de Llamada: Un servicio que proporciona el número de teléfono de una llamada entrante.

**Backdoor** – (Puerta Trasera): Una puerta trasera generalmente evade los programas de seguridad y brinda acceso a un programa, a un servicio online o a todo un sistema de computación. Puede ser autorizado o no autorizado, documentado o no documentado.

**Client** - (Cliente): Una computadora o programa que se conecta o solicita servicios de otra computadora o programa. Cliente también se puede referir al software que permite a la computadora o al programa establecer una conexión.

**Clipboard** – (Portapapeles): Memoria temporaria de una computadora que permite al usuario almacenar texto y gráficos para un uso futuro.

##### DHCP - Ver Dynamic Host Configuration Protocol.

**Dynamic Host Configuration Protocol** – Un servicio que automatiza la asignación de direcciones de Protocolo de Internet (IP) en una red. DHCP asigna una dirección IP cada vez que una computadora se conecta a la red. DHCP usa el concepto de una “cesión” (“lease”) o cantidad de tiempo que una dirección IP dada será válida para una computadora específica. El DHCP puede reasignar direcciones IP dinámicamente para redes que tienen un requerimiento de más direcciones IP que las que están disponibles.

**Firewall** – (Corta Fuego): Un programa de software o dispositivo de hardware que protege del acceso no autorizado a los recursos de una red. Un firewall filtra los paquetes de la red para determinar si va a enviar los paquetes al destino requerido, permitiendo el acceso.

**Fully qualified domain name** - (Nombre de dominio totalmente calificado): El nombre jerárquico de un host (servidor) individual incluyendo el nombre de host junto con la ruta de red hacia ese host (por ej., adsl226.dyn996.pushme.nist.gov).

**Gateway**: Un dispositivo para direccionar tráfico entre redes. Típicamente, un gateway está físicamente en el perímetro de una red interna hacia Internet.

**Header** - (Encabezado): Información de identificación transmitida como parte del paquete de datos o del mensaje de correo electrónico o información de ruta de un grupo de contacto o de discusión (newsgroup).

**Malware**: Programa malicioso, desarrollado para producir inconvenientes, destrucción, o violar la política de seguridad

##### NAT - Ver Network Address Translation

**Network Address Translation** - Un servicio que permite que las computadoras en una red privada tengan acceso a Internet sin requerir públicamente su propia dirección de Protocolo de Internet (IP). NAT modifica los paquetes de la red que salen para que la dirección de retorno sea un host de Internet válido, protegiendo así las direcciones privadas de la vista pública.

**Packet** - (Paquete): Una unidad de transmisión que contiene datos y un encabezamiento que es ruteado (routed) entre un origen y un destino en una red.

**Point of Presence (POP)** - (Punto de Presencia): Un Punto de Presencia es un lugar físico que alberga a los servidores, routers, conmutadores ATM, y otros dispositivos. No hay que confundirlo con “Post Office Protocol” (Protocolo de Correo).

**Port** - (Puerto): Un punto de acceso abierto por el software— un “sitio de conexión lógica”—para mover información hacia o desde una computadora. A cada servicio de comunicación en una computadora (por ej., FTP, e-mail, Web) se le asigna un número de puerto. Los puertos están numerados desde 0 a 65535. Los puertos 0 a 1023 están reservados para ser usados para ciertos servicios estándar.

**Post Office Protocol (POP)** - (Protocolo de Correo): Un protocolo usado para recuperar correo electrónico de un servidor de correo.

**Protocol** - (Protocolo): Un conjunto estándar de reglas que gobiernan la forma en que las computadoras se comunican o realizan una acción.

**Proxy server** - (Servidor Proxy): Un servidor que actúa como un intermediario entre un usuario de una estación de trabajo e Internet para facilitar la seguridad, el control administrativo y los servicios de “cache”. Un servidor de proxy trabaja como un gateway que separa una red (interna) de la red externa (Internet) y como un firewall que protege la red de la intrusión externa.

**RADIUS logs** - (Remote Authentication Dial-In User Service); Método para autenticar usuarios remotos conectándose a una red. Los registros de un servidor RADIUS proporcionarán la dirección IP (Internet Protocol) o un número de teléfono del usuario que está solicitando autenticación para la red.

**Redirector** - (Redireccionador): Un dispositivo o comando utilizado para enviar o rutear tráfico de Internet a otra dirección de IP; a veces es utilizado para ocultar la dirección fuente o de destino.

**Router** - (Ruteador): Un dispositivo que determina el siguiente punto de la red al cual el paquete de datos debe ser enviado para llegar a su destino. El router está conectado a por lo menos dos redes y determina qué curso va a tomar cada paquete de datos basado en su conocimiento actual del estado de las redes a las cuales está conectado.

**Server** – (Servidor): Una computadora que proporciona archivos y servicios para uso por parte de otras computadoras.

**Sniffer** – (Husmeador): Software que monitorea los paquetes de red que pueden ser usados para interceptar datos incluyendo contraseñas, números de tarjeta de crédito, etc.

**Spoof** – (Alteración con fines fraudulentos): Cambiar la información de identificación a fin de esconder la verdadera identidad.

