ObE Forensics: Una herramienta para el Análisis Forense de Correos Electrónicos

Enzo Notario [1], Beatriz Parra de Gallo[1], Marcela Vegetti [2]

[1] *IEsIIng – Facultad de Ingeniería, Universidad Católica de Salta, Salta, Argentina,*

[2] *INGAR – Instituto de Desarrollo y Diseño (Conicet/UTN), Santa Fe, Santa Fe, Argentina*

Abstract

*El presente trabajo contiene la descripción de **ObE Forensic** (**O**ntology **b**ased **E**mail **Forensic**), una herramienta informática para el análisis forense de correos electrónicos, basada en una ontología. El objetivo de este trabajo es describir sus características técnicas y funcionales, el modo en que la misma se integra en el procedimiento pericial de correos electrónicos y las primeras instancias de validación realizada –por parte de usuarios expertos- sobre el prototipo de la aplicación.*

Palabras Clave

Ontología, Análisis Forense, Correos Electrónicos.

Introducción

En el presente trabajo se describe el proceso de desarrollo de ObE Forensic, una aplicación informática para el análisis forense de correos electrónicos, basada en una ontología. El objetivo de este trabajo es presentar la herramienta, sus características técnicas y funcionales, cómo se integra la misma en el procedimiento pericial de correos electrónicos y las primeras instancias de validación realizada sobre el prototipo de la aplicación.

Siendo que las tecnologías semánticas permiten generar un espacio de interacción entre todos los actores del proceso pericial (jueces, abogados, otros peritos, policías, etc.) se construyó primero OntoFoCE, una ontología que modeliza el proceso de trazabilidad del envío de un correo electrónico, definiendo los conceptos, relaciones y axiomas que representan a esta evidencia digital. Más detalles de esta ontología se pueden ver en [1], [2] y [3]. Una vez construida OntoFoCE, se avanzó en el desarrollo de una aplicación informática que permitiera el uso de OntoFoCE para realizar el análisis forense de correos electrónicos.

A la fecha, la aplicación construida está en fase de validación por parte de usuarios expertos, observándose que la propuesta ha sido bien recibida aun cuando son varias e interesantes las mejoras sugeridas.

Este trabajo cuenta con las siguientes secciones: en la Sección 1 se describe el correo electrónico como objeto de estudio, en la sección 2 se incluyen una descripción general del análisis forense digital; luego la sección 3 aborda el procedimiento de realización de pericias sobre correos electrónicos; la sección 4 describe algunas herramientas para el análisis forense de correos electrónicos, y en la sección 5 se presenta ObE Forensic con detalle de la arquitectura de procesamiento y la funcionalidad que mantiene la aplicación; la sección 6 en la que se describe las validaciones del prototipo realizada por usuarios expertos; la sección 7 contiene una breve descripción de la aplicación en cuanto a interfases y funcionalidades; y por último, en la sección 8 se describen las conclusiones y futuras líneas de investigación.

1. El Correo Electrónico

Se trata de un servicio de red que permite el envío y recepción de mensajes entre el grupo de usuarios. Su nombre proviene de la analogía con el correo postal, en donde también existen remitentes y destinatarios, que se transmiten mensajes empaquetados a través de una estructura de comunicación compleja conformada por múltiples centros de distribución vinculados entre sí. Un correo electrónico responde al mismo esquema que la correspondencia en papel en donde las oficinas de distribución de envíos son los servidores que van recibiendo el correo electrónico y lo redireccionan para que siga su camino, según los datos de remitente y destinatarios que figuran en el "encabezado" del correo, y en este último, se

van registrado los pasos por los distintos servidores de distribución. El correo electrónico mantiene la característica de confidencialidad e inviolabilidad del contenido de la correspondencia.
En el marco de este trabajo se define al mismo en función de los elementos necesarios para la realización del análisis forense, i.e., *un correo electrónico es un documento digital que consta de dos partes: a) una cabecera que contiene información sobre el proceso de transmisión que se desarrolla con identificación de las cuentas intervinientes y los distintos servidores en que el correo se fue almacenando durante la transmisión; y b) un cuerpo que contiene el mensaje que se transmite.*
Desde el punto de vista técnico, el correo electrónico se ajusta a la norma RFC 822[1] (y sus modificatorias) que contiene los estándares de formato para mensajes de texto. Esta norma señala cómo debe estructurarse la cabecera de un correo electrónico, y dispone la forma en que el servicio de envío agrega información sobre el servidor de mail en su cabecera. Básicamente, un correo electrónico es manejado por un mínimo de cuatro equipos distintos: el equipo emisor, el servidor de correo del remitente, el servidor de correo del receptor y el equipo receptor. En todos ellos, el proceso de transmisión *deja una huella* del correo emitido, que se encuentra en la *cabecera o encabezado del correo.* En base a la información agregada a la cabecera durante la transmisión, es posible establecer la ***trazabilidad*** del envío de un correo.
La norma ISO 9000:2015 [2] define trazabilidad como la "*capacidad para seguir el (desarrollo) histórico, la aplicación o la localización de un objeto; al tratarse de un producto o servicio, la trazabilidad puede estar relacionada con el origen de los materiales y las partes, el histórico del proceso y la distribución y localización del producto o servicio después de la entrega*". La principal ventaja que reporta la trazabilidad es poder conocer con certeza la procedencia de un producto. Así, mediante la misma se puede probar la existencia del correo electrónico recibido en una cuenta. La reconstrucción del camino de inverso del correo permite avalar el carácter probatorio de este documento digital y reforzando la capacidad de no repudio del mismo.

2. Análisis Forense Digital

Si bien son varios los autores que abordan la definición del proceso de análisis forense digital, conjugando cuestiones propias de la criminalística con protocolos y normas de la ingeniería, conviene considerar aportes de investigadores argentinos pues referencian el proceso pericial que se sigue en Argentina. En particular, se toma la propuesta del Grupo de Investigación sobre Forensia Digital de la Universidad FASTA[4], quienes incorporan componentes de la ingeniería de Software y proponen el Proceso Unificado de Recuperación de Información (PURI). Se selecciona esta metodología pues conjuga aspectos informáticos y criminalísticos que apuntan al objetivo que se persigue con ObE Forensic –cual es- desarrollar una herramienta que satisfaga las condiciones de "principios científicos y técnicos" requeridos por el derecho procesal argentino[3].
La ***Fase de Relevamiento*** abarca la investigación para conocer el caso e identificar los posibles objetos de interés, para considerar la documentación legal y técnica y la infraestructura de IT con que se va a trabajar. La ***Fase de Recolección*** abarca las acciones necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se deberá trabajar posteriormente. La ***Fase de Adquisición*** abarca todas las actividades en las que se obtiene la imagen forense[4] del contenido

