Análisis de los Documentos Oficiales sobre Obtención, Tratamiento y Preservación de la Evidencia Digital

Aportes para el Tratamiento del Correo Electrónico como Evidencia Digital

Esteban Rivetti, José Aráoz Fleming, Beatriz Parra de Gallo
IEstIIng – Facultad de Ingeniería
Universidad Católica de Salta
Salta, Argentina
erivetti83@gmail.com, josearaozf@gmail.com, bgallo@ucasal.edu.ar
Horacio Leone,
INGAR/ Facultad Regional Santa Fe
Universidad Tecnológica Nacional
Santa Fé, Argentina
hleone@santafe-conicet.gov.ar

Abstract

En este trabajo se aborda el análisis de los documentos emitidos por distintas autoridades respecto de procedimientos fijados para la obtención, presentación y tratamiento de la evidencia digital. Se observa que –si bien se definen desde el contexto procedimental del derecho- lo hacen con escaso rigor técnico en cuanto al procedimiento técnico-informático de tratamiento de los documentos digitales como evidencia. Por ello, se concluye con un aporte que podría considerarse en estas normas oficiales, en todo aquello que implique la obtención, presentación y tratamiento de los correos electrónicos como evidencia digital.

1. Introducción

La recolección, tratamiento, estudio de la evidencia digital y posterior realización de los informes periciales requieren un protocolo esquematizado que se perfila como uno de los elementos fundamentales en el ámbito judicial.

La información de estos dispositivos se debe conseguir de manera muy estructurada y donde quede de manifiesto que ha sido recogida y tratada de manera aséptica, es decir sin interferencias exteriores de ningún tipo. Es decir, haciendo que el estudio de la información sea, en todo momento, objetiva y eficaz, evitando la manipulación de estos datos.

"Los informes periciales deben de tener un perfil técnico y tecnológico, fundamentados en procesos forenses, de investigación legal y criminalística, apoyados con amplios conocimientos legales en derecho penal, civil y administrativo. Dada la complejidad de estos informes, se debe proceder de una manera esquemática y dirigida" [1].

Totalmente acertado y es, justamente, el análisis del estado de situación normativo y técnico de la cuestión lo que se pretende abordar en el presente trabajo; haciendo especial hincapié en lo que al correo electrónico como evidencia digital respecta.

La organización de este trabajo es la siguiente: la sección 2 describe las características del correo electrónico como evidencia digital. En el capítulo 3 se tratan diversos documentos producidos por instituciones jurídicas que sirven de marco para los procedimientos de obtención, tratamiento y preservación de la evidencia digital. El apartado 4 describe la propuesta de Procedimiento para la Obtención, Tratamiento y Preservación del correo electrónico como evidencia digital, enfatizando los aspectos procedimentales de la cadena de custodio. Finalmente, en la sección 5 se presentan las conclusiones y trabajos futuros.

2. El correo electrónico como evidencia digital

El Dr. Horacio Juan Azzolín (titular de la Unidad Fiscal Especializada en Ciber-delincuencia) somete a consideración de la Procuración General de la Nación el documento titulado "*Guía de obtención, preservación y tratamiento de evidencia digital*", que fuera aprobado por este organismo mediante Resolución Nº 756/2016 [2].

En este texto se define la evidencia digital como *"... el conjunto de datos e información, relevante para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico*", de modo que se puede considerar que el

correo electrónico es una subespecie de esta; compartiendo las características distintivas de la misma, tales como la volatilidad propia de los componentes digitales.

Pero, no es esta la única definición normativa existente en nuestro país de evidencia digital. Otra norma, de recientísima aprobación por parte del Ministerio de Seguridad de la Nación y orientada a las fuerzas policiales y de seguridad, el "*Protocolo General de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos*" [3], da una definición de evidencia digital como "*… la prueba fundamental en los ciber delitos. Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Dicha prueba se adquiere cuando se secuestra y asegura para su posterior examen. Normalmente las pruebas consisten en archivos digitales, de texto, video o imagen, que se localizan en ordenadores y todo tipo de dispositivos electrónicos*".

Este protocolo, aprobado por resolución del Ministerio de Seguridad Nº 234/2016 en el mes de Junio del corriente año 2016, ha contado con la adhesión de la mayoría de las provincias argentinas resultando a partir de dicha adhesión de aplicación obligatoria para las fuerzas policiales y de seguridad de las distintas Provincias.

Con la definición normativa a la vista, y teniendo presente la intención de la validez judicial de la evidencia digital, su tratamiento le permitirá constituirse en *prueba pertinente*, o en *prueba admisible*, de acuerdo a cual sea la terminología utilizada por la pertinente norma provincial aprobatoria.

Cualquiera sea el caso, para que se considere *evidencia útil*, el documento digital debe estar dotado de recaudos especiales en tareas tales como la recolección, la manipulación, la interpretación. En el caso del correo electrónico será fundamental observar todos estos recaudos y algunos adicionales tales como su inalterabilidad obviamente.

Gómez Aparicio [1] sostiene que una de las primeras definiciones minuciosas sobre el concepto de la Prueba Electrónica se encuentra ampliamente precisada en el Convenio de Budapest; se trata por tanto de pruebas que por su naturaleza y características propias poseen información y datos que se podrán estudiar como el clásico documento probatorio, pero con un formato electrónico.

