# Pruebas documentales y periciales de Internet en el marco del Procedimiento Civil Colombiano.

**Índice.**

1. [INTRODUCCIÓN GENERAL. 2](#_TOC_250025)
2. [PRUEBAS DE INTERNET DOCUMENTALES. 4](#_TOC_250024)
   1. CORREOS ELECTRONICOS. 5
      1. [Cómo funciona el correo electrónico. 5](#_TOC_250023)
      2. [Componentes básicos de un correo electrónico. 8](#_TOC_250022)
      3. [Temas a tener en cuenta. 14](#_TOC_250021)
      4. Presentación de correos electronicos aspectos formales. 15
3. [Pruebas documentales de sitios web. 19](#_TOC_250020)
   1. [Viendo la fuente HTML de una página web. 20](#_TOC_250019)
   2. [Capturando información de una página web. 21](#_TOC_250018)
      1. [Capturar un pantallazo. 21](#_TOC_250017)
      2. [Comando “guardar como” . 22](#_TOC_250016)
      3. [Herramientas para capturar sitios web. 24](#_TOC_250015)
   3. [Embalaje y presentación de páginas de Internet. 25](#_TOC_250014)
      1. [• Legitimidad. 25](#_TOC_250013)
      2. [• Autenticidad. 26](#_TOC_250012)
      3. [• Integridad. 26](#_TOC_250011)
4. [Pruebas relacionadas con los Servicios de Mensajería Instantánea y Salas de Chat. 27](#_TOC_250010)
   1. [Servicios de mensajería instantánea. 29](#_TOC_250009)
   2. [Cómo funcionan los servicios de Mensajería Instantánea (IM). 30](#_TOC_250008)
   3. [Consideraciones para tomar la evidencia. 31](#_TOC_250007)
   4. [Salas de Chat. 33](#_TOC_250006)
   5. [Recolección, embalaje y presentación de chats. 34](#_TOC_250005)
5. [Pruebas periciales en Internet. 34](#_TOC_250004)
   1. [Traza de correos - rastreando un e-mail. 36](#_TOC_250003)
      1. [Qué es una dirección ip? 36](#_TOC_250002)
   2. [Lectura y/o análisis de logs. 37](#_TOC_250001)
   3. [Reconstrucción de lo navegado en Internet. 37](#_TOC_250000)

1 Abogado, Magister Bussines Administrator, especializado en derecho de Nuevas Tecnologías, derecho administrativo, Certificado por la Unión Europea en Manejo de Evidencias Digitales y Cibercrimen; profesor de crímenes de alta tecnología, pruebas técnicas e inspección judicial, manejo legal de incidentes informáticos, evidencias digitales, seguridad de la Información, litigios de Internet, entre otros.

* 1. **Otras pericias informáticas. 37**

# INTRODUCCIÓN GENERAL.

Las pruebas que nacen de Internet o pasan por esta red, día a día cobran mayor relevancia, es claro que las comunicaciones en general viajan por este medio, cartas, miles de negocios, documentos del comerciante, relaciones personales o familiares y en general todo aquello que existió en el mundo que construimos de papel se esta digitalizando, al punto que por ejemplo el certificado de pago de seguridad social, audiencias de juicios penales, pasado judicial, contratación pública, entre otros no existen sino en este gran universo de bits.

Así es como en los procesos judiciales, ya no es extraño ver como prueba correos electrónicos, chats, paginas web, log´s, fotografías digitales, videos, archivos de audio, DVD´s y en general todo tipo de información almacenada, generada, transmitida, visualizada o recibida en un computador, un teléfono móvil, pda´s, gps, memorias Usb, teléfonos ip, cámaras, grabadoras, vehículos con computador y en general medios ópticos, digitales o electrónicos.

La validez de estos medios de prueba de marras es innegable, pues como pruebas documentales han sido introducidos por la ley 527 de 1999, así el principio de equivalencia funcional2, hace que siempre que cumplan los requisitos normativamente exigidos tendrán

2 Tomado de manual de seguridad de la Información Rincón Cárdenas Eric y Guzmán Caballero Andrés. [www.adalidabogados.com/alumnos/guia1.pdf](http://www.adalidabogados.com/alumnos/guia1.pdf) *“La equivalencia funcional entre el documento papel y el documento electrónico se ve complementada con los equivalentes funcionales de firma, original y archivo2. El artículo 6 de la Ley 527 de 1999 establece que cuando una norma exija que determinada información conste por escrito, este requisito queda satisfecho con un mensaje de datos. Otros principios jurídicos de los medios electrónicos, que merecen especial atención son. 1) La neutralidad tecnológica; 2)Buena fe; 3)La libertad contractual; 4)No modificación y/o alteración del régimen general de contratos; 5)Transparencia; 5)Seguridad. El artículo 5° de la Ley atribuye efectos jurídicos, validez y fuerza obligatoria a los mensajes de datos. El capítulo II de la Parte I – Parte General – (Artículos 6°, 7°, 8° y 9° ) regula el escrito, la firma, el original y la integridad de un mensaje de datos. En general la legislación dispone que cuando cualquier norma requiera que la información conste por escrito, que se presente o conserve en su forma original, exija la presencia de una firma o prevea consecuencias por su ausencia, se entenderán satisfechos los requerimientos si se cumplen las*

la misma validez legal que cualquier otro documento impreso, mecanografiado o fijado de cualquier forma en papel.

Ahora bien las pruebas documentales recaudadas en la Web y presentadas en formato digital, para ser valoradas por un juez tendrán que tener siempre estos requisitos de forma, por lo que he de aclarar que la simple impresión de un correo o una página de Internet no es

un mensaje de datos y no podrá ser valorado prueba documental, será necesario entonces un tratamiento técnico pertinente que garantice la integridad, disponibilidad, no repudio y legalidad de la prueba como veremos para su presentación.

Hoy día existe una creencia errada entre algunos juristas que piensan que en general si en un proceso para la extracción, presentación o preservación de evidencias digitales media un computador y/o un ingeniero estamos hablando de pruebas periciales, afirmación evidentemente incongruente, razón por la que haremos un paralelo que diferencie los dos tipos de pruebas, periciales y documentales, que se puedan presentar en Internet hoy día, sin olvidar que para todos es claro que la tecnología avanza a una velocidad mayor que la normatividad, por lo que pronto podrán ser más.

*siguientes condiciones, así: (i) en relación con el escrito, si la información que el mensaje de datos contiene es accesible para su posterior consulta; (ii) en relación con la firma, si se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y que permita indicar que el contenido cuenta con su aprobación y, que el método sea confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado; (iii) en relación con el original, si existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de dato o en alguna otra forma y, de requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se debe presentar.2”*

# PRUEBAS DE INTERNET DOCUMENTALES.

Recordemos inicialmente que las pruebas generadas en Internet, por regla general son mensajes de datos3, de conformidad con los artículos 2, 5, 6 y 10 de la ley 527 de 1999, que la incluyen dentro de las descritas en el capitulo VIII del titulo XIII, sección tercera, del libro segundo de Código de Procedimiento Civil, es decir las pruebas documentales.