[1] RFC (*Request for Comments)* son una serie de publicaciones técnicas que describen diversos aspectos del funcionamiento de internet, fijando protocolos, estándares y procedimientos avalados por el IETF (Internet Engineering Task Force) que es una organización internacional abierta de normalización de de Internet.
[2] https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-4:v1:es
[3] Art. 477 del Código Procesal Civil y Comercial de la Nación (CPCyC), Ley Nacional 17454, 1967.
[4] Una ***imagen forense*** es una copia exacta, sector por

que se analizará. La ***Fase de Preparación*** incluye las tareas técnicas de preparación del ambiente de trabajo del informático forense, la restauración de las imágenes forenses y volcados de datos, su correspondiente validación, y la selección de las herramientas y técnicas apropiadas para la extracción y el análisis, de acuerdo al objeto origen, y a las necesidades del caso. La ***Fase de Extracción y Análisis*** comprende las tareas forenses de extracción de la información de las imágenes forenses, la selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales. Finalmente, la ***Fase de Presentación*** comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes.

Más adelante, se describe el escenario del procedimiento pericial en el cual interviene ObE Forensic, señalando las fases de PURI en las que se introduce esta aplicación como herramienta para el análisis forense.

Es importante destacar la necesidad de contar con una *metodología científica* para el desarrollo del análisis forense, toda vez que la justicia está demandando la participación de peritos informáticos en la obtención y tratamiento científico de evidencias digitales que se presentan como *prueba* de un hecho, dado que los rastros digitales son cada vez más numerosos en los procesos investigativos.

De igual modo, la justicia demanda a los peritos informáticos un entrenamiento en materia judicial y criminalística, en particular respecto de los principios de mantenimiento de la cadena de custodia, no contaminación de la prueba y el uso de criterios de actuación compatibles con el derecho procesal.

2.1. Los Puntos de Pericia

La legislación argentina establece los procedimientos a seguir para la obtención de evidencia digital. Estos procedimientos varían –en amplitud y profundidad- según se trate del ámbito del derecho que se aborda (Civil, Penal, Laboral, etc.).

Para [5] la pericia *es un medio probatorio con el cual se intenta obtener, para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útiles para el descubrimiento o la valoración de un elemento de prueba*. Su regulación se encuentra definida de manera general en los códigos procesales de forma meramente enunciativa. Se puede tomar la definición de prueba pericial de [6]: *La prueba pericial consiste en el informe brindado por una persona ajena al proceso, con especiales conocimientos técnicos, y/o científicos sobre la materia en litigio, que a través de un proceso deductivo (de lo general a lo particular), partiendo de sus conocimientos específicos, los aplica al caso concreto y elabora su opinión fundada con los elementos ciertos que surgen de la causa en análisis.*

De una pericia interesa particularmente el *objeto de la pericia* o *los puntos de pericia*, mediante los cuales el Juez define el alcance de la actividad pericial. Estos elementos usualmente se expresan en términos de acciones "*verificar… constatar… informar… explicar…"* en la cual el perito recurre al conocimiento científico de su disciplina, para responder a la solicitud del Juez, atendiendo a las normas y buenas prácticas de cada disciplina.

3. Procedimiento de Realización de una Pericia sobre Correos Electrónicos

El procedimiento de realización de la pericia incluye una serie de pasos a realizar para lograr resultados exitosos que se enuncian siguiendo la metodología PURI.

3.1. Fase de Relevamiento

El análisis pericial de correos electrónicos debe realizarse siempre en el correo *recibido*, ya que el correo emitido en sí mismo no garantiza que haya sido recibido por el destinatario. Es necesario acceder al cliente de correo en el que se encuentra éste y –de ser posible- al propio equipo en el cual se recibió el correo, pues la investigación

sector, bit a bit, de un medio de almacenamiento. De esta manera, es posible trabajar con la imagen de la misma manera que si se hiciera sobre el original.

debe realizarse sobre el correo original.
Se debe considerar además, que tanto el proveedor de Internet como el del correo electrónico, pueden ser consultados para rastrear un mensaje.
Atendiendo a la condición de *documentación epistolar* que se le asigna legalmente al correo electrónico, es importante salvaguardar la privacía del mismo. [7] dice que para preservar la inviolabilidad de la correspondencia epistolar es importante que la búsqueda de información en la casilla de correo 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 a la causa judicial.

3.2. Fase de Recolección

El procedimiento para extracción y preservación del material o documento digital a peritar, depende de varios escenarios, vinculados al área del derecho en el que se desarrolle la pericia. Si es el Fuero Penal, los procedimientos son sumamente rigurosos puesto que está en juego la detención y/o la vida de las personas. En el Fuero Comercial o Laboral es distinto, la pericia de la documentación digital de prueba consiste en certificar y validar la misma. Es en este último foro –el laboral- en donde mayormente se solicitan pericias de correos electrónicos, de modo que se abordará el procedimiento bajo el supuesto de la solicitud de pericia en dicho contexto.
Para poder realizar el análisis forense del correo electrónico, es necesario obtener la *cabecera* del correo electrónico. 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, denominado *cadena de custodia*. Lo ideal es contratar los servicios de un escribano (o contar con la presencia de un oficial de justicia) para que dé fe del procedimiento seguido para su extracción, además que la actividad sea realizada por un experto informático conocedor de la importancia y características que debe cumplir un archivo digital para que luego se presente como evidencia digital.
Por otra parte, para garantizar que la prueba no ha sido alterada desde su extracción y depósito hasta la entrega en el juzgado, se recurre a herramientas de cifrado que proporcionan una función *HASH*[5], de tal forma que, a través de la secuencia de caracteres resultante, se puede comprobar que el fichero extraído por el perito y el depositado en el juzgado son idénticos. Así, una vez finalizado el copiado forense, el perito debe aplicar la función hash de dicha copia y entregarla al juzgado para su resguardo.

3.3. Fase de Adquisición

Para seguir el rastro de los mensajes de correos electrónicos se deben analizar las cabeceras del mensaje. [8] indica cuales son las funciones que cumple el encabezado del correo electrónico:

- 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.

La cabecera del correo electrónico figura como metadato[6] en el archivo digital que lo

[5] Una ***función criptográfica hash*** es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una secuencia de caracteres única. Si se cambia un solo caracter del texto original, la secuencia resultante será diferente. Las funciones hash permiten identificar unívocamente a un conjunto de datos digitales, sea éste un documento, un video, etc.