Este carácter electrónico le confiere una facilidad de manipulación, reproducción, copia, almacenado, certificación, autentificación, que debemos estudiar y aprovechar. No obstante, esto conlleva también un número alto de dificultades perceptivas a la valoración de las pruebas por la administración de justicia en las partes públicas o privadas, que aseguren la autenticidad del hecho investigado.

Esta justamente será la causal por la cual cualquier estudio serio sobre la temática se debe encarar no solo desde una matriz puramente técnica sino también desde la normativa existente o por generar, desde el status quo jurídico de la cuestión.

Y es por eso que justamente la jurisprudencia, la opinión de los jueces, no ha sido del todo conteste en aceptar como prueba evidencias digitales o pruebas electrónicas que se apartaran de principios normativos fundamentales, tales como el derecho de defensa, el debido proceso, la intimidad, y tantos otros alegados a favor o en contra de la recepción de la prueba electrónica.

En una demanda incoada por un trabajador contra Coca Cola [4], el Juzgado de primera instancia hizo lugar a la demanda por despido del trabajador por el mal uso de las herramientas informáticas, entre ellas el correo electrónico. Este mal uso se probó mediante una auditoria externa encargada por la empresa demanda. La Cámara Nacional de Apelaciones del Trabajo cuestionó la prueba preconstituida entre otras cuestiones trascendentes por la falta de participación de la parte demandada del procedimiento de extracción de la prueba, para poder controlarlo, y por la falta de resguardo del medio de prueba pues la computadora auditada *"…había cambiado el día del análisis por parte del perito judicial, en tanto la misma había sido reinstalada y se encontraba operativa"*.

Sin ir al extremo de solicitar la presencia de la parte demandada en el procedimiento de obtención de la prueba, en los autos "Pardo Rubén Ricardo c/Fernández, Juan Carlos s/ medidas precautorias", se hizo lugar a diligencias preliminares en las cuales un perito informático constate la existencia de correos electrónicos en el disco rígido de una computadora de la demandada, in audita parte, pero con la designación del Defensor Oficial para que represente a la parte contra la cual se dispuso la medida. Como se observa, esta última disposición buscó garantizar el derecho de defensa de la otra parte y evitar el posterior planteo de nulidad de la prueba pericial a obtener.

En algún otro caso [5] y siguiendo un criterio que Agustín Bender considera el más adecuado, la justicia concedió una pericia y registro de los registros informáticos de la demandada como prueba anticipada en base al riesgo existente, por la naturaleza misma de los elementos documentales a ser examinados, de que su contenido sea adulterado o suprimido antes de arribarse a la etapa probatoria pero se rechazó su producción in audita parte, considerando que la petición no halló su causa en razones de urgencia sino en el riesgo existente. Es decir la justicia dispuso que el secuestro de los soportes donde están almacenados los documentos se efectúe como diligencia preliminar in audita parte para

evitar su adulteración pero consideró que, una vez asegurada su integridad, no existía razón para impedir a la contraparte participar de la pericia que sobre aquellos debía realizarse.

Otro de los fallos citados en el trabajo de Bender es el de autos "B., T.E. c/Q. C.N. s/Divorcio" en donde se dijo que las partes solo podrán invocar los correos electrónicos como prueba cuando sean obtenidos por medios lícitos.

Y es justamente por estos y otros muchísimos casos que la construcción normativa, que otorgue sustento a la tarea técnica, debe ocuparse por el irrestricto respecto de estos principios fundamentales, a que antes se hacía referencia.

3. Análisis del documento de la Procuración

El documento citado en [2] que fuera aprobado por la Procuración General de la Nación transciende por el hecho de ser la primera norma de este tipo de carácter nacional.

Este documento aborda, o trata de abordar, la forma en que se debe obtener, conservar y tratar la evidencia digital; como el mismo documento lo sostiene *"... para mejorar los niveles de eficiencia en materia de persecución penal, en tanto resulta ser un eje central de preocupación de la comunidad internacional para la investigación transfronteriza del delito."*

Se dice "trata de abordar" pues no es un compilado completo, es solo un comienzo –necesario, si, pero solo comienzo- del abordaje legal de la problemática. Como el mismo documento lo sostiene, *"... no pretende abarcar la totalidad de procedimientos a tener en cuenta, sino brindar recomendaciones utilizadas a nivel mundial para incautar, analizar y preservar evidencia digital que deben ser consideradas por los operadores judiciales."* Y se dice "necesario" pues, desde lo legal, cualquier abordaje de la problemática resulta sumamente novedoso, a la fecha; en donde las distintas partes involucradas, ya sean jueces, fiscales, peritos o abogados, se mueven en un tiempo de constante innovación tecnológica, la mayor parte de las veces desprovista del soporte legal correspondiente.

Desde este punto de vista, resulta sumamente dificultoso, tanto para los jueces como para los abogados (entendidos estos como auxiliares de la justicia), y demás operadores judiciales, encarar esta problemática realmente creciente y en continua evolución.