Hemos de aclarar que tratándose de evidencias digitales, cuando hablamos de archivos y existiendo varios, si estos son digitalmente idénticos no estaremos hablando de copias, todos ellos serán originales de conformidad con el articulo 8 de la citada ley 527, por ej. si Camila envía un correo electrónico a Pedro, este documento estará en el equipo donde se creó, es decir el computador de Camila, también en el servidor de correo de Camila, puede ser Gmail® o Yahoo®, y en el equipo y servidor de correo de Pedro, pero legalmente todos los archivos son iguales, siempre que cuando se presente la prueba exista alguna garantía confiable de que se ha conservado íntegro desde que se generó, esto se puede lograr por varios medios técnicos siendo el más confiable una estampa cronológica de fecha y hora emitida por una entidad Certificadora abierta avalada por la Superintendencia de Industria y Comercio para tal fin; también se puede colocar un mecanismo llamado sistema HASH4 además la ley exige que se pueda presentar.

3 Ley 527 de 1999 ARTICULO 2o. DEFINICIONES. Para los efectos de la presente ley se entenderá por: a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

4 Tomado de www.adalidabogados/alumnos/glosarios.pdf . En informática, **Hash** se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o*algoritmo hash*. Un **hash** es el resultado de dicha función o algoritmo.

Una **función de hash** es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo).

# Correos Electrónicos.

Los correos electrónicos, son hoy día la forma más común de comunicar todo tipo de información, así son el 90% de las evidencias digitales presentadas en procesos judiciales en el mundo, por esto los juristas debemos tener clara la forma correcta de preservarlos, embalarlos y presentarlos en procesos judiciales.

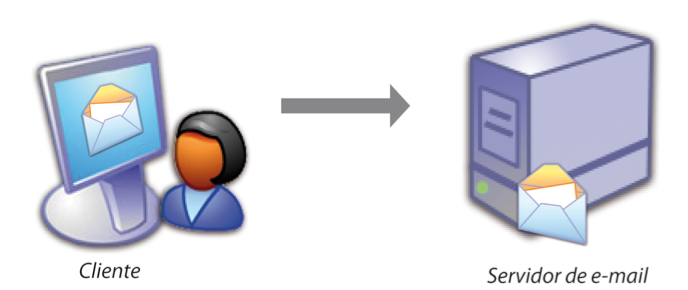
Por regla general los e-mails son pruebas documentales, que se entienden correspondencia, sin dejar a un lado que sobre ellos podrán practicarse todo topo de pruebas periciales como lo veremos en este documento; verbigracia las pruebas documentales y grafológicas que se realizan sobre cualquier documento en soporte de papel.

# Cómo funciona el correo electrónico.

El correo electrónico puede generarse de diferentes formas y equipos, aunque la forma más común es cuando un usuario compone un mensaje en su propio computador o teléfono móvil y luego lo envía a su servidor de correo. En este punto el computador del usuario ya no participa más en el proceso, pero el servidor de correo aún debe enviar el mensaje. El servidor de correo funciona como si fuese una oficina de correos pero electrónica –envía y recibe el correo Electrónico. La mayoría del tiempo, el servidor de correo es un equipo diferente del computador en el que se escribió dicho mensaje de correo. (Ver la figura 1)

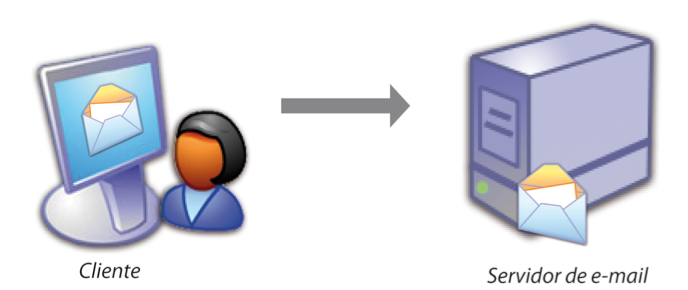
Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada. Una propiedad fundamental del *hashing* es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.

Figura No. 1.



El servidor de correo del remitente envía el mensaje buscando y encontrando el servidor de correo del destinatario y remite el mensaje a esa ubicación. El mensaje luego se almacena en ese segundo servidor de correo y queda a disposición del destinatario. Por “e-mail *client”* se conoce a el software usado para redactar y leer el mensaje de correo electrónico por ej. Gmail® o Yahoo®. Dependiendo de cómo se configure el “e-mail client” se podrá encontrar una copia del mensaje en el computador del destinatario, otro aparato electrónico como un teléfono móvil o una PDA y/o el servidor de correo o sus cintas de backup (copia de respaldo). También podrá encontrarse una copia del e-mail en el computador del remitente en la bandeja de elementos enviados o en la papelera o en el servidor de correo del remitente o sus cintas de backup. Ver la Figura 2.

Figura 2. Enviando el correo electrónico



A medida que el mensaje viaja a través de la red de comunicaciones, en un área del mensaje denominada *encabezado (header,* en inglés) queda un registro abreviado del recorrido del correo electrónico; como en el sobre de una carta los sellos postales o estampillas fijadas por donde pasa. A medida que el mensaje se enruta a través de uno o más servidores de correo, cada servidor incluye en el encabezado del mensaje su propia información. Una de las pruebas periciales es la “traza de correos” que no es más que identificar las direcciones IP5 (Internet Protocol) del encabezado y emplear esta información para establecer el remitente del mensaje, usando las técnicas apropiadas.

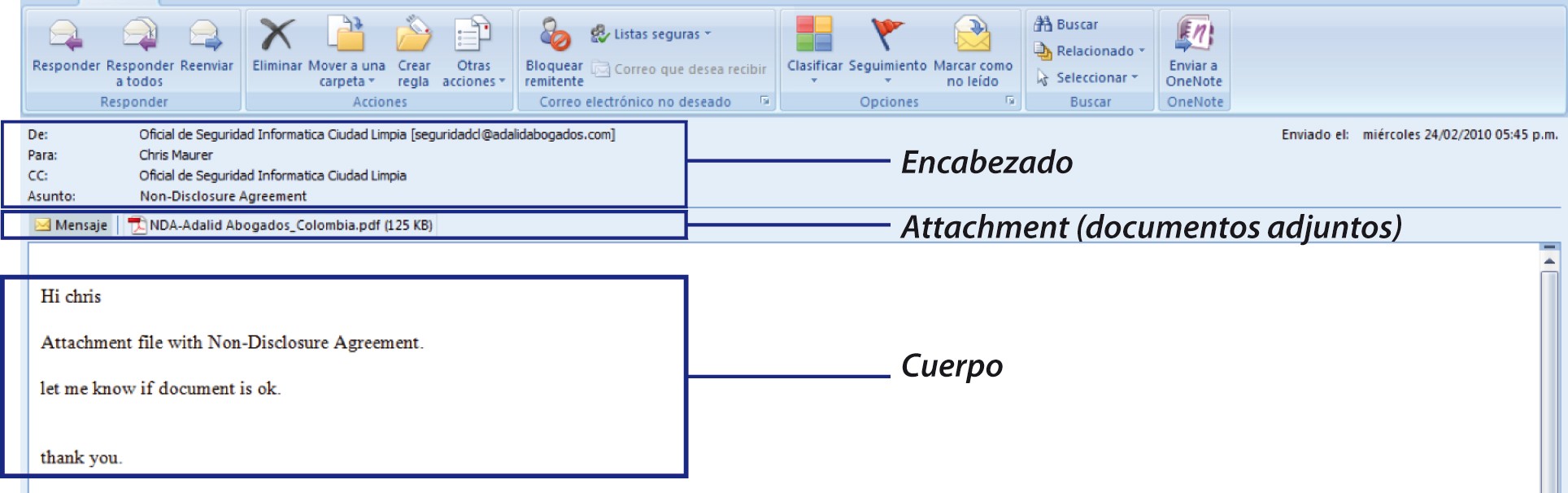
1. Dirección ip: Del mismo modo que una casa tiene una dirección, cada computador conectado a Internet también la tiene. Se le conoce como dirección IP (Internet Protocol, en inglés). Tomado de [www.adalidabogados.com/alumnos/glosarios](http://www.adalidabogados.com/alumnos/glosarios)

# Componentes básicos de un correo electrónico.

Existen varios métodos para crear y enviar correos electrónicos. La apariencia de un correo electrónico depende del dispositivo o del software usado. Sin embargo, típicamente un mensaje tiene un encabezado y un cuerpo (body en ingles) y puede ir acompañado de documentos adjuntos. El encabezado del correo electrónico contiene la información de envío y la ruta que el e-mail debe tomar desde el remitente hasta el destinatario, el cuerpo contiene el contenido de la comunicación. Los documentos adjuntos (attachment en inglés) pueden ser de cualquier tipo de archivo como por ejemplo fotos, documentos, archivos de sonido y de video.