[6] Los ***metadatos*** (metadata) son campos de texto incrustados en los archivos con información adicional sobre

contiene, 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 cliente de correo utilizado para la gestión del mismo.

3.4. Fase de Extracción y Análisis

Sobre la base de lo definido en [9] en este apartado se formulan los pasos a seguir durante el procedimiento de obtención de la cabecera 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 si el proveedor de la cuenta es un servicio de dominio gratuito o se trata de una cuenta corporativa con dominio propio. En este último caso, se abre la posibilidad de buscar una copia del correo en el servidor de correos corporativos de manera más fácil que en el caso de un servicio de dominio gratuito.

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. En el primer caso, 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 permite trabajar con la trazabilidad del.

4) Acceder a la cuenta en la cual se encuentra residente el correo, sea éste un cliente remoto o local. Aunque al cliente remoto se puede acceder desde cualquier computadora, siempre es preferible hacerlo desde el propio dispositivo del aportante del correo. En cambio, si se utilizó un cliente local solo se puede acceder al correo electrónico que se pretende analizar, desde la computadora o dispositivo del aportante. Es en este momento donde se obtiene la información auxiliar para el informe pericial: dirección física del equipo, cliente de correo utilizado para gestionar la cuenta y otra información relevante para el informe pericial (datos del usuario, lugar donde se realiza la pericia, personas presentes en el acto, entre otras). Se debe destacar que, para no acceder a correos no vinculados a lo indicado por el juez en los puntos de pericia e incurrir en el delito de acceso no autorizado a datos privados, el perito debe acceder a la cuenta cuidando de identificar y separar solo los correos pertinentes.

5) Una vez identificado el correo se debe extraer la cabecera completa, accediendo a la misma a través de los metadatos

5.1 Cuando la evidencia digital es un único correo, el perito accede a la opción de menú del cliente de correo en el que se muestre la cabecera del correo electrónico, y de allí toma el archivo digital en texto plano requerido.

5.2 Cuando la evidencia digital es un conjunto de correos, el perito debe acceder a la opción de menú del cliente de correo que le permita exportar el conjunto de correos. Si la exportación genera como resultado un archivo con formato de texto plano (.eml, .txt u otro similar) no será necesario ninguna otra acción más que la de resguardar el archivo mediante la encriptación con una función hash. Pero si el cliente de correo no cuenta con la opción de exportar el conjunto de correos como texto plano, se debe buscar un cliente de correo que permita la conversión adecuada. En este sentido, la aplicación *Thunderbird* [7] , cuenta con herramientas que permite importar/exportar archivos de correos en los formatos más habituales, De este modo, el perito realiza este paso intermedio y obtiene el archivo digital en formato de texto plano.

6) Se debe realizar una copia forense de la evidencia con su correspondiente valor hash.

7) Accediendo a esta copia forense, se

el mismo (fecha de creación, resolución, tamaño, fecha de modificación, autor, etc.). Usualmente no están visibles a simple vista.

[7] https://www.thunderbird.net

debe utilizar la herramienta forense adecuada para analizar el encabezado.

8) Una vez accedido al encabezado el análisis comprende las siguientes verificaciones:

8.1 Verificar la existencia del campo X-Originating-IP, en caso afirmativo analizarlo.

8.2 Analizar el primer encabezado Received (desde abajo hacia arriba)

8.3 Identificar los datos de la dirección IP encontradas en el paso anterior.

8.4 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 geolocalizar (cuando es posible) la instalación donde se encuentra un computador[8].

9) Realizar el paso 8 con las sucesivas IP halladas en el encabezado.

10) Con la información obtenida elaborar el INFORME DE PERICIA, de acuerdo a las normas de estilo de presentación de documentos judiciales.

Obsérvese que el procedimiento es sencillo cuando se debe peritar un único correo electrónico, pero no lo es cuando se trata de múltiples correos. Principalmente porque al tratarse de un solo correo, el análisis del encabezado puede realizarse manualmente y si el perito es ordenado en su tarea, es probable que no incurra en errores u omisiones producto de realizar una tarea rigurosa un número importante de veces.

Necesariamente el perito debe recurrir a alguna herramienta que automatice la tarea de analizar los correos cuando la cantidad lo amerita en pos de ganar tiempo y realizar una tarea eficiente y sin errores técnicos.

4. Herramientas para el análisis forense de Correos Electrónicos

La Forensia Digital ha entrado en una crisis producto del impacto de dos elementos que marcan la época actual de la tecnología informática: la masividad de los datos y la multiplicidad de plataformas tecnológicas. [10] presenta varios desafíos, involucrando no solo los modelos de "visibilidad y búsqueda" que proponen las herramientas forenses de uso actual sino también la falta de integración de las estrategias (como la ingeniería reversa) con dichas herramientas para reducir tiempos y costos. Cita este autor como próximos desafíos a resolver:

- Diseño de las herramientas orientadas a la evidencia: usualmente las herramientas actuales se orientan a la búsqueda de elementos digitales (evidencia) pero no a la presentación, resumen o análisis de correlaciones entre los datos encontrados.
- Modelo de visibilidad, filtro e informe: las herramientas utilizan interfaces de comunicación con el experto forense que habitualmente no permiten establecer vínculos o relaciones de prioridad entre los datos encontrados. Incluso algunas herramientas se basan en algoritmos computacionales costosos en tiempo y pueden faltarle características de usabilidad para el usuario final. La automatización o generación de scripts para búsqueda y filtro no siempre resultan. Y se complica aún más ante el avance continuo de las tecnologías (procesamiento paralelo, deep web, etc.).
- Problemas estructurales en las herramientas forenses: en muchos casos se recurre a software desarrollado para el contexto de negocios o para sistemas transaccionales y no responden exactamente a las necesidades puntuales de la búsqueda de evidencia digital. Ocurre lo mismo con tecnologías integradas, tales como las

[8] 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 (American Registry for Internet Numbers). LACNIC (Latin American and Caribbean Internet Addresses Registry y DNS(Sistema de Nombres de Dominios), reverso de la dirección IP del hostname (lookup), nombre asociado con la dirección IP, Nombre del contacto del proveedor y Nombre del Responsable de tramitar el dominio.

aplicaciones monolíticas.

- Abstracción y modularización: debido al volumen de datos que se procesan en la búsqueda de la evidencia digital, se requieren estándares para la identificación, transmisión e intercambio de los datos; también es importante generar arquitecturas de procesamiento que superen los conflictos del software abierto y propietario.
- Enfoque en la identidad del individuo: tomando como atributos todos aquellos datos que puedan generar una "imagen" de la persona (datos de identificación, datos bancarios, correos, vínculos de las redes sociales, etc.).