Si bien a esta altura, tanto las herramientas de comunicación instantánea como las utilizadas como redes de comunicación social, deben ser minuciosamente estudiadas en el marco de la norma, serán motivo de próxima acometida, centrándose el presente trabajo en el tema específico, el correo electrónico. Ubicados en el contexto acotado del correo electrónico, se abordarán los aportes que el documento en análisis puede realizar a la pericia de correos electrónicos, así como se intentará avanzar con aspectos técnicos que puedan fortalecer la propuesta de Azzolín.

3.1. Análisis de Documentos Similares

Un documento de similar espíritu al que se encuentra en análisis, y que ya se citara ut supra es el dictado en fecha reciente (junio del corriente año 2016) por el Ministerio de Seguridad de la Nación, durante la III Reunión del Consejo de Seguridad Interior, que se llevó a cabo en la localidad bonaerense de Pilar.

Allí se aprobó por primera vez en la historia del país un protocolo de actuación para las fuerzas de seguridad y policiales enfocado en la investigación, recolección de pruebas y resguardo de la cadena de custodia digital en materia de Ciber delitos.

Si bien el contenido es similar a la guía de Azzolín vale destacar que aquella está apuntada a los integrantes del ministerio público fiscal mientras que la antes citada Resolución 234 del ministerio de seguridad, es aplicable a las fuerzas de seguridad y policiales.

En lo que a éste análisis respecta, también trata generalidades que apuntan a los principios ordinarios de intervención y algunos específicos pero se queda en este primera etapa que se veía antes, de "preservar la encomienda"; no aportando mucho mas al análisis puntual del correo electrónico.

Se debe reconocer que agrega algo importante y, en algún punto cuestionable, cuando dicta la prescripción de que **"***... Si la misma consiste en correos electrónicos, se deben guardar los mismo o ser reenviado a una casilla oficial como archivo adjunto. La impresión en papel de los mismos impide rastrear el remitente original del material probatorio***".**

Esto es cuestionable, desde el punto de vista del presente análisis, pues puede ocurrir que desde la cuenta oficial se "*altere*" el correo (en el sentido técnico de la expresión), y aunque ello no ocurra, pone en duda la imposibilidad de alterar el documento digital.

Asimismo, el documento prescribe que **"***Si la prueba se encuentra almacenada en un dispositivo de telefonía celular, quien reciba la denuncia deberá tomar los recaudos necesarios para que un informático forense realice una copia forense del dispositivo móvil para su análisis y posterior estudio."*

Finalmente que, *"Es imprescindible que si el material probatorio se encuentra en páginas de internet, redes sociales, etc. se solicite inmediatamente a los responsable la preservación de la evidencia digital allí contenida hasta tanto se obtenga la orden judicial pertinente***".**

Importante en cuanto a "Extracción de la Prueba", el documento del acápite resalta que "*Una parte es extraída*

mediante procedimientos forenses de la propia terminal de la victima y de los elementos secuestrados. Otra es facilitada por los proveedores del servicio de Internet, quienes son depositarios de la mayoría de los datos de tráficos validados para la investigación. Para poder acceder a esta información se requiere una autorización judicial…." y que "*... No se debe trabajar con la prueba original sino con una copia forense del dispositivo*".

También se establece la obligatoriedad de aplicar el método HASH[1] para asegurar la inalterabilidad del documento digital.

Entre otro de los documentos que abordan la cuestión, también se encuentra el **"***Protocolo de Actuación para pericias informáticas***"**, aprobado por el Poder Judicial de la Provincia de Neuquén [6]. Trata sobre los mismos o similares puntos que los anteriores, sobre el contenido, sobre el cuidado de la encomienda, pero no avanza en cuanto al análisis y validación del correo electrónico en particular.

Otros documentos provinciales dictados en la Provincia de Salta [3] han adherido las resoluciones nacionales ya citadas pero tampoco han avanzado normativamente en este último análisis y validación del e-mail requeridos. Similar situación se registra en el resto de las Provincias argentinas.

4. Propuesta de un procedimiento para la obtención, tratamiento y preservación de un correo electrónico como evidencia digital

Efectuado el análisis del estado de situación técnico y normativo de la cuestión, se propone validar normativamente el procedimiento que a continuación se detalla, para el análisis del correo electrónico por parte de peritos de parte, peritos judiciales o de fuerzas policiales y de seguridad, incumbencia que deberá ser determinada en cada caso concreto y de acuerdo a las competencias que la normativa actual les asigna a los distintos actores para entender en la cuestión.

4.1. Identificación de la evidencia digital

Un correo electrónico puede ser almacenado en el equipo del cliente, o en un servidor, dependiendo el proveedor y el tipo de gestor de correo que se está utilizando.

Es importante resaltar que la investigación debe realizarse siempre sobre el correo original. Cualquier acción de reenvío del correo bajo análisis impacta en la cabecera del correo, agregando los datos de la transacción en el propio correo, y alterando con ello la base de análisis forense de este tipo de documento digital.