La primera vez que se ve un mensaje de correo electrónico, se despliega sólo una pequeña porción del encabezado. Por lo general, esta información la escribe el remitente, tal como se muestra en la figura 3.

Figura 3. Componentes de los correos electrónicos



Sin embargo, el e-mail que se muestra arriba no muestra toda la información disponible. La información adicional del correo puede obtenerse mirando el encabezado con más detalle,

lo cual puede hacerse de varias formas dependiendo del programa que se esté usando, por ejemplo:

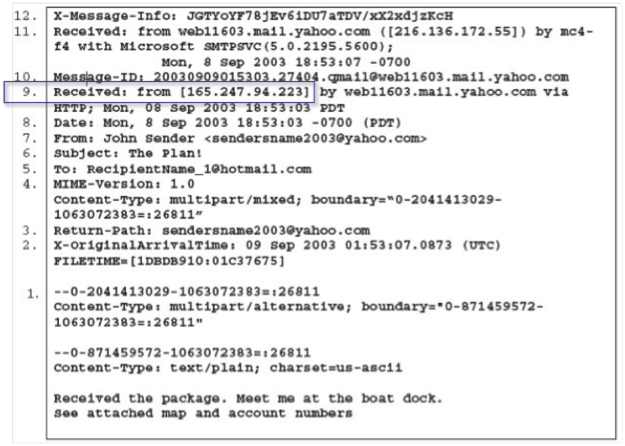
Cuadro 1.

|  |  |
| --- | --- |
| **Software Cliente de Correo Electrónico e- mail clients** | **Desplegando la Información Detallada del Encabezado** |
| **Gmail®** | Buscar la opción “mostrar original” en la parte superior derecha del mensaje, al lado derecho de “responder”. Se  abrirá otra ventana con la información. |
| **Hotmail®** | Hace clic sobre el botón derecho del Mouse, y escoge la opción “Ver código Fuente del Mensaje”**.** |
| **Outlook®** | Haga doble clic en el mensaje de correo en su bandeja de entrada para abrir el mensaje. Seleccione **View (Vista),** luego seleccione **Options (Opciones).** |

\*\*\*Tenga en cuenta que no todos los e-mail clients están en la lista y que las actualizaciones a estas aplicaciones pueden modificar el método para obtener información detallada del encabezado.

Usualmente, el recorrido del mensaje puede reconstruirse leyendo el encabezado del correo desde arriba hacia abajo. A medida que el mensaje pasa a través de servidores de correo adicionales, cada uno añade su información por encima de la información anterior en el encabezado. Una de las más importantes partes del correo que se debe obtener del encabezado detallada es la dirección IP de origen. La dirección del ejemplo en la figura 4 es [165.247.94.223) .

Figura No. 4.



Abajo se describe el encabezado línea por línea con el fin de entender las partes que lo componen de acuerdo con la figura 4. Observe que el encabezado del e-mail lo componen dos áreas generales: *encabezado del sobre* y el *encabezado del mensaje.*

El *encabezado del sobre* contiene información que han añadido al encabezado los servidores de correo que reciben el mensaje durante su recorrido. Las líneas “Recibido:” y la línea Message-ID son los componentes principales del encabezado del sobre y, por lo general, son más difíciles de *burlar.* En el siguiente ejemplo, las líneas 9 a 12 son parte del encabezado del sobre.

El *encabezado del mensaje* contiene información que el e-mail client del usuario añade al encabezado. Generalmente, esta información es creada por el usuario y es la más fácil de

burlar, contiene el Para:, De:, Ruta de retorno: (Return-Path, en ingles), Asunto: Tipo de contenido: (Content-Type, en inglés) y la primera fecha y hora. En el siguiente ejemplo las líneas 2 a 8 forman parte del encabezado del mensaje.

12. X-Message-Info: JGTYoYF78jEv6iDU7aTDV/xX2xdjzKcH

*Los X-headers son encabezados inusuales y no son esenciales para el envío del correo. Para poder obtener alguna utilidad de los x-header será necesario indagar con el Proveedor de Servicios de Internet (ISP Internet Service Provided, en ingles) que es quien provee en este caso la cuenta de correo.*

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

*Recibido:*

*La línea “Recibido” es la última que se pega en el encabezado. El último servidor de correo que recibe el mensaje la coloca allí e identifica el servidor de correo del cual se recibe el e-mail. Note que la fecha y la hora la genera el servidor de correo que recibe e indica un ajuste de la UTC (-0700). En este ejemplo se indica el nombre del servidor de correo. Esto se puede obtener cuando el servidor que recibe descifra la dirección IP del último servidor de correo o por que el servidor de correo transmite su propio nombre*

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

*Message-ID: (dientificación del mensaje)*

*Es un identificador único asignado a cada mensaje. Usualmente lo asigna el primer servidor de correo y es pieza clave de información. A diferencia de la dirección IP de origen (abajo), la cual puede suministrar información del suscriptor, la message-id puede conectar el mensaje con el remitente si es que se logra contar con los registros pertinentes.*

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

*Recibido:*

*La línea “Recibido” de abajo identifica la dirección IP del servidor de correo de origen. Puede indicar el nombre del servidor, el protocolo empleado y la configuración de fecha y hora del servidor. Note que se reporta información de la zona horaria.*

*CUIDADO: Si la fecha y hora relacionada con el e-mail llegan a ser importantes para el proceso deberá tener en cuenta que la hora registrada en esta línea “Recibido” en el encabezado del correo, proviene del servidor de correo y puede no ser muy precisa.*

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

*Fecha:*

*Esta fecha la asigna la máquina del remitente y puede no coincidir con la indicación de fecha y hora del servidor de correo. Si la fecha y hora de creación del mensaje llega a ser importante para el proceso, tenga en cuenta que la hora registrada en el encabezado del e- mail viene de la máquina del remitente y puede no ser precisa.*

7. From: John Sende[r <s](mailto:sendersname2003@yahoo.com)e[ndersname2003@yahoo.com](mailto:sendersname2003@yahoo.com)>

*De:*

*Por lo general, ésta información la configura el usuario en la aplicación (e-mail client) y puede no ser muy confiable.*

6. Subject:The Plan!

*Asunto:*

*Esta información la ingresa el usuario.*

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

*Para:*

*Esta información la ingresa el usuario.*

4. MIME-Version: 1.0 Content-Type: multipart/mixed; boundary=”0-2041413029- 1063072383=:26811”

*El propósito de estas dos líneas es dar información al e-mail client del destinatario sobre cómo interpretar el contenido del mensaje.*

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

*Trayecto de retorno:*

*Por lo general, esta información la configura el usuario en su aplicación (e.mail client) y por consiguiente, puede no ser muy confiable.*

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

*Los X-headers son encabezados poco comunes y no son necesarios para el envío del correo. La utilidad de los X-header deberá establecerse con el ISP.*

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

*Información de la aplicación; no relevante para la prueba.*

Una vez se identifiquen las direcciones IP en el encabezado, podrán usarse los procedimientos para rastrear el recorrido del e-mail. Tenga en cuenta que las direcciones IP pueden ser creadas o burladas en un intento por esconder la verdadera identidad del remitente.