Existen muchas y diversas herramientas disponibles para analizar un correo electrónico que fueron analizadas en [11]. A los allí citados se agrega el trabajo de [12] 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.)

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:

Aid4Mail[9] soporta más de 40 formatos de correo electrónico y programas de cliente de correo, así como muchos servicios populares de correo web y cuentas remotas a través de IMAP. Las carpetas y archivos de correo local se pueden procesar fácilmente cuando se desconectan de su cliente de correo electrónico, incluidos los almacenados en discos duros externos y medios como DVD y dispositivos USB. *Aid4Mail* puede leer archivos mbox de sistemas Mac y Linux sin conversión previa.

EmailTrackerPro [10] no sólo ofrece la capacidad de rastrear un correo electrónico usando su encabezado, sino que también tiene un filtro de spam (edición avanzada), que escanea cada correo electrónico a medida que llega y advierte al usuario si se sospecha de spam La característica más valiosa de *EmailTrackerPro* es la capacidad de rastrear más de una dirección IP o nombre de dominio a la vez.

MailNavigator[11] fue creado a partir de dos herramientas para la lectura de email: FILTER, que es un poderoso sistema para la búsqueda de correos en ficheros de los distintos programas de e-mail; y NAVIGATOR, que es un lector de correos y noticias con funciones avanzadas.

OSForensics [12] permite extraer pruebas forenses de computadoras rápidamente con búsquedas e indexación de archivos de alto rendimiento. Puede identificar archivos sospechosos y actividad con coincidencia hash, comparaciones de firmas de unidad, correos electrónicos, memoria y datos binarios. También permite administrar una investigación digital y crear informes de datos forenses recopilados.

La empresa creadora de *E-mail Examiner*[13] ha sido una de las pioneras en soluciones para dispositivos móviles, teléfonos inteligentes y correo electrónico, y su enfoque de trabajo en la movilidad le permitió avanzar en muchas otras áreas de la innovación incluyendo la investigación y el desarrollo en el Internet de Cosas (IoT) con el *Forensics of Everything TM* (FoE). *E-mail Examiner* permite analizar los encabezados, los cuerpos y los archivos adjuntos de los correos electrónicos. Analiza

[9] http://www.aid4mail.com

[10] http://www.emailtrackerpro.com
[11] http://www.mailnavigator.com
[12] http://www.osforensics.com
[13] https://www.paraben.com

el mensaje de principio a fin, incluyendo la clasificación y análisis detallado de archivos adjuntos. Soporta los principales tipos de correo electrónico que se almacenan en equipos locales para análisis, generación de informes y exportación/conversión de datos. Systools Software, creador de *MailXaminer*[14], se dedica a proporcionar herramientas de alta tecnología con interfaz de usuario amigable. Ha contribuido con la recuperación de datos, soluciones de copia de seguridad, así como herramientas forenses de investigación y análisis de correo electrónico. El primer lanzamiento importante realizado en el campo de las aplicaciones de *eDiscovery* fue *MailXaminer*, es un conjunto completo de herramientas para la documentación, análisis, examen y notificación de evidencias de correo electrónico.

Incluso existen frameworks integrados para el análisis forense de correos electrónicos, tales como el *Integrated E-mail Análisis Forense Framework (IEFAF)*, propuesto por [13], que consta de 5 módulos basados en técnicas y herramientas de minería de datos. *EnCase Forensic* [15] es una poderosa plataforma de investigación que recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales, en el caso de correos electrónicos cuenta con una amplia compatibilidad con los distintos formatos de archivos de correos y permite obtener un archivo imagen del mismo con el objeto de preservar la prueba original libre de manipulación. Aquí también es distintiva la funcionalidad de la herramienta para el análisis forense de correos electrónicos, y los informes de resultados que muestran los datos desde varias ópticas, pero dejando a consideración del perito la selección de los resultados que le permitan responder a los puntos de pericia.

Para el caso particular de los dispositivos móviles que se encuentran en el mercado, se pueden usar las siguientes herramientas de análisis forense: *TULP2G*[16], y *MOBILedit FORENSIC*[17]. Incluso existen herramientas diseñadas específicamente para el análisis forense de determinada tecnología celular, tal como el *Elcomsoft Phone Breaker* [18] diseñada específicamente para realizar el análisis forense mejorado en los dispositivos con iOS[19].

Si bien las técnicas y herramientas mencionadas constituyen el marco formal 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 fundada sobre los puntos en litigio, o mejor dicho, responder los puntos de pericia de manera clara y contundente.

El principal inconveniente radica en las dificultades que tienen los partícipes no informáticos de la causa (jueces, fiscales, abogados, investigadores forenses de otras disciplinas) para interpretar los datos técnicos a la luz de la causa judicial, y en el contexto del resto de las pruebas documentales presentes en el litigio. De allí que se requiera de un sistema de representación que haga posible mostrar los datos en función del objetivo que se persigue (expresado en los puntos de pericia) y vinculados semánticamente en base a la relación que los mismos mantienen entre sí.

En el contexto forense, es importante vincular los datos a partir del significado de cada cosa. No se trata solo de "encontrar la evidencia digital", sino de interpretarla en el contexto de la situación, vinculándola con el resto de los componentes de la investigación (pruebas físicas, marco legal y procedimental, interrogatorios, etc.).

De modo que es indispensable avanzar en la forensia digital desde la óptica de la semántica como elemento vinculante de todos los componentes del sistema, ese es el objetivo de la ObE Forensic: realizar el análisis forense de correos electrónicos

[14] https://www.mailxaminer.com/
[15] https://www.guidancesoftware.com
[16] http://tulp2g.sourceforge.net/
[17] https://www.mobiledit.com/mobiledit-forensic
[18] https://www.elcomsoft.es/eppb.html
[19] Sistema operativo móvil desarrollado por Apple para los teléfonos inteligentes de esa marca

atendiendo a los requerimientos realizados sobre la evidencia digital (o sea los puntos de pericia), sustentando dicho análisis en los criterios científicos y técnicos que aporta la ingeniería ontológica.