Se debe considerar además, que tanto el proveedor de Internet como el del correo electrónico, pueden ser consultados para rastrear un mensaje. Dado el volumen de trafico de mensajes que manejan los proveedores de Internet, no suelen almacenar los registros por mucho tiempo, por lo tanto, cuando se efectúa el seguimiento de un correo electrónico se debe consultar al proveedor lo más pronto posible. Desde el punto de vista legal, no existe obligatoriedad de guardar estos registros. Abordándolo desde el lado de la ciber-delincuencia, en análisis, sería fundamental generar una normativa que prescriba esta obligación para todos los proveedores del servicio de Internet, sin perder de vista el debido resguardo de derechos tales como el derecho a la intimidad de las personas. Normativa que se cree debe ir provista de la fuerte sanción de la violación o divulgación de esta información por parte de los proveedores, información que solo debe ser almacenada a los efectos de la solicitud judicial de las mismas.

Justamente, en aras de este resguardo de la privacidad y la confidencialidad, los Dres. Facundo Viel Temperley y Tomás M. Bidegain, citados por Agustín Bender [7], explican que "en nuestro derecho, la inviolabilidad de la "correspondencia epistolar" y de "los papeles privados" se encuentra reconocida expresamente en el artículo 18 de la Constitución Nacional; y tuvo claro reconocimiento jurisprudencial desde el fallo de la Corte Suprema "Dessy, Gustavo Gastón s. Habeas Corpus". Esta protección luego fue extendida a las comunicaciones telefónicas, para posteriormente ser ampliada a las comunicaciones electrónicas y, entre ellas, los correos electrónicos, lo cual ocurrió primero en sede penal, donde la analogía se encuentra prohibida, interpretación que solo se extendió al ámbito comercial mas de dos años después."

Bender [7] dice que para preservar la inviolabilidad de la correspondencia epistolar es importante que la búsqueda de información en la casilla de correo de la contraparte se realice con el contralor de la afectada y que se individualice con la mayor precisión posible los documentos que deben buscarse, evitando acceder a otros que no se encuentren directamente vinculados con el objeto de la litis. En autos "Royal Verding S.A. c/Cablevisión S.A. y otro s/ordinario" la justicia ha dicho que la pericia sobre los sistemas informáticos de la contraria debía realizarse con su participación, evitando que terceros observen mensajes ajenos al litigio y con control del órgano judicial, para respetar el derecho a la inviolabilidad de correspondencia reglado por la constitución.

[1] Una función hash es método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible.

4.2. Extracción y preservación del material informático

El primer documento en estudio (Guía de Azzolín) establece pautas generales para la recolección y preservación de la evidencia digital *"... al momento de analizar la escena del crimen*". Evidentemente acá encontramos un gran condicionante pues circunscribe el aporte al caso penal dejando de lado múltiples circunstancias que pueden requerir el análisis de la evidencia digital y no necesariamente se encontrarán en la escena del crimen (el mejor de los escenarios, adelanto). En futuros trabajos se abordará otros escenarios que no necesariamente se relacionan con lo penal y que tienen que ver con la necesidad de obtención y validación de pruebas en el ámbito civil, en el laboral, por citar solo dos ejemplos.

Se vuelve a la tarea actual, situados en la escena del crimen, en donde el documento plantea varios escenarios posibles y su correspondiente abordaje. Por citar solo algunos ejemplos se plantean casos que van desde lo mas simple (computadora apagada) hasta lo mas complejo (computadora encendida, en red, y en proceso de destrucción de evidencia).

Más allá de estas pautas generales que el documento aporta, se debe volver a centrar la búsqueda en lo específico del correo electrónico.

Obtenida la evidencia en las formas estipuladas, embalada, trasladada y resguardada la evidencia, lograda la "*encomienda*" comienza la segunda y no menos importante etapa que es el análisis del contenido, la evaluación del correo electrónico en si; etapa que necesariamente requiere de un mayor análisis, evaluación para la cual el documento en estudio no prevé mayores formalidades que las ya expuestas por lo cual se debe– hasta tanto alguna normativa lo establezca- hacer uso de las practicas usuales de la seguridad informática, todavía no normadas en el ámbito del análisis forense.

Para poder realizar el análisis forense del correo electrónico, es necesario obtener el *encabezado*. El conjunto de datos que permiten que un correo electrónico tenga validez como evidencia digital se encuentra en su encabezado. Allí figura la información relativa al emisor del correo, fecha de envío, camino de recorrido por los servidores intermedios hasta llegar a destino y los datos referidos al destinatario del correo electrónico.

Se debe garantizar la posibilidad de la otra parte del juicio de poder inspeccionar el procedimiento seguido para la obtención de la prueba. Esto se hace a través de un procedimiento adecuado de extracción y conservación, lo que se denomina "cadena de custodia". Lo ideal es contratar los servicios de un escribano para que dé fe del procedimiento seguido para su extracción, además que el procedimiento sea realizado por un experto informático conocedor de la importancia y características que debe cumplir un archivo digital para que luego se presente como evidencia digital.

Además, para garantizar que la prueba no ha sido alterada desde su extracción y depósito hasta la entrega en el juzgado, se puede recurrir a herramientas de cifrado que proporcionan una función denominada HASH, de tal forma que a través de una cadena relativamente corta de caracteres, se puede comprobar que el fichero depositado es idéntico al aportado como prueba al juicio. Si se hubiese cambiado una coma por un espacio, la cadena de caracteres del HASH cambiaría.