# Temas a tener en cuenta.

**Los encabezados pueden ser burlados en los e-mail**: Cualquier cosa en el encabezado de un mensaje hasta la última línea “Recibido:” (que es la más importante de todas) puede ser burlado o falseado. Compare la información en el encabezado del mensaje con aquella en el encabezado del sobre. Si las dos no coinciden, existe la posibilidad de que el correo haya sido burlado.

**Ubicaciones remotas:** Advierta que existen muchos lugares públicos de acceso remoto a Internet como bibliotecas, colegios, aeropuertos, hoteles y cafés Internet. Si se envía un mensaje de correo electrónico desde alguno de estos sitios resultará muy difícil determinar

el remitente real de dicho mensaje, pero con un arduo trabajo pericial se podrá localizar al iniciador.

**Posponer el envío:** Muchos proveedores y aplicaciones (e-mail clients) tienen la funcionalidad para programar el momento en que se enviará el e-mail. De igual manera, algunos servidores envían el mensaje en ciertos momentos preprogramados. Cualquiera de estas situaciones podrá permitir a los individuos estar en otro lugar al momento en que el correo sea enviado.

**Ubicación del e-mail:** Sin importar el tipo de correo electrónico que se use, el mensaje puede almacenarse en múltiples ubicaciones. Considere obtenerlo de tantas fuentes como sea posible. Por ejemplo, si el mensaje es de tipo web y un proveedor de servicios (Ej. Gmail®, Hotmail®, Yahoo!®) lo tiene almacenado, el tiempo es crucial pues muchas de estas compañías tienen políticas de purga o limpieza de información después de un cierto periodo de tiempo. Será necesario, entonces, emitir una carta de preservación, dirigida al proveedor para evitar, precisamente, la purga de datos; puede ser solicitada al Juez como prueba anticipada.

# Presentación de correos electrónicos aspectos formales.

Por lo volátiles que resultan ser las evidencias digitales este es el tema más relevante, es por ello que si no se tiene la pericia o conocimientos en informática es recomendable dejarlo a

expertos que utilicen equipo especializado.

Lo primero es determinar dónde se encuentran los correos, es decir si están alojados en el cliente de correo electrónico (Ej. Gmail®, Yahoo®, Hotmail®) servidores empresariales o en

programas de ordenador que los almacenan como Entourage, Outlook®/Outlook Express® y Netscape®.

Si están alojados en el Cliente de correo, es esencial garantizar que se guarden digitalmente con el encabezado, para esto deberá ingresar directamente desde el explorador (ej. explorer®, firefox®, chrome®) y verificar que en el computador quede guardado como

.Html o .Php según la opción asignada, pero siempre asegurando que sea el formato original, como se explica en el cuadro 1.

Si el documento esta alojado en un programa de ordenador, deberá guardarlo en el formato original, por ejemplo en Outlook®, escribir guardar como y escoger el formato .msg para conservar tanto el texto como el encabezado, paso siguiente deberá hacerle una estampa cronológica de fecha y hora, colocar una firma digital o un Hash, con las herramientas tecnológicas pertinentes, para así lograr garantizar que el documento no ha sido ni será alterado en el proceso, al mismo tiempo es recomendable guardar en dos formatos asequibles, el encabezado y el texto del correo, por ejemplo .pdf y .rtf como se muestra en la figura 4 y 5.

Figura 5.

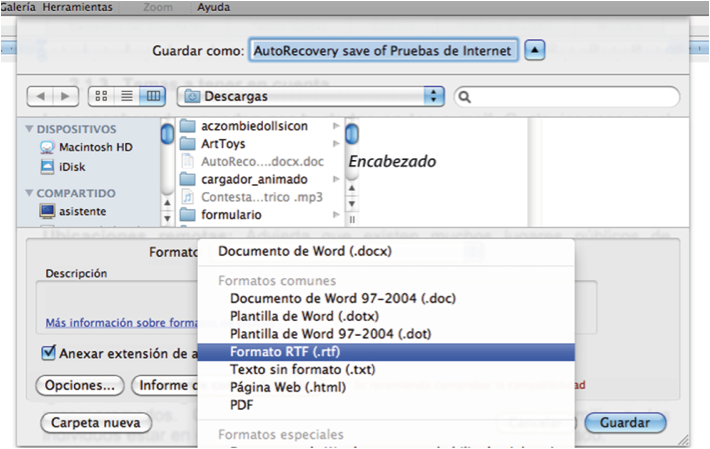
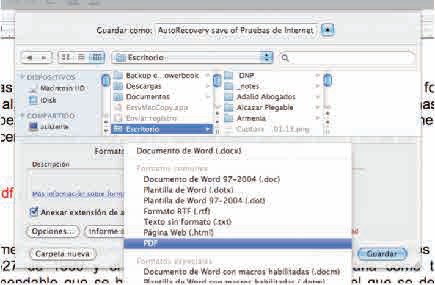
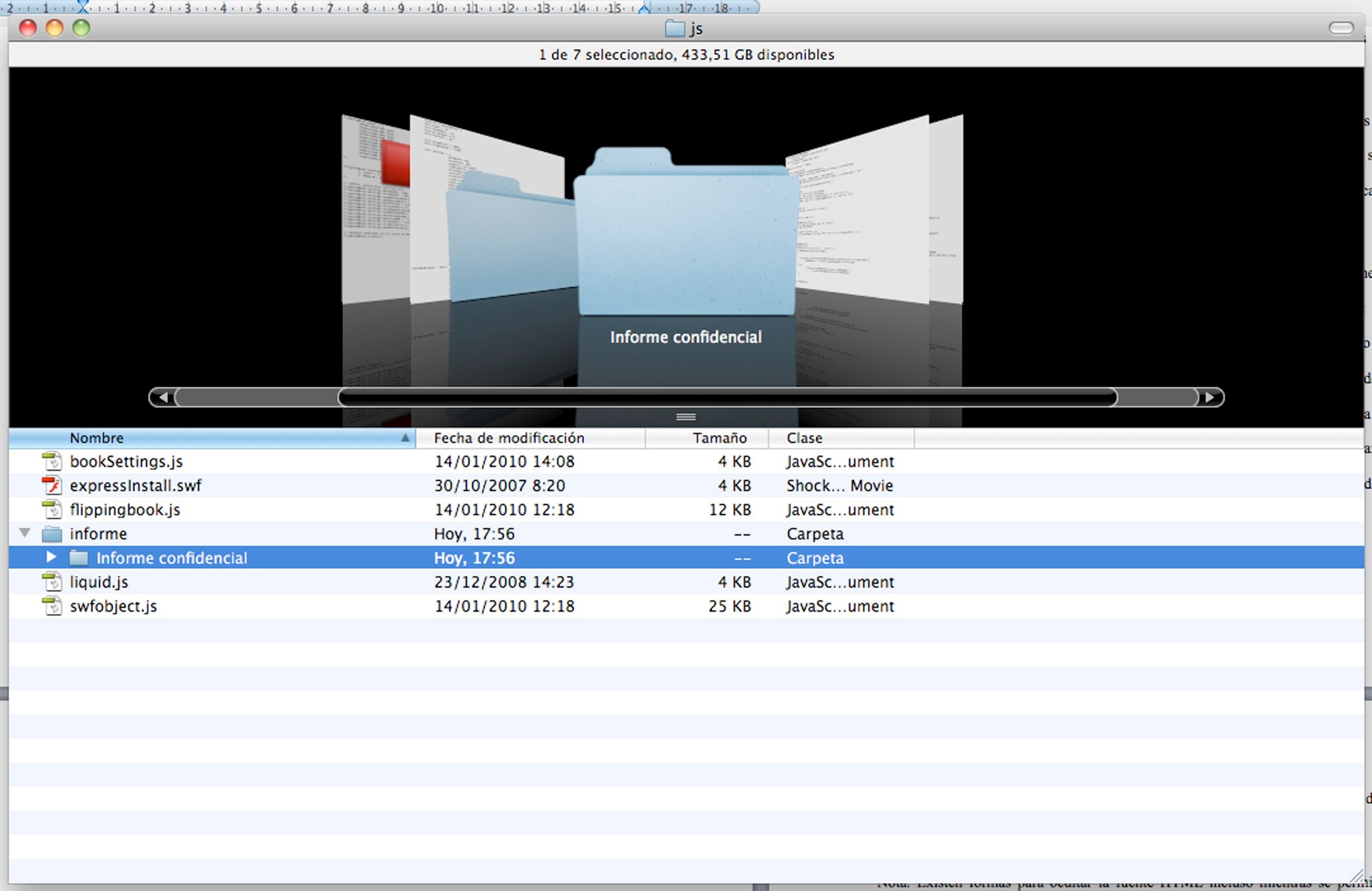