**Telnet** -: Aplicación de Protocolo de Internet para iniciar una sesión remota con una terminal.

**Threads** – (Hilos - Tramas): Grupos de mensajes y respuestas asociados, generalmente pertenecientes a un mismo tema de discusión.

**Trojan** – (Troyano): Una aplicación que abiertamente hace una cosa mientras que encubiertamente hace otra.

**UTC:** Coordinated Universal Time es el nuevo estándar de tiempo mundial basado en un reloj atómico altamente preciso, utilizado en reemplazo de la Hora de Greenwich (Greenwich Mean Time - GMT). El UTC, como el GMT, están fijados en el grado 0 de longitud en el meridiano principal.

**Virus**: Una aplicación maliciosa que por su propio diseño, se propaga de una computadora a otra.

**Wayback Machine**: Un archivo histórico del contenido de la World Wide Web que se encuentra en [www.archive.org.](http://www.archive.org/)

**Worm** – (Gusano): Un tipo de virus que se auto replica a través de la red.

# Apéndice C. Acceso a Encabezados Detallados en los Mensajes de Correo Electrónico

|  |  |
| --- | --- |
| Software del cliente de correo electrónico | Mostrar Información Detallada del Encabezamiento |
| AOL® | Seleccionar **Mail**, seleccionar **Mail Settings**, seleccionar  **Advanced**, luego seleccionar **Never Minimize Headers**. |
| Claris Emailer® | Bajo **Mail**, seleccionar **Show Long Headers**. |
| Eudora® (antes versión 3x) | Seleccionar **Tools**, seleccionar **Options**, seleccionar **Fonts & Display**, luego seleccionar **Show all headers**. |
| Eudora® (ver. 3.x a ver. 6x IBM® o Macintosh®) | Seleccionar el botón **BLAH, BLAH, BLAH** en el mensaje de mail entrante. |
| GroupWise® | Hacer clic en “**actions” and “delivery.”** |
| HotMail® | Seleccionar **Options** en la barra de navegación de Hotmail® a la derecha de la página. En la página de Options, seleccionar **Preferences**. Bajar hasta **Message Headers**, y seleccionar **Full**. |
| Lotus Notes® 4.6.x | Desde la barra de menú, seleccionar **Actions**, luego seleccionar **Delivery Information**. |
| Lotus Notes® R5 | Desde la barra de menú, seleccionar **Actions**, seleccionar  **Tools** luego seleccionar **Delivery Information**. |
| Netscape® 4.xx | Hacer doble clic sobre el mensaje de e-mail. Seleccionar  **View Headers**, luego seleccionar **All**. |
| Outlook® | Hacer doble clic sobre el mensaje de e-mail en su bandeja de entrada para abrir el mensaje. Seleccionar **View**, luego seleccionar **Options**. |
| Outlook Express® | Abrir el mensaje de e-mail. Desde el menú File hacia abajo (drop-down menú), seleccionar **Properties**, luego seleccionar la pestaña **Details**. |
| PINE | Activar la opción de encabezamiento en setup, luego tipear “h” para obtener los encabezamientos. |

Algunos clientes de correo electrónico no cumplen con ninguno de los estándares de Internet (por ejemplo, cc-Mail, Beyond Mail, VAX VMS) y por lo tanto no mantienen la información detallada del encabezado. No será posible obtener encabezados detallados desde estos mensajes de correo electrónico.

Cuando se investiguen mensajes de correo electrónico enviados dentro de una intranet (red interna), es necesario saber que en muchos casos no se generan encabezados de correo electrónico. América Online (AOL) actúa como una intranet para los mensajes de correo electrónico que se envían desde un miembro de AOL a otro miembro de AOL. Estos mensajes no contienen una información de encabezados de mensaje de correo electrónico estándar. Sin embargo aún se puede disponer de una identificación del mensaje de correo electrónico.

# Apéndice D. Lista de Control Sugerida para la Investigación sobre Archivos Compartidos

##### Hay presentes archivos/datos ingresados sin autorización o se cometió un delito

* + Confirmar jurisdicción.Identificar al sospechoso.
  + Identificar cualquier nombre oculto (screen names) y cómo se conectan con el sospechoso. Identificar el programa utilizado.
  + Detallar cómo se ubicó al sospechoso.
  + Determinar si hay alguna evidencia exculpatoria presente (Troyano, virus, etc.).
  + Revisar la declaración/entrevista/confesión.
  + Usar los métodos y procedimientos de investigación tradicionales.
  + Establecer el intento.
  + Consultar a un experto si fuere necesario.

##### Consideraciones Online

* + - Nombres/números de cuenta.
    - Información del servidor (host).
    - Contraseñas.
    - Canal/sala.
    - ¿Estaba el sitio FTP activo—IP era ruteable?
    - Servicio que está siendo usado.

##### Documentación

* + - Cronogramas.
    - Cadena de custodia-registros de eventos (logs)/archivos.
    - Resumen.
    - Glosario.
    - Ayudas Visuales.
    - Antecedentes del sospechoso en Internet
    - Notas positivas en cada etapa de la investigación.
    - Apéndice de evidencia.
    - Fotos/impresiones de pantalla.