En este punto, cabe destacar que la norma en estudio prevé que una vez finalizado el copiado forense, el agente debe realizar el cálculo hash de dicha copia, que tiene como funciones primordiales la autenticación (permite corroborar la identidad de un archivo) y la preservación de integridad de los datos (asegura que la información no haya sido alterada por personas no autorizadas u otro medio desconocido), resultando entonces de vital importancia a los fines de controlar la preservación de la cadena de custodia y evitar planteos de nulidad.

4.3. Obtención del encabezado de un correo electrónico

El encabezado figura en el archivo digital del correo electrónico como *metadato*, es decir, no está visible directamente sino que debe obtenerse mediante al acceso a las propiedades del archivo digital del correo, que cambian según sea el sistema de software utilizado para trabajar con el correo electrónico. Así, hay dos modos generales de obtener los datos de la cabecera del correo electrónico:

- Seleccione "Código Fuente, o Mostrar Original" por medio de opciones o preferencias en la barra de herramientas de la página Web de su proveedor de Correo Electrónico (YAHOO, GMAIL, HOTMAIL, etc.).

- Si se trata de un gestor de correo como ser Outlook o Thunderbird, se debe abrir el mensaje, seleccionar opciones y luego Encabezados de Internet o Fuente de mensaje, dependiendo de la versión que se trate.

La Figura 1 muestra un ejemplo del contenido de la cabecera de un correo electrónico:

```
Received: from mail-qk0-f178.google.com
([209.85.220.178]) by BAY004-MC3F30.hotmail.com over
TLS secured channel with Microsoft
SMTPSVC(7.5.7601.23143);
Sat, 22 Aug 2015 10:56:21 -0700
Received: by mail-qk0-f178.google.com with SMTP id
h123so41000494qkc.0 for<erivetti@hotmail.com>; Sat, 22
Aug 2015 10:56:21 -0700(PDT)DKIM-Signature: v=1; a=rsa-
sha256; c=relaxed/relaxed;d=gmail.com; s=20120113;
h=mime-version:reply-to:in-reply-
to:references:date:message-id:subject:from....[2]
```

[2] Se quitaron partes del correo que no son de interés para este trabajo.

```
MIME-Version: 1.0
X-Received: by 10.55.209.25 with SMTP id
s25mr33286802qki.84.1440266181090;
Sat, 22 Aug 2015 10:56:21 -0700 (PDT)
Received: by 10.55.12.11 with HTTP; Sat, 22 Aug 2015
10:56:21 -0700 (PDT)
Reply-To: beagallo@gmail.com
In-Reply-To: ...[2]
Subject: Re: va el archivo
From: "Ing. H. Beatriz P. de Gallo"
<beagallo@gmail.com>
To: Esteban Rivetti<erivetti@hotmail.com>
Content-Type: multipart/alternative;
boundary=001a1147a6161b2319051dea1a07
Return-Path: beagallo@gmail.com
X-OriginalArrivalTime: 22 Aug 2015 17:56:21.0439 (UTC)
FILETIME=[DA82CCF0:01D0DD03]
```

Figura 1: Vista de la Cabecera de un correo

Rivetti y Gallo [8] describen en detalle la definición y función de cada componente de la cabecera del correo electrónico. A los fines del presente trabajo consideremos solo aquellos aspectos que resulten de interés para el lector no avezado en informática:

- *From:* Contiene la dirección de correo electrónico del remitente y posiblemente el nombre real.
- *To***:** Ésta es la dirección de e-mail del destinatario. Si hay varias direcciones se separan por comas
- *Date***:** indica la fecha y hora en que se envió el mensaje.
- *Return-Path***:** es la dirección desde donde se envió el correo electrónico.
- *Reply-To***: e**specífica la dirección a la que el remitente desea que el destinatario le conteste. Este campo es opcional.
- *Message-ID***:** es una cadena de identificación generada por el transporte de correo en el sistema remitente. Es única para cada mensaje.
- *Recieved:* Es el campo más interesante para observar los pasos que sigue el mensaje desde su origen hacia su destino. Cada servidor en donde se deposita el mensaje agrega un nuevo encabezado *Received* que permite efectuar el rastreo o seguimiento de la ruta del mensaje.

Para seguir el rastro de los mensajes de correos electrónicos se deben analizar los encabezados del mensaje. Las funciones que cumple el encabezado son las siguientes [9]:

- Indican a los servidores de correo donde entrega el mensaje.
- Indican a las aplicaciones lectoras de correo electrónico como procesar el contenido de los mensajes de correo.
- Ofrece un registro de la ruta seguida por el mensaje desde su origen a su destino.

Es importante destacar algunas características del encabezado de los mensajes electrónicos:

- Generalmente todos los campos del encabezado necesarios son generados por la interfaz de correo.
- Algunos son opcionales y pueden ser añadidos por el usuario.
- Otros campos son añadidos por el software de transporte de correo.
- Por ejemplo, se puede ver que cada mensaje esta precedido por una linea From (nota: sin dos puntos). Ésta no es una cabecera RFC-822[3] , ha sido insertada por el software de correo para facilitar la lectura a los programas que usen ese archivo.