Figura 6.



Así las cosas ya guardados el texto de correo y encabezado en su formato original, el archivo de aseguramiento digital (ej. Estampa cronológica, hash) los encabezados y textos en formatos .rtf y .pdf deberá embalarse en un medio de almacenamiento como un DVD que se cierre técnicamente y verse así:

Figura No. 7.



Finalmente pese a que la evidencia digital tiene los requisitos exigidos por la ley 527 de 1999 y el juez deberá aceptarla y valorarla como tal, es recomendable que se haga un breve informe impreso en el que se describa claramente qué clase de prueba es, el contenido del encabezado, el texto del correo y se detalle el proceso seguido para garantizar la integridad de la prueba documental.

# PRUEBAS DOCUMENTALES DE SITIOS WEB.

He de advertir que por regla general las páginas de Internet o páginas web, son mensajes de datos es decir pruebas documentales, siempre que tengan los requisitos que la ley 527 de 1999 exige, estas son muy importantes pues son fácilmente cambiantes en su esencia, razón de más por la que deberá existir basta atención en su recolección, embalaje y presentación.

Se debe tener claro que por lo general, un sitio web es un conjunto de páginas web o archivos relacionados (como fotos, sonidos o texto) que se almacenan en un servidor web. El lenguaje típico en el que están escritas o diseñadas estas páginas es HyperText Markedup Language (HTML). Este lenguaje permite a los usuarios navegar fácilmente entre las páginas o archivos del grupo o conjunto de páginas, también permite conectar un grupo relacionado de páginas a otro grupo relacionado de páginas, en palabras simples, el HTML permite crear conexiones entre sitios web.

Un servidor web es un computador con software especial que provee páginas web a los clientes a través de Internet. Un servidor web puede hospedar múltiples sitios web, adicionalmente, los archivos que componen un solo sitio web pueden estar localizados en más de un servidor web.

Para accesar a una página web se digita un Localizador de Recursos Uniforme (Uniform Resource Locator o URL, en inglés) en un navegador web como Internet Explorer®, Netscape® Navigator®, or Mozilla®. el URL es la dirección del recurso o archivo disponible en Internet y contiene el *protocolo* del recurso (p.e. http://, https://) el nombre del dominio

del recurso y el nombre jerárquico del archivo (dirección) . Por ejemplo, una página en Internet puede localizarse en el URL [http://www.urosario.edu.co.](http://www.urosario.edu.co/) La primera parte (http://) indica el protocolo; la siguiente parte (www) es un apuntador a un servidor web; y urosario.edu.co es el dominio.

Los hipervínculos (links) son atajos que emplean los usuarios para navegar de una página web a otra página web o archivo sin tener que ingresar manualmente la dirección URL complete. Los links pueden esconderse en las páginas web de manera que solo los usuarios que la conocen puedan encontrarlos. Los links también pueden re-direccionar el servidor web automáticamente a un sitio web distinto.

Se deberá tener en cuenta que a pesar de que las páginas web típicamente se escriben en HTML, también pueden estar escritas en lenguajes script. Estos lenguajes permiten que la página web despliegue contenido individualizado para cada usuario; el contenido puede entonces adaptarse a la medida de la dirección IP de cada usuario, de los sitios web que visitó con anterioridad, de las cookies que tiene almacenadas o de algún otro criterio. Por consiguiente, es posible que dos personas que hubiesen navegado simultáneamente el mismo URL vieran contenido diferente.

# Viendo la fuente HTML de una página web.

La fuente HTML de una página web es el texto que define el contenido y el formato de la página. Además de la representación gráfica que se define para el observador, la página puede contener información adicional relacionada con su autor, códigos de programación,

Metadatos6 y otra información de identificación que puede no mostrarse al ver la página web. Los browsers o navegadores más comunes permiten a los usuarios ver la fuente de la página web. La figura 10 muestra el pantallazo del sitio web [www.urosario.edu.co,](http://www.urosario.edu.co/) seguido por la información de la fuente de HTML. Para ver la fuente de HTML usando Internet Explorer®, seleccione “vista” en la barra de herramientas y luego en el menú desplegable seleccione “fuente”.

Nota: Existen formas para ocultar la fuente HTML incluso mientras se permite ver una página web normalmente, en un navegador.

# Capturando información de una página web.

Dependiendo de la naturaleza y alcance de lo que se quiera probar con el documento, puede llegar a ser útil capturar información de una simple página web o de un sitio web. Las técnicas para obtener esta información incluyen: capturar un pantallazo empleando el comando “guardar como”, utilizar herramientas para descargar sitios web o localizar y confiscar el servidor web.

# Capturar un pantallazo.

Existen varias formas para capturar el pantallazo de una página web. Un método es la función de Windows® [Ctrl]+[PrntScrn], la cual capturará la pantalla completa y la copiará al *portapapeles (clipboard)* de Windows®*.* Luego, la imagen podrá pegarse (usando [Ctrl]+[v] or Edición > Pegar) en cualquier otra aplicación como un procesador de palabras

1. En este contexto metadatos corresponde a la información que describe los atributos o las palabras clave de búsqueda que han sido incluidas en el código fuente de la página web.

o un editor de gráficos y guardarla para conservarla. Otro método es usar una aplicación de software de un tercero especialmente diseñada para capturar imágenes de pantallazos o de ventanas activas. Estos métodos pueden capturar únicamente el contenido desplegado de la ventana activa y no el contenido que está por fuera de ésta. No se capturará la fuente de HTML a menos que ésta se haya desplegado también.

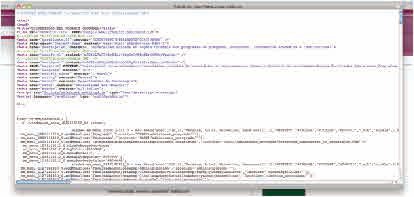
# Comando “guardar como” .