5. ObE Forensic

ObE Forensic es una herramienta de análisis forense de correos electrónicos desarrollada para cumplir con los criterios definidos por [10] acerca de las herramientas forenses: el diseño de ObE Forensic está orientado a la evidencia, particularmente a la obtenida en casos en donde dicha evidencia es un correo electrónico; el modelo de visibilidad, filtro e informe de ObE Forensic le permite al experto forense establecer vínculos o relaciones de prioridad entre los datos encontrados a través de una interfase de comunicación sencilla; ObE Forensic es una aplicación dedicada, i.e., diseñada y desarrollada específicamente para el análisis forense de correos electrónicos, y responde a las necesidades propias de este tipo de evidencia digital; la arquitectura de procesamiento está conformada por herramientas no propietarias, y su diseño se ajusta a criterios de abstracción y modularidad que garantizan la mejora del algoritmo inicial a partir de las sucesivas pruebas cumplidas en el prototipo de la aplicación puesta a disposición de usuarios expertos; ObE Forensic considera los datos necesarios para enfocar el análisis en la identidad del individuo, al tomar los valores referidos a nombres de cuentas, identificación de equipos que pueden asociarse al usuario participante del correo.

Es posible encontrar herramientas disponibles para el análisis forense de correos electrónicos que permiten procesar un conjunto de cabeceras de correos electrónicos, pero la mayoría de ellas se agotan en mostrar los datos de la cabecera, que permiten responder puntos de pericia simples (como por ejemplo cuales son los datos de emisión/recepción del correo), dejando a consideración del perito la respuesta a los puntos periciales complejos como por ejemplo, establecer la trazabilidad del correo, identificar correos enviados y recibidos en rangos de fechas, o buscar información de correos asociadas entre un conjunto de cuentas de correo, entre otros.

Durante la FASE DE EXTRACCIÓN Y ANÁLISIS descripta en la sección 3.4 es cuando se utiliza ObE Forensic, tomando como insumo la cabecera del correo electrónico más los datos descriptivos relevados por el perito durante la actividad. A partir de este conjunto de datos iniciales, la aplicación busca e identifica los valores que luego se instancian en la ontología.

Es aquí en donde se observan las ventajas de esta herramienta respecto de otras propuestas para el análisis forense de correos electrónicos, ya que automatiza el análisis de la cabecera del correo y en función de la instanciación realizada sobre la ontología, permite responder a los puntos de pericia mediante los resultados de las preguntas de competencia.

Por último, ObE Forensic permite emitir un informe impreso sobre los resultados del análisis forense que el perito adjunta a su Informe Pericial en la FASE DE PRESENTACIÓN DE RESULTADOS.

5.1. Arquitectura de Procesamiento de ObE Forensic

A continuación se describe los componentes presentes en la arquitectura de procesamiento de ObE Forensic**.**

Desde el punto de vista del *hardware*, ObE Forensic ha sido desplegado en un servidor HP ProLiant DL360 G6 bajo Linux Mint 18, ubicado físicamente en el laboratorio Digilab de la Universidad Católica de Salta, el cual cuenta con un procesador Intel Quad Core Xeon E5504 y 4GB de RAM, cabe destacar que el sistema completo puede ser perfectamente utilizado en una instancia t2.micro del servicio EC2 ofrecido por Amazon Web Services, t2.nano[20].

El conjunto de herramientas de *software* utilizadas para desarrollar el sistema es variado. Se utilizó el framework para PHP[21]

[20] https://aws.amazon.com/es/ec2/instance-types
[21] http://php.net/

Laravel 5.6[22], el cual provee un entorno de trabajo del tipo Modelo-Vista-Controlador (MVC) que es la aplicación de tres componentes esenciales: el dominio de la aplicación (el modelo), la visualización del estado de la aplicación (la vista) y la interacción entre la vista y el modelo (el controlador). A través de las Vistas, el usuario interactúa con el sistema, proveyendo las entradas necesarias y pudiendo visualizar los procesamientos que el sistema realiza. Los Controladores se encargan de la lógica, el enrutamiento y la conexión con los Modelos, quienes proveen una interfaz para el acceso a los datos. Una particularidad de la aplicación es la posibilidad de incrementar el banco de preguntas de competencia, en caso de encontrar un punto de pericia que no pueda responderse desde las preguntas existentes. Esto es así debido a que una nueva pregunta de competencia se formaliza e integra en la aplicación mediante la definición del código correspondiente según criterios técnicos de modularidad de un software.

ObE Forensic se basa en *estructuras de datos* muy básicas, tales como texto plano para leer los correos electrónicos, y las estructuras propias del lenguaje PHP (String, Integer, Arrays, etc.).

En cuanto a la *conectividad*, los usuarios pueden acceder a OntoFoCE a través de un navegador web y el mismo se encuentra activo en la dirección https://digilab.ucasal.edu.ar.

La interfase de *comunicación con el usuario* está estructurada en base a una aplicación web construida con HTML5[23], CSS3[24] y jQuery[25], que permite realizar distintas acciones, listadas a continuación: seleccionar las cabeceras de los correos electrónicos a través de una ventana de selección de directorios de trabajo y subirlos a OntoFoCE; ingresar los datos adicionales sobre el caso en estudio, tales como Hardware y Software del equipo emisor, servidores y equipo receptor, cliente de correo utilizado, etc.; visualizar las instancias pobladas en la ontología y la trazabilidad de un correo; consultar preguntas de competencias relacionadas a un correo o un grupo de correos.

Las especificaciones requeridas sobre seguridad informática a cumplir por la aplicación son las siguientes: se requiere de la definición de políticas de seguridad para garantizar el acceso solo a los usuarios autorizados, así como para el resguardo y recuperación de datos, se requiere de un formulario de aceptación de condiciones de servicio por parte del usuario que ingresa por primera vez; se requiere del cumplimiento de normas referidas a la protección de datos personales y otras normas pertinentes a la realización de pericias informática.

Asi, se establecieron las políticas de acceso por parte de los usuarios expertos, restringiendo el ingreso a la aplicación mediante la entrega de un usuario y contraseña que debe solicitar vía correo electrónico. Cada usuario posee un espacio privado para el procesamiento que realiza y el mismo no es compartido con otros usuarios. En atención a que la aplicación utiliza información reservada como insumo, se estableció el formulario de aceptación de las condiciones de servicio de la herramienta, establecidas en una página de "Términos de Uso", mediante la cual se informa al usuario acerca de las restricciones y condiciones de utilización de la aplicación, en la que se enfatizan los aspectos legales vinculados con la responsabilidad en el uso de datos que provienen de una evidencia digital. En relación a las cuestiones de protección de datos personales, como a lo relativo a la seguridad informática en general, la aplicación fue desarrollada atendiendo a las cuestiones de seguridad informáticas propias de una aplicación web.

5.2. Estructura Funcional de ObE Forensic

La característica más destacable de ObE Forensic es que se basa en una ontología,

[22] https://laravel.com/
[23] https://developer.mozilla.org/es/docs/HTML/HTML5
[24] https://developer.mozilla.org/es/docs/Web/CSS
[25] https://jquery.com/

con lo cual se otorga a esta herramienta la capacidad de respuesta científica y metodológica que la ley exige a los procedimientos periciales.