Al realizar el análisis del encabezado del mensaje debe tenerse presente que:

- El orden de lectura se realiza de abajo hacia arriba, i.e., la primera dirección IP[4] que se encuentra señala la dirección del último servidor visitado.
- La cadena de caracteres que aparece delante de los () puede ser falsificada.
- Los encabezados Recibidos brindan información para determinar la ruta del mensaje.
- El identificador del Mensaje –Message ID-, es asignado por el cliente de correo que creó el mensaje. Este identificador permite buscar un determinado mensaje entre los registros de uno o varios servidores.
- Si el campo X-Originating-IP existe, tiene mayor relevancia que el campo recibido, ya que este nos permite conocer quién es el proveedor o sea el ISP del emisor del correo.

4.3.1. Herramientas Forenses

Existen muchas y diversas herramientas disponibles para analizar un correo electrónico que fueron analizadas por Gallo, Vegetti y Leone [10]. A los allí citados se agrega el trabajo de Devendran, Shahriar y Clincy [11] acerca de un estudio comparativo de varios software open source para el análisis de correos electrónicos.

La elección de la técnica y herramientas más adecuadas se deduce de la estrategia de investigación que siga el perito, la cual dependerá de ciertos factores: dispositivo a analizar (PC, celular, servidor, etc.); cliente de correo (residente en el dispositivo o web mail); cantidad de correos (se debe analizar toda la cuenta o solo un correo determinado) y facilidad de acceso a la prueba (acceso al email enviado y al recibido, solo a uno de ellos, al servidor de correo, etc.)

Si bien las técnicas y herramientas mencionadas constituyen el marco formal y científico que califican la profesionalidad y rigor metodológico que se requiere en un análisis forense, los resultados que se obtienen no siempre cumplen su cometido: brindar información

[3] RFC-822: Formato estándar Internet para cabeceras de mensajes de correo electrónico

[4] Protocolo de Internet, es un número único que identifica un dispositivo en una red

fundada sobre los puntos en litigio, o mejor dicho, responder los puntos de pericia de manera clara y contundente.

Para realizar el análisis del encabezado de un correo electrónico es necesario utilizar herramientas forenses las cuales nos proporcionan información que extrae del encabezado y nos brinda la posibilidad de generar distintos tipos de reportes que pueden integrarse el informe parcial. Sin agotarse, el siguiente listado enumera las herramientas forenses más usuales para el análisis de correos electrónicos:

- Forensics Tool Kit
- Mail Navigator
- MailXaminer
- Add4Mail
- Encase
- Digital Forensic Framework
- eMailTrackerPro

4.4. Procedimiento para la obtención del correo electrónico como evidencia digital

En este apartado se formulan los pasos a seguir durante el procedimiento de obtención de un correo electrónico, resguardando todos los requerimientos señalados en el apartado anterior, a fin de que ese documento digital tenga validez como evidencia en una litis:

1. Identificar la cuenta de correo a analizar, y determinar el proveedor de correo, por ejemplo Hotmail, gmail, yahoo, etc. o puede tratarse de una cuenta corporativa de una determinada empresa.
2. Identificar el dispositivo (PC, Celular, Tablet, servidor de correo, etc) en el cual reside el correo electrónico aportado como prueba.
3. Identificar si el correo en análisis corresponde a un correo Emitido por el usuario o a un correo Recibido por el usuario. Si es un correo emitido, el encabezado solo dará certeza de que el correo salió de la cuenta de correo en análisis, mientras que si se trata de un correo recibido, el encabezado nos permite trabajar con la trazabilidad del correo hasta su origen.
4. Indicar al juez la necesidad de acceder a la cuenta y/o al dispositivo en el cual se encuentra residente el correo. Existen dos gestores de correo: las aplicaciones webmail (como Hotmail, gmail, etc) y los clientes de correo local que están en la PC del usuario como ser el MS Outlook o Thunderbird entre otros. Al webmail se accede desde cualquier maquina, no es necesario hacerlo desde el dispositivo del usuario, pero siempre es preferible hacerlo desde el propio dispositivo del aportante del correo. En cambio, si se utilizó un cliente de correo local solo se puede acceder al correo electrónico que se pretende analizar, desde la maquina o dispositivo del aportante.
5. Una vez identificado el correo electrónico se debe extraer el encabezado completo, accediendo a la misma a través de los metadatos señalados.
6. Se debe realizar una copia forense de la evidencia con su correspondiente valor hash.
   Accediendo a esta copia forense, se debe utilizar la herramienta forense adecuada para analizar el encabezado.
   Un asunto práctica que usualmente resulta difícil de resolver es decidir *en cual equipo se realizará el análisis forense*, si el perito cuenta con un laboratorio forense, seguramente tendrá el área aséptica para evitar la contaminación de la prueba. En otros casos, el juzgado aporta el equipamiento, con lo cual el perito debe asegurarse de descontaminar los componentes de hardware de cualquier resto de otros documentos digitales.
7. Verificar la existencia del campo X-Originating-IP, en caso afirmativo analizarlo.
8. Analizar el primer encabezado Received (desde abajo hacia arriba)
9. Identificar los datos de la dirección IP encontradas en el paso anterior.
   Con la información del encabezado técnico podemos verificar el origen del mensaje enviado, buscando con el número IP registrado el dominio de donde se originó el mensaje.
   Para ello se puede utilizar una interfaz de identificación de direcciones IP, que ayudan a identificar el servicio utilizado, ubicar la dirección geográfica de los servidores y los puntos de contacto, y localizar (a veces) la instalación donde se encuentra un computador.
   Existen varias páginas web que ofrecen el servicio gratuito de identificación de una IP, entre ellas:
   - http://network-tools.com/
   - http://whois.domaintools.com
   - https://www.whatismyip.com
   - https://www.whois.net/