Legalmente hablando, un método sencillo y correcto de capturar la información de una página web que incluya la fuente de HTML y los archivos incrustados, es empleando el comando “guardar como” del navegador. Este comando guardará la página web en una ubicación específica del computador que esté utilizando quien recaude la prueba. En la figura 10 se muestra el comando “guardar como” a la izquierda y el destino de la captura de la página a la derecha. Observe que dependiendo de la versión del navegador usado hay varias opciones de comando “guardar como” para capturar la página completa y todos los archivos incluidos. En la figura 10, la opción de “guardar como” producirá una copia de todo el sitio web con sus archivos incluidos que se guardarán en una carpeta ubicada en el mismo directorio. Una buena práctica es verificar y evaluar la información que se captura usando opciones diferentes de “guardar como” antes de emplear esta.

Figura 8. Captura de pantallazo y de la fuente HTML del sitio web de la Universidad del Rosario.



Figura No. 9.



Advertencia. Una vez se complete la captura, debería verificarse inmediatamente para garantizar que se ha guardado toda la información que se estaba buscando.

Figura 10. Comando “Guardar como” y captura de la página Web



# Herramientas para capturar sitios web.

Una forma de capturar un grupo de páginas dentro de un sitio web es usando aplicaciones de terceros, navegar y grabar manualmente cada página de un sitio web muy grande puede consumir mucho tiempo. En el comercio encontrará un gran número de herramientas, incluso gratuitas, para capturar sitios web. En general, estos programas están diseñados para navegar cada link de una página y capturar todo el contenido, incluyendo los archivos incrustados y el código fuente de esos links/vínculos.

Es importante que tenga en cuenta que el contenido del sitio web observado pueda cambiar desde que se inició la investigación hasta la actualidad. En consecuencia, deberá documentarse la fecha y hora de las capturas que se realicen. Podrá ser posible determinar

el contenido previo de un sitio web empleando sitios de archivo web (Ej. la herramienta de búsqueda *Wayback Machine,* en http://www.archive.org) o en sitios similares.

Nota: Puede no ser posible capturar todo el contenido de interés específico de los sitios web escritos con lenguajes script con las herramientas de captura de sitios web; se deben usar herramientas forenses profesionales.

# Embalaje y presentación de páginas de Internet.

Al respecto he de aclarar que las páginas de Internet siempre ocupan un lugar físico en un servidor, así, si Usted sabe cuál es el ISP podrá además de presentar la prueba como explicaremos, solicitar al Juez que por oficios ordene al Proveedor, la remita tanto en soporte lógico como impreso, especificando la fecha y hora en que la página estaba disponible.

La ley 527 de 1999 es clara en que este tipo de mensajes de datos deberán garantizar:

# • Legitimidad.

La prueba debe ser capaz de ser usada y admitida por el Juez en un procedimiento judicial, por lo tanto, es imprescindible la utilización de los procedimientos y tecnologías necesarias para una correcta extracción y presentación de las pruebas.

No tener en cuenta este requisito no sólo puede suponer un problema económico, sino también legal.

Así se deberá guardar en el formato original de la página, siendo el más común como ya se explicó el HTML. (ver guardar como)

# • Autenticidad.

Es necesario establecer una relación directa entre la prueba y los hechos a demostrar; de no ser así, ésta no podrá ser utilizada en el procedimiento judicial.

Por eso es importante describir el procedimiento adelantado y colocar toda la información técnica de nombres de dominios, tiempo y lugar de acceso, quién y cómo realiza la recolección de la prueba.

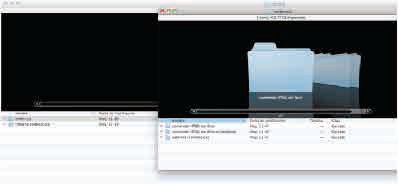
# • Integridad.

Debido a la gran volatilidad de las Pruebas Electrónicas y con el objetivo de salvaguardar la admisibilidad de éstas en el proceso judicial, durante todo el proceso de adquisición y análisis se garantizará que se preservará la integridad de los medios de almacenamiento originales, sin alterar ni un solo bit del medio tecnológico y aportará los mecanismos de seguridad necesarios para demostrar su integridad, esto se logra colocando una estampa cronológica de fecha y hora puesta por una entidad Certificadora Colombiana o un sistema de HASH confiable.

Para la presentación es recomendable un informe donde se especifique, quien y cómo realizó la toma de la prueba, que herramientas técnicas uso y las impresiones de pantalla tomadas como se describe en este capitulo, para que el Juez tenga a la mano una representación gráfica del documento.

El disco deberá verse así:

Figura No. 11.



# PRUEBAS RELACIONADAS CON LOS SERVICIOS DE MENSAJERÍA INSTANTÁNEA Y SALAS DE CHAT.

La mensajería instantánea (IM siglas en ingles) es cada día más común, al punto que programas como MSN, SKYPE, AOL o YAHOO MESSENGER, que fueron creados como una herramienta para que los adolescentes “chatearan” hoy se convirtió en una interesante aplicación de negocios, útil por demás, si se tiene en cuenta que se integran video, voz, datos, IM y en algunos casos servicios de telefonía Ip (Voip). Lo anterior, sin contar con la característica de la inmediatez, pues las personas saben si sus clientes o proveedores están conectados a la red de manera confiable, permitiendo sostener conversaciones en tiempo real. Se estima que en el mundo mas de 75 millones de personas usan estas aplicaciones para negocios.

Trasciende preguntar si de conformidad con la legislación vigente es obligación de los comerciantes llevar un registro de estas comunicaciones, en tal sentido hemos de aplicar articulo 19 del Código de Comercio que evidentemente incluye la obligación de conservar

la “*correspondencia y demás documentos relacionados con los negocios o actividades del comerciante”* concluyendo que los mensajes generados en el comercio utilizando IM deben ser considerados correspondencia7 legalmente hablando, en tal sentido si un empresario utiliza tecnología IM para contactarse internamente o con sus clientes o proveedores, al igual que el correo electrónico tradicional, él esta obligado a cumplir la obligación de guarda, lo que hace necesario que el mercante invierta en una solución administrativa basada en herramientas de software, integrando funciones de archivo, monitoreo y bloqueo, comúnmente conocidos como servicios de Gateway, lo que facilitará el trabajo de recaudo y presentación como mensajes de datos ante los jueces.

En ese orden de ideas, se explicarán las herramienta para la recolección, presentación y preservación de este tipo de mensajes de datos como documentos en un proceso judicial y las pruebas periciales que puedan realizarse siempre que estén relacionadas con el uso de programas de mensajería instantánea (IM) o salas de chat.

Los IM y las salas de chat permiten a los usuarios comunicarse con otros en tiempo real. Estas formas de comunicación ya no son exclusivas de los computadores de escritorio y pueden encontrarse en muchos equipos portátiles como teléfonos celulares, Blackberry (pin to pin) agendas digitales (PDA), buscapersonas y otros equipos de comunicación. En este capítulo el término “computador” se referirá colectivamente a todos estos equipos. Los programas de mensajería en línea, las salas de chat, por lo general, también permiten voz, video e intercambio de archivos. El material de voz y video puede ser de contenido

1. Tomado del Diccionario de la Real Academia de la Lengua 2009. ***correspondencia. 1.*** *f. Acción y efecto de corresponder o corresponderse.* ***2.*** *f. Trato que tienen entre sí los comerciantes sobre sus negocios.”.*

pregrabado o puede transmitirse en vivo. La mayoría de las salas de chat cuentan con múltiples participantes, mientras que los programas de mensajería instantánea permiten a los usuarios de computador comunicarse directamente uno a uno. Durante una sesión de chat, puede también estar disponible la funcionalidad de enviar y recibir mensajes privados.