La W3C (World Wide Web Consortium)[26] define una ontología como *"…los términos utilizados para describir y representar un área de conocimiento. Las personas, bases de datos y aplicaciones que necesitan compartir información de dominio utilizan ontologías (un dominio es solo un área temática específica o área de conocimiento, como medicina, fabricación de herramientas, bienes raíces, reparación de automóviles, administración financiera, etc.). Las ontologías incluyen definiciones computables de conceptos básicos en el dominio y las relaciones entre ellos [...]. Codifican el conocimiento en un dominio y lo hacen extensible a varios dominios. De esta manera, hacen que ese conocimiento sea reutilizable…".*

La utilidad de las ontologías se observa en la capacidad de describir una realidad en los propios términos de sus actores. Es decir, permite establecer una base de comunicación e interpretación de los conceptos referidos a un dominio que facilita la comprensión entre aquellos que comparten ese dominio.

La herramienta de análisis forense ObE Forensic es una aplicación que brinda soporte para dos actividades principales: i) la instanciación de los datos obtenidos de las cabeceras como conceptos y relaciones en la ontología y ii) la generación de respuestas a los puntos de pericia mediante las preguntas de competencia de la ontología.

Para lograr esto, se integra en un mismo ambiente tres componentes: Gestor de Instancias de la Ontología, Analizador de Puntos de Pericia y la ontología OntoFoCE, que mediante un servicio *SPARQL Endpoint*[27] que realizan consultas sobre la información almacenada en OntoFoCE.

A modo de breve explicación, puede decirse que ObE Forensic toma la cabecera de uno o un conjunto de correos que se ingresan mediante una interfase diseñada a tal fin. Con estos datos actúa el *Gestor de Instancias de OntoFoCE* realizando la instanciación en OntoFoCE en dos pasos: primeramente, el *Identificador de Instancias* recorre el texto del archivo plano para separar la cabecera y el cuerpo del correo electrónico y verifica que la cabecera sea válida; luego interviene el *Clasificador*, algoritmo responsable de asignar cada valor a instanciarlo en su correspondiente clase. Una vez obtenida la cabecera del correo electrónico e identificado los datos requeridos para instanciar las clases y relaciones de la ontología, se ejecutan las consultas a través del SPARQL Endpoint que brindan los datos necesarios para responder a las preguntas de competencia. Esto se ejemplifica considerando la cabecera de un correo que se muestra en la Figura 1.

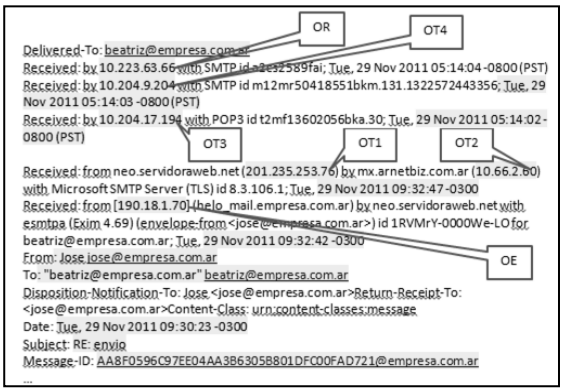

Figura 1: Cabecera de un correo de ejemplo con identificación de las ocurrencias

La cabecera de este correo contiene seis ocurrencias: una de emisión (OE), cuatro ocurrencias de transmisión (OT1, OT2, OT3 y OT4) y una de recepción (OR). También se observan los datos de fecha, hora y dirección IP de los distintos equipos intervinientes en la transmisión (equipo emisor, servidores y equipo receptor). La cabecera de un correo se debe leer de abajo hacia arriba, pues a medida que va siendo transportada, los procesos de control de la transmisión añaden información al inicio de la misma. Cada línea define un atributo y su valor según el siguiente formato *{Palabra clave}: {Valor}.* En la Tabla 1 se muestran

[26] https://www.w3.org/2003/08/owlfaq

[27] SPARQL Endpoint es un punto de presencia en una red HTTP que es capaz de recibir y procesar solicitudes de consulta SPARQL.

alguno de los valores que se instancias.
Por último, el Analizador de los Puntos de Pericia muestra los resultados a las preguntas de competencia que sean pertinentes al punto de pericia requerido.

Tabla 1: Patrón {Palabra_Clave:Valor} para la cabecera del correo de ejemplo

Palabra clave	Clase	Valor para Correo Ejemplo de Fig. 3
Subject	Asunto	RE: envio
Message-ID	CorreoValido	AA8F0596C97EE04AA3B6305B801DFC00FAD721@empresa.com.ar
Date	OcurrenciaDeEmisión	29/11/2011 09:30
From	CuentaEmisor	jose@empresa.com.ar
To, Delivered-To o X-Original-To	CuentaReceptor	beatriz@empresa.com.ar
Received o X-Received	OcurrenciaDeEmision (OE)	29 Nov 2011 09:32:42 -0300
	IP / HostName	190.18.1.70
	…	…

Algunas de las 21 preguntas de competencia a las que la ontología propuesta puede responder son las siguientes:
PC 01: ¿Cuál es la fecha, hora y dirección IP de emisión del correo electrónico?
PC 11: Dado un correo, un emisor y un receptor ¿cuál es la secuencia de equipos por los que ha pasado ese correo?
PC 14: Dada una dirección IP ¿cuál sería la localización geográfica del mismo?
PC 15: ¿Cuáles son los correos que han pasado por el dispositivo que posee una IP dada?
PC 16: ¿Cuáles son los mails enviados desde una determinada cuenta en una fecha dada?
PC 21: ¿Cuáles son los correos intercambiados entre las cuentas C1 y C2 en un rango de fechas dado?
Cabe mencionar que estas preguntas de competencia se elaboraron a partir de un relevamiento realizado mediante la consulta a usuarios expertos (peritos informáticos), obteniéndose 86 puntos de pericias diferentes, que por similitud de contenidos, se resumieron a 43 puntos periciales diferentes, que se pueden responder con estas preguntas de competencia.