   Estas páginas web brindan información de la dirección IP, propietario del registro en ARIN[5] - LACNIC[6] y DNS[7] reverso de la dirección IP del hostname (lookup) el nombre asociado con la dirección IP. Nombre del contacto del proveedor y responsable.
10. Realizar los pasos 8 y 9 con las sucesivas IP halladas en el encabezado.

[5] American Registry for Internet Numbers
[6] Latin American and Caribbean Internet Addresses Registry
[7] Sistema de Nombres de Dominios

11. Identificar el campo *Message ID*, este permitirá buscar coincidencias en el servidor de correo en caso que se requiera. Debe tenerse presente que para acceder a un servidor de correo, se deberá contar con la debida autorización judicial, en el marco de la causa en cuestión.
12. Todo el procedimiento debe ser efectuado en presencia de un escribano el cual validara las tareas realizadas.

4.5. Informe Pericial

El informe pericial es el documento redactado por el perito informático o forense actuante, en el que se exponen las conclusiones obtenidas por el experto, tras la investigación.

Cuando el análisis forense es solicitado por un juez, el informe debe cumplir con todo el rigor formal, de estilo y de escritura que dicta el derecho procesal en cuanto a las presentaciones escritas adosadas a un expediente judicial.

Cuando es solicitado fuera del contexto judicial, igualmente se sugiere mantener la formalidad y completitud señalada a continuación, aunque ajustando los datos de identificación y otros que no son de interés.

Este documento debe incluir:

- Nota de elevación del informe pericial, con inclusión completa de los datos de la causa (N° Expediente, Juzgado Actuante).
- Enunciación de los puntos de pericia ordenados por el juez.
- Declaración previa del perito informático, en la que se establecen los principios de profesionalidad, veracidad e independencia.
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación.
- Documentación (fotográfica o digital) sobre el proceso de adquisición de pruebas.
- Resultados de la investigación informática y conclusiones.
- El encabezado completo del correo electrónico debe ser entregado impreso como anexo al informe.
- Toda la documentación se debe entregar en formato digital en un cd o pen drive, según se determine.

Es de fundamental importancia evaluar la forma en que se va a entregar al Juzgado la evidencia digital obtenida, juntamente con el informe pericial ordenado.

Es importante que se utilice un lenguaje claro y llano tanto el contenido de los hallazgos digitales obtenidos como también un detalle exhaustivo de todas las tareas técnicas desarrolladas.

La cantidad de información técnica resultante del análisis de un correo electrónico debe insertarse en el conjunto de pruebas documentales de la causa judicial, colocándolo en un estadio de lectura que facilite la interpretación de esos datos técnicos por parte de los profesionales de la criminalística y el derecho.

Se requiere mucho más que la identificación de una dirección IP o la trazabilidad del correo electrónico.

Hoy en día se exige que estos datos se presenten ***sistemáticamente*** y ***semánticamente*** en el marco de la causa judicial, no como información técnica, sino como dato documental.

Además de los ítems que integran el informe pericial, se pueden adjuntar como anexo los reportes que generan las herramientas forenses utilizadas.

El informe pericial debe ser firmado por el perito actuante y las personas que intervinieron en la investigación.

4.6. Preservación de la Evidencia Digital

Piccirilli [12] enfatiza la importancia de la *preservación de la evidencia digital*, al considerar que la misma puede ser necesario volver a analizarse en una nueva investigación, ya sea cuando se amplían los puntos de pericia, o porque se requiere una confirmación de los datos obtenidos por parte de otro perito actuante.

Es fundamental que la evidencia digital se preserve de manera adecuada cumpliendo los siguientes pasos:

- *Resguardo lógico*:
  Se debe calcular el hash correspondiente y registrarlo en el informe pericial o acta de devolución de los elementos informáticos. Almacenar la evidencia en un pen drive, discos rígidos o similares, mayormente en dispositivos que no puedan alterarse fácilmente.
- *Resguardo Físico:*
  Este paso permite continuar con la preservación de la prueba desde el punto de vista físico. Ello, con el objetivo de desalentar otras posibles manipulaciones en los datos o para evitar la destrucción involuntaria de la prueba.

A partir de este punto, se deben utilizar los mecanismos de resguardo de pruebas existentes en el juzgado para la salvaguarda de pruebas materiales y documentales.