# Servicios de mensajería instantánea.

Existen muchos programas y servicios para permitir a los usuarios comunicarse en tiempo real. Ellos realizan funciones similares, pero sus características varían así como la información que almacenan en los computadores. Algunos ejemplos incluyen:

* America Online (AOL®)
* AOL Instant Messenger™ (AIM)
* ICQ ®
* IRC ®
* MSN Messenger ®
* Net Meeting ®
* Trillian ®
* Yahoo!® Messenger
* Windows® Messenger
* Skype®
* Facebook ®
* Google Talk®

Antes de usar un servicio de mensajería instantánea o sala de chat, la mayoría de los servicios requieren que el usuario suministre o cree una cuenta de correo electrónico, algunas compañías como Yahoo!® y Hotmail® dan cuentas de correo gratis. En muchos casos la información suministrada por el suscriptor no se verifica y puede que no sea verídica, como resultado, los usuarios de estas cuentas pueden ocultar fácilmente su identidad e información personal.

# Cómo funcionan los servicios de Mensajería Instantánea (IM).

Un usuario debe crear o establecer primero una cuenta un nombre de usuario o alias. La información del usuario suministrada al momento de crear la cuenta puede ser falsa. Sin embargo, algunos servicios de mensajería registran la dirección IP que se encontraba en uso al momento de la creación de la cuenta. Esta información puede obtenerse de un proveedor de servicios de mensajería a través de un procedimiento legal apropiado, como sería una solicitud mediante orden de un Juez o Policía Judicial.

Una vez se ha creado la cuenta el usuario recibe un número de opciones disponibles para encontrar otros individuos con los cuales comunicarse en línea. Las personas pueden iniciar el contacto revelando sus nombres de usuario o pueden buscar a otros según las características descritas en sus perfiles de usuario.

Un usuario inicia una comunicación abriendo el programa de IM, seleccionando el nombre de usuario con el que se quiere comunicar, escribiendo el mensaje y haciendo clic en el botón “enviar”. Si el otro usuario está en línea el texto aparece casi instantáneamente, en una ventana en la pantalla del destinatario. Mientras la sesión esté activa, el texto completo

de la conversación aparece en ambas ventanas aunque puede llegar a ser necesario desplazarse arriba o abajo de la ventana con el fin de ver la totalidad del mensaje. La comunicación aparece como si los usuarios están conectados “punto a punto” (computador a computador) aun cuando tenga múltiples puntos de transmisión durante su recorrido.

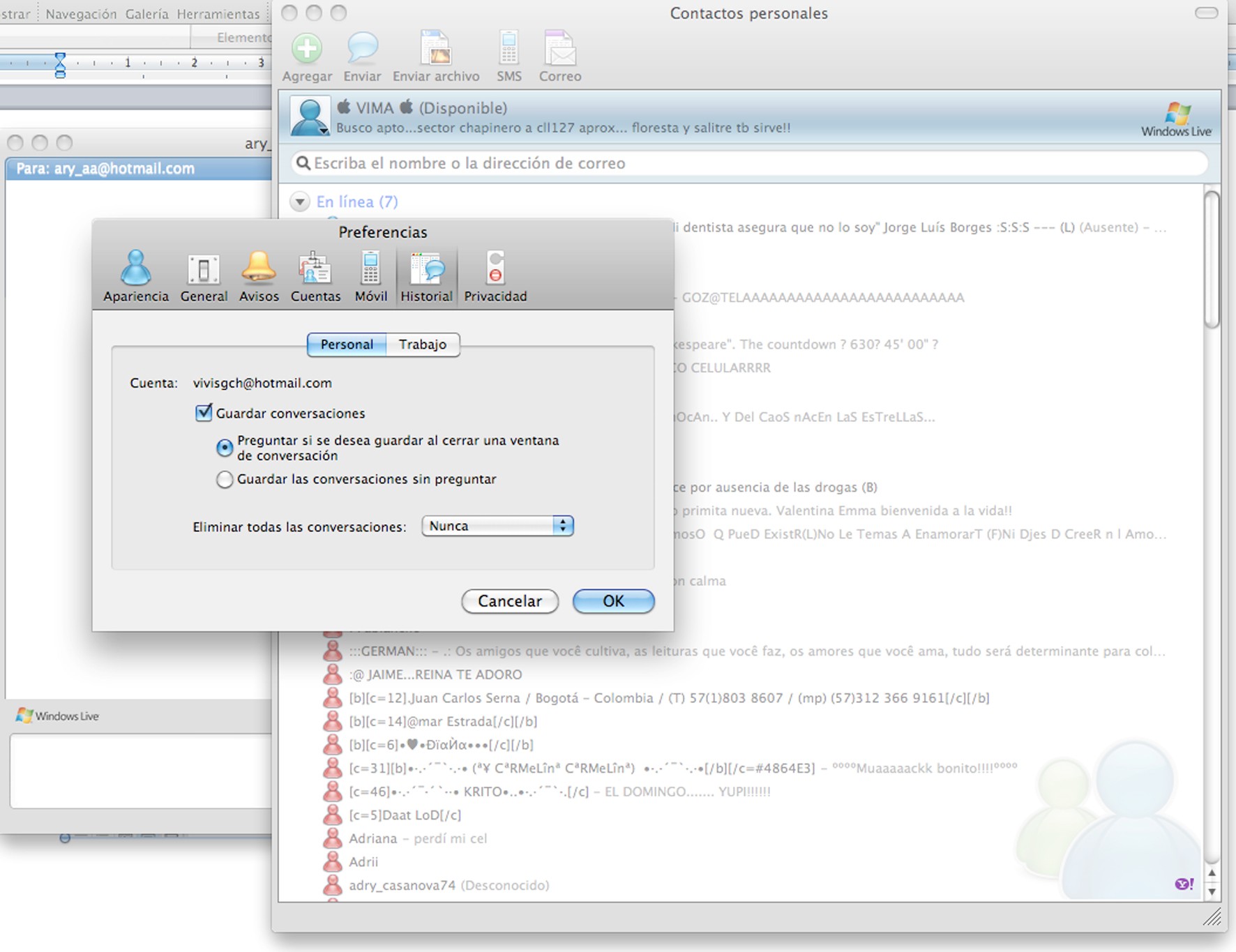
# Consideraciones para tomar la evidencia.

En cuanto a los procesos relacionados con los IM, podrá ser benéfico obtener la siguiente información de parte de quien está interesado en presentar la prueba.

* El computador usado para recibir la comunicación.
* El nombre de usuario.
* El propietario de la cuenta de ISP usada.
* El servicio de IM usado y la versión del software.
* El contenido (cuenta de contacto o actividad del testigo).
* La fecha y hora en que el mensaje fue recibido o visualizado.
* Las fechas y horas de los contactos anteriores.
* Cualquier registro o impresión de las comunicaciones guardadas.
* Las contraseñas respectivas.
* Testigos que pudiesen haber observado la comunicación.
* Si el software de seguridad que estaba en uso pudo haber capturado información adicional.

Los programas de mensajería tienen por regla general sistemas de guarda de los mensajes el él se tienen, para activarlo se puede ver la figura 12.

Figura No. 12.