6. Descripción de la Aplicación

Una vez que el usuario se registra e ingresa el archivo de la cabecera, la aplicación realiza el proceso de separación de la cabecera del cuerpo del correo electrónico, e instancia los valores correspondientes a cada clase y relación de OntoFoCE. El proceso termina cuando se muestra la pantalla de análisis (Figura 2):

Figura 2: Análisis de la/s cabecera/s ingresadas

Si se selecciona la opción de "Preguntas sobre 1 correo", la interfase indica las preguntas de competencia con sus respuestas (Figura 3):

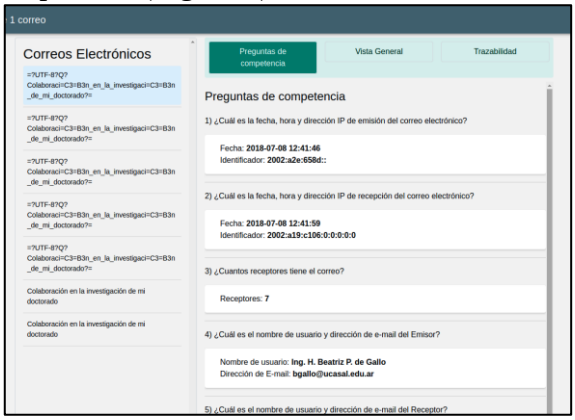

Figura 3: Preguntas de Competencia sobre una única cabecera

También es posible visualizar la *trazabilidad* del proceso de transmisión para la cabecera ingresada, un ejemplo se muestra en la pantalla de la Figura 4.

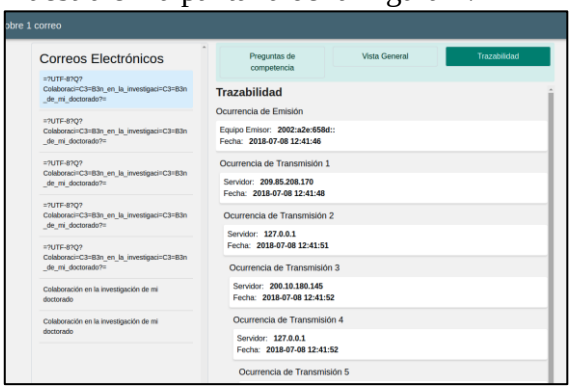

Figura 4: Trazabilidad de una Cabecera

La aplicación también permite el ingreso de los datos complementarios (identificación de equipos, expediente, etc.) y la impresión de un informe con todos los datos identificados más las respuestas a las preguntas de competencia.

7. Validación de ObE Forensic por parte de Usuarios Expertos

La aplicación web destinada al análisis forense de correos electrónicos también fue validada por un equipo de usuarios expertos a quienes se convocó expresamente para que utilizaran el prototipo inicialmente desarrollado, y con sus aportes y comentarios fue posible mejorar la capacidad de respuesta de ObE Forensic.

En este caso los usuarios expertos son aquellos profesionales informáticos que actúan además como peritos. Una vez desarrollada la aplicación en su primera versión, se invitó a los mismos a probarla a partir de casos reales de pericias de correos electrónicos, en los que ellos hubieran participado, y de los cuales tienen además los resultados del análisis forense. De este modo, se contrastó los resultados emitidos por ObE Forensic con los obtenidos por los peritos en cada caso.

Para utilizar datos de pericias reales, se pidió a los usuarios expertos que anonimizaran las cabeceras de los correos electrónicos que utilizarían para las pruebas, ya que las mismas son evidencia digital y es necesario preservar la identidad de las personas y/o instituciones que pudieran estar comprometidas.

Una vez que los peritos aceptaron probar ObE Forensic, se les envió un Formulario de Experimentación que debían completar cada vez que validaran la aplicación.

De los resultados de las pruebas experimentales realizadas se obtuvieron aportes, críticas y propuestas de mejoras, algunas de las cuales se incorporaron de inmediato en la aplicación y otras se tomaron como acciones futuras a considerar en el desarrollo a mediano plazo de ObE Forensic.

Sobre las preguntas de competencia

Del conjunto de 21 preguntas, los peritos identificaron 11 preguntas que les brindaron las respuestas necesarias para contestar los puntos de pericia. Al respecto los peritos dijeron:

- *"…En este caso no fue posible aplicar el software puesto que no se encontró una funcionalidad que diera el soporte necesario para responder al punto de pericia en cuestión (Comprobar la autenticidad de dichos correos). Se buscó alguna opción que contemplara el análisis de validez de correos electrónicos a través de mecanismos como DKIM, SPF o DMARC pero no fue hallado…"*.

Los mecanismos DKIM, SPF o DMARC[28] hacen referencia a técnicas de autenticación de correo electrónico que permite al receptor comprobar que un correo electrónico fue realmente enviado y autorizado por el propietario del dominio de la cuenta emisora. Si bien se consideran estas técnicas como adecuadas para comprobar la autenticidad de un envío, no invalida la capacidad de autentificación a partir de la trazabilidad del proceso de comunicación del correo electrónico, sino que la refuerza. Se está estudiando la viabilidad de implementar el mecanismo DKIM en ObE Forensic.

Sobre la efectividad de ObE Forensic

Si bien en la mayoría de los experimentos los peritos informan que los datos obtenidos sí coinciden con el análisis forense realizado previamente para el caso, resulta conveniente atender los siguientes casos:

- *"… si bien no hubo ningún caso en el que el sistema informe algo erróneo (falso positivo), sí existieron casos en los que no encontró información que sí estaba presente…"*.

El perito hace referencia aquí a que el algoritmo no identificó una ocurrencia de transmisión intermedia, por lo que se realizó la prueba paso a paso de la ejecución del algoritmo para ese caso particular, identificando el error y ajustándolo debidamente para que no volviera a generarse el inconveniente.

- *"…Solo en algunos casos. Por ejemplo no responden ninguna de las preguntas generales…"*.

Durante la entrevista realizada con el

[28] https://www.dmarcanalyzer.com/es/dkim-3

experto a fin de identificar cuáles era el inconveniente señalado, se observó que en realidad, el problema estaba más orientado a las cuestiones de usabilidad de la aplicación. Las interfases de comunicación con el usuario no eran lo suficientemente claras respecto de los botones habilitados para ver las preguntas de competencia para un correo en particular, respecto de los botones habilitados cuando se analiza un conjunto de correo. Es decir, hay preguntas de competencia (las indicadas como 09 a 21) que requieren de al menos dos cabeceras ingresadas, de lo contrario no se pueden responder, esto no estaba suficientemente aclarado en las interfases de comunicación de la aplicación, situación que se modificó de inmediato.

Sobre la utilidad de la aplicación

Los peritos consideran la aplicación como provechosa, asignándole un puntaje promedio de 3 a 4 puntos y señalando las mejoras que agregarían calidad y/o usabilidad a la aplicación.

Sobre las dificultades para realizar el experimento

No se indicaron dificultades más allá del aprendizaje propio de encontrarse con una nueva aplicación.