Para ello se recomienda:

1. Si son discos rígidos, pendrives o similares, es conveniente colocarlos en bolsas antiestáticas, y protegidos con espuma antiestática
2. Envolver todos los elementos en papel madera.
3. Generar una franja de contención (tipo secuestro), en la que se identifica:
   - La carátula de la causa (nombre y número de la misma)
   - El Tribunal interviniente (Juzgado – Secretaría, Fiscalía, Cámara, Corte, etc.)
   - Datos básicos del elemento protegido

- Fecha del procedimiento
- Firmas de los intervinientes (peritos, fuerza de seguridad)

4. Cubrir dicha franja con cinta de embalaje transparente (no utilizar cinta de embalaje color marrón)
5. Cerrar todas las partes del envoltorio con dicha cinta, de manera que no quede un espacio posible de abrir, sin ser sellado por la cinta de embalaje.
6. Completar el formulario de cadena de custodia, con los datos señalados en el punto 3.

Hasta aquí la enunciación de los componentes principales del análisis forense en correos electrónicos, con el objeto de considerarlos evidencia digital en un juicio.

5. Conclusiones

Existen varios aspectos normativos pendientes, referentes principalmente a la incorporación normativa, tanto de derecho de *fondo*: existen nuevos delitos que se valen de la tecnología y no están contemplados, o no se prevé con la suficiente dureza, como por ejemplo la omisión de información por parte de los responsables de las empresas telefónicas ante el pedido judicial.

Desde el derecho de *forma* se observa que no existen protocolos normativamente validados para el tema en estudio, el correo electrónico en particular, ni para tantos otros temas que son objeto de nuestra diaria atención (mensajería instantánea, redes sociales, etc).

Es válido aclarar que este procedimiento debe validarse a través de experiencias concretas, y que solo se ha planteado para el caso particular del análisis forense de un único correo.

Si bien la estructura podría mantenerse, seguramente hay aspectos a revisar cuando se debe analizar una cuenta de correo con cientos o miles de correos.

Este trabajo, a partir de un análisis técnico-legal de la cuestión, intenta ser un aporte a fin de lograr normar la actuación pericial en un tema puntual, el del correo electrónico como evidencia digital *normativamente validada y sin posibilidad de repudio* por la contraparte.

6. Referencias

[1] Gómez Aparicio, L.M. (2016). *Protocolo de actuación en peritaciones informáticas*, Escuela Politécnica Superior, Universidad Autónoma de Madrid. Puede ser consultado en la siguiente dirección web: https://repositorio.uam.es/xmlui/bitstream/handle/10486/671503/Gomez_Aparicio_LuisMiguel_pc.pdf?sequence=1

[2] Este documento puede ser consultado en la página oficial del Ministerio Público Fiscal (Procuración General de la Nación), puntualmente en el siguiente link https://www.mpf.gob.ar/biblioteca/protocolos-y-guias-para-la-investigacion-de-delitos/

[3] Tanto el protocolo como el convenio con la Provincia de Salta pueden ser consultados en la página oficial del Ministerio de Seguridad de la Nación: http://www.minseg.gob.ar

[4] "Lopez, Ricardo Luis c/Coca Cola Femsa de Buenos Aires S.A. s/despidos", publicado en ElDial.com en fecha 3/2016 y comentado por Agustín Bender. Se puede consultar texto completo de los fallos de 1era y 2da instancia en la página web http://e-legales.blogspot.com.ar Citar: DC2082

[5] "LUXURY WATERS LTDA C/NEW PATAGNIA S.A. S/DILIGENCIA PRELIMINAR", comentado pro Agustín Bender en su artículo "Validez Probatoria del correo electrónico en la jurisprudencia y en el Proyecto de Código Civil y Comercial de la Nación" y publicado en ElDial.com de fecha 10/04/2013. Se puede consultar en http://e-legales.blogspot.com.ar . Ref: DC1A33

[6] Puede ser consultado en la página web del Poder Judicial de la Provincia de Neuquén http://www.jusneuquen.gov.ar

[7] "Validez Probatoria del correo electrónico en la jurisprudencia y en el Proyecto de Código Civil y Comercial de la Nación" y publicado en ElDial.com de fecha 10/04/2013. Se puede consultar en http://e-legales.blogspot.com.ar . Ref: DC1A33

[8] Rivetti E., Gallo Beatriz P. de . (2016) *Verificación de la trazabilidad de un correo electrónico mediante un caso ejemplo*, Cuadernos de la Facultad de Ingenierìa, UCASAL (en proceso de publicación).

[9] Darahuge, M. E. (2011) *Manual de Informática Forense*. Editorial Errepar

[10] Gallo Beatriz P. de, Vegetti Marcela, Leone Horacio, "Ontología para el Análisis Forense de Correo Electrónico", CoNaIISI 2014 Actas del 2° Congreso Nacional de Ingeniería Informática/Sistemas de Información, San Luis, Argentina, ISSN: 2346-9927, 2014

[11] Devendran, Vamshee Krishna, Hossain Shahriar, and Victor Clincy. "A Comparative Study of Email Forensic Tools." Journal of Information Security6.2 (2015): 111.

[12] Piccirilli, D. (2016). *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia–forensia y cibercrimen)* (Doctoral dissertation, Facultad de Informática, UNLP, Argentina