Aunque algunos servicios de IM tienen la habilidad de registrar información en el disco duro del usuario, a menudo esta función no está habilitada. Es importante saber que una inspección forense del computador, como prueba pericial, puede en la mayoría de los casos reconstruir las conversaciones no guardadas o borradas.

No se espera que los proveedores de servicio (ISP) retengan información de la dirección IP. Por consiguiente, cuando un programa IM se vea envuelto en una investigación, el tiempo será crucial. Deberá enviarse un oficio de preservación al proveedor de servicios de mensajería instantánea con el fin de que éste mantenga la información mientras se ejecutan otros pasos legales adicionales; esto podrá hacerse como prueba anticipada.

# Salas de Chat.

Las salas de chat funcionan de forma similar a los servicios de IM en cuanto a que ambos permiten a los usuarios comunicarse en tiempo real. Sin embargo, la mensajería instantánea usualmente funciona uno a uno, mientras que en las salas de chat por lo general se trata de un grupo de conversación donde confluyen dos o más personas. Ciertos programas o ISP suministran listas de salas de chat basados en las áreas de interés o temas de discusión. Los usuarios podrán tener acceso irrestricto a estas salas de chat o éstas podrán tener restricciones de tamaño (número de participantes) o de contraseña.

Las sesiones de chat pueden ser monitoreadas y registradas por el proveedor del servicio, otorgando así un testigo potencial y un contenido documentado de las sesiones. No obstante, la retención de dichos registros varía dependiendo del proveedor del servicio por lo cual el tiempo es esencial. Deberá enviarse una carta de preservación al proveedor del servicio con el fin de mantener la información mientras se ejecutan otros pasos legales adicionales, esto se podrá hacer como prueba anticipada.

Puede ser que en las salas de chat no se reserve un nombre de usuario permanentemente para un individuo por lo cual no podrá confiarse en la identificación de una persona. Cada usuario en una sala de chat debe tener un nombre de usuario único para cada sesión, sin

embargo, cuando ese individuo se sale del sistema, el nombre de usuario que estaba utilizando puede quedar disponible para otro individuo. Aun más, varios individuos pueden emplear el mismo nombre de usuario al mismo tiempo si es que se encuentran en diferentes salas de chat. Solo porque vea que un nombre de usuario se está usando en una sala de chat en otro momento, ello no significa necesariamente que el mismo usuario lo estuviese usando en el mismo momento en que la demanda se recibió.

# Recolección, embalaje y presentación de chats.

Para embalar los chat, es muy importante no abrir los archivos donde se conserven las conversaciones, por que esto modifica el registro y el cambio de una palabra o fecha es muy probable, por ende antes de cualquier acción deberá asegurar los archivos con una estampa cronológica de fecha y hora o un sistema de Hash confiable.

Así luego de estar debidamente aseguradas las evidencias, es necesario que se guarde en el formato original, siendo recomendable además guardarlas en formato .rtf y .pdf .

Finalmente es recomendable hacer un informe donde se imprima quién tomo la evidencia, la forma en que la conservó para su presentación y el texto literal del chat.

# PRUEBAS PERICIALES EN INTERNET.

Las pruebas periciales que se practican sobre Internet, por lo general necesitan equipo y personal altamente calificado, razón por la que no cualquier ingeniero podrá realizar estas experticias, se necesitará que además cuente con un laboratorio de evidencias digitales y con equipo forense especializado que puede recaudar, embalar y presentar estas pruebas en

juicios, aunado a lo cual también podrá adelantar investigaciones sobre equipos de cómputo, teléfonos móviles, entre otros.

En cuanto a las calidades de los expertos, creemos que de conformidad con los artículos 233 y siguientes del C.P.C, Art. 250 de la ley 600 de 2000, Art. 406 de la ley 906 de 2004, podrán ser designados por el Juez y/o propuestos por las partes peritos particulares, que sin necesidad de estar en la lista de auxiliares de la Justicia, tengan los equipos, software y experiencia legal y técnica para este fin, teniendo en cuenta que para lograr la experticia, en algunos casos será necesario que existan más de 2 peritos por la especialidad de los temas aún tratándose de un mismo objetivo.

Ahora bien el perito designado podrá ser técnico, ingeniero8 o estar certificado en manejo de evidencias digitales, en el mundo actualmente existen certificaciones en este tema incluso para Abogados.

Debemos aclarar que se pueden hacer experticias sobre equipos de cómputo, memorias, teléfonos móviles, archivos, paginas de Internet, chats, correos electrónicos y en general cualquier medio o archivo en formato digital; sin que esto garantice que se logre el objetivo planteado por el cuestionario, pues como se ha explicado estas pruebas son altamente volátiles.

8 Recuerde que en Colombia los ingenieros deben tener registro profesional, además su experiencia sólo se valida desde la fecha en que tienen la respetiva matricula (ley 842 de 2003).

# Traza de correos - rastreando un e-mail.

Como lo estudiamos en el capitulo correspondiente a los mensajes de datos Correos Electrónicos, vimos que el encabezado tiene toda la información referente a de dónde salió el mail y por dónde pasó entre otras, así cuando identifique el encabezado como se explica en el numeral 2.1.2. , en la línea Recibed from: está la dirección ip.

# Qué es una dirección ip?

Del mismo modo que una casa tiene una dirección, cada computador conectado a Internet también la tiene. Se le conoce como dirección IP (Internet Protocol, en inglés). Este capítulo explica cómo se asignan las direcciones IP y cómo rastrearla hasta la fuente.

Debemos diferenciarla de otros tipos de direcciones. Algunos ejemplos son las direcciones de correo electrónico y las direcciones de los sitios web (del tipo www, World Wibe Web, en inglés).

|  |  |
| --- | --- |
| **Tipo** | **Ejemplo** |
| Dirección de correo electrónico | [alguien@urosario.edu.co](mailto:alguien@urosario.edu.co) |
| Dirección del sitio web | [www.urosario.edu.co](http://www.urosario.edu.co/) |
| Dirección IP | 129.6.13.23 |

Todas pueden rastrearse con el fin de suministrar pistas en la traza de un e-mail.

# Lectura y/o análisis de logs.

Esta prueba pericial busca recaudar y analizar los sucesos de una red, un computador, un teléfono móvil y en general cualquier hecho de una máquina.

Los logs, son un registro de todo cuanto sucede en una maquina, es un conjunto de archivos, que registran los programas que se instalan, las unidades externas que se colocan, los usuarios que se conectan, los programas que se ejecutan, entre otros muchos sucesos.

Ésta información es muy importante por ejemplo en hurtos bancarios que utilizan la red, accesos no autorizados a sistemas informativos, hurto de información, entre otros casos que buscan información dentro de los sistemas operativos de las máquinas.

# Reconstrucción de lo navegado en Internet.

Con un equipo especializado se puede reconstruir bastante información de lo que los usuarios han navegado en Internet, esto se logra con equipo técnico que reconstruye las páginas visitadas en determinado tiempo en una máquina, aunque no hayan sido guardadas y hasta cuando se ha formateado el disco duro.

# Otras pericias informáticas.

Existen otros tipos de pericias informáticas, por ejemplo la historiografía de archivos, que determina quien modificó un determinado dato, la información que se cambió, adicionalmente quién y cuando lo hizo, también se puede determinar por ejemplo si una fotografía, grabación de video o audio fue modificada, quien lo hizo, cuando y qué cambio, todo esto teniendo claros los parámetros de cadena de custodia, usando los equipos

adecuados y claro con una base legal sólida para que la prueba no pueda ser tachada de falsa.