Se informaron inconvenientes menores que se solucionaron a la brevedad:

- *"… Cuando se ingresa un mail sin cabecera la aplicación no genera un error…"*.
- *"…No permite cerrar la sesión del usuario logueado…",*
- *"…En la carga de cualquier dato, posiblemente tenga una vulnerabilidad de SQL INJECTION ya que cualquier dato que antecede con un " ' " provoca un error y por ello luego ya no se puede cargar. Un ejemplo de ello es en la carga de los datos de hardware y software. Dependiendo del lenguaje utilizado se debería prevenir a fin de evitar el robo de datos…".*

Se tomó en cuenta este comentario para reforzar las reglas de validación de ingreso de los datos. Muchas de esas vulnerabilidades ya están resueltas por el framework Laravel. La más crítica de ellas, SQL INJECTION, no se aplicaría en este caso, ya que no se utiliza una base de datos SQL, sino un conjunto de tripletas RDF. Pero este comentario advierte acerca de si no es posible un caso de "inyección SPARQL", respecto de lo cual hay opiniones encontradas[29].

Sobre los aspectos a mejorar en la aplicación

Se realizaron varias sugerencias, entre las que se destacan las siguientes:

- *La aplicación podría enriquecer su funcionalidad permitiendo concatenar filtros para el tratamiento de los correos. Por ejemplo "filtrar aquellos que correspondan al período X" concatenado con "de lo filtrado, extraer aquellos correos que hallan transitado por la IP xx.xx.xx.xx".*
- *Si los correos electrónicos no se encuentran en la misma carpeta, la aplicación no permite elegir más de uno.*

8. Conclusiones

El uso de una herramienta para el análisis forense, de por sí aporta rigor metodológico a la tarea pericial. Por otra parte, el hecho de basar la aplicación en una ontología, garantiza que el modelo construido mediante OntoFoCE responda a los criterios de metodológicos y de cientificidad que se exige al procedimiento pericial, porque genera un contexto de comunicación con el resto de los actores judiciales (jueces, abogados, otros peritos) basado en un mismo *sistema terminológico y conceptual*.

Otro beneficio de aplicar las tecnologías semánticas en la aplicación es que se logró representar la trazabilidad del envío de un correo electrónico permitiendo con ello avalar el carácter probatorio de este documento digital y reforzando la capacidad de no repudio del mismo.

Puede decirse que ObE Forensic responde a los objetivos que persigue: representar la trazabilidad del proceso de transmisión e identificar los datos de las cuentas intervinientes. Aun así, es necesario atender las sugerencias de mejora aportadas por los usuarios expertos, así como continuar realizando más pruebas de validación.

Si bien las 21 preguntas de competencia se formularon en base al relevamiento de puntos de pericia, es posible que surjan

[29] https://www.owasp.org/images/0/0f/Onofri-NapolitanoOWASPDayItaly2012.pdf

nuevos puntos de pericia que no se puedan responder con las preguntas existentes hoy en ObE Forensic, por ello, sería deseable contar con un *editor de preguntas de competencia,* a fin de aprovechar al máximo la base de conocimiento que brinda OntoFoCE y no limitar la aplicación a un conjunto cerrado de resultados.

Otras líneas de investigación surgen de esta propuesta: como por ejemplo, considerar el análisis forense de una cuenta de correo electrónico mediante modelos correlacionales que vinculen fechas, usuarios, palabras claves, etc, También sería de utilidad avanzar en el análisis forense de correos considerando múltiples dispositivos que comparten una única cuenta.

No está todo dicho, considerando que la tecnología avanza en el desarrollo de nuevas áreas (Internet de las Cosas por ejemplo) y en la profundización de áreas existentes (Inteligencia Artificial por citar alguna), de seguro surgirán nuevas aplicaciones basadas en las tecnologías semánticas y que resuelvan cuestiones de la forensia digital, ya sea con generación de nuevas herramientas como en la generación de ámbitos que promuevan el trabajo interdisciplinario como en el caso del Derecho y la Informática.

Referencias

[1] B. P. De Gallo, M. Vegetti, and H. Leone, "Población de ontologías con datos no estructurados utilizando herramientas de minería de datos," in *CONAIISI 2015*, 2015.

[2] B. P. De Gallo and H. Leone, "Aplicación de la Ingeniería Ontológica para representar la trazabilidad de un Correo Electrónico," *2º Simp. Argentino Ontol. y sus Apl. (SAOA 2016)*, pp. 108–121, 2016.

[3] B. P. De Gallo, M. Vegetti, and H. Leone, "Hacía una Ontología para el soporte de la trazabilidad del correo electrónico en la Forensia Digital," in *V Congreso Iberoamericano de Docentes e Investigadores de Derecho e Informática (CIIDDI 2017)*, 2017.

[4] A. H. Di Ioro *et al.*, "El rastro digital del delito Aspectos técnicos , legales y estratégicos de la Informática Forense." Esitorial UFASTA, Mar del Plata, p. 556, 2017.

[5] J. I. Cafferata Nores and G. García, *La prueba en el proceso penal*, 5a Edición. Buenos Aires: Depalma, 2003.

[6] M. Gilardi and G. Unzaga Domínguez, "La Prueba Pericial en el Proceso Penal de la Provincia de Buenos Aires," *Rev. Buenos Aires La Ley*, vol. Año 14 Núm, p. 709, 2007.

[7] A. Bender, "La prueba digital. Jurisprudencia y normas del Código Civil y Comercial de la Nación," *elDial.com Biblioteca Jurídica OnLine*, 2017.

[8] M. E. Darahuge and L. E. Arellano González, *Manual de Informática Forense III*. 2016.

[9] E. Rivetti, J. A. Fleming, B. P. De Gallo, and H. Leone, "Análisis de los Documentos Oficiales sobre Obtención , Tratamiento y Preservación de la Evidencia Digital Aportes para el Tratamiento del Correo Electrónico como Evidencia Digital," in *CONAIISI 2016*, 2016.

[10] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, no. SUPPL., pp. S64–S73, 2010.

[11] E. A. Rivetti and B. P. De Gallo, "Estudio comparativo de desempeño de herramientas para el Análisis Forense de Correos Electrónicos," in *CONAIISI 2017*, 2017, pp. 46–51.

[12] V. K. Devendran, H. Shahriar, and V. Clincy, "A Comparative Study of Email Forensic Tools," *J. Inf. Secur.*, vol. 06, no. 02, pp. 111–117, 2015.

[13] R. Hadjidj, M. Debbabi, H. Lounis, F. Iqbal, A. Szporer, and D. Benredjem, "Towards an integrated e-mail forensic analysis framework," *Digit. Investig.*, vol. 5, no. 3–4, pp. 124–137, 2009.