Metodología de obtención de Evidencia en la Nube

Methodology for Obtaining Evidence in the Cloud

Lic. Gastón Semprini, Lic. Gerardo Nilles, Lic. Gastón Silva

Departamento de Informática Forense,
Poder Judicial de la Provincia de Rio Negro,
Argentina.
gsemprini@jusrionegro.gov.ar
gnilles@jusrionegro.gov.ar
gsilva@jusrionegro.gov.ar

Resumen. La computación en la nube es la tendencia, en el proceso de transformación digital, más adoptada por organizaciones de todos los tamaños. El uso del servicio del almacenamiento de la información en la nube empieza a tomar gran participación en la disciplina de la informática forense. La utilización de la nube ha permitido que los informáticos forenses que puedan adquirir y preservar a distancia evidencia digital almacenada en cualquier dispositivo informático como puede ser un dispositivo móvil. Esto ha llevado no solo a mejorar y optimizar el servicio de justicia en lo que refiere a investigaciones donde se encuentre involucrado evidencia digital sino también a un cambio de paradigma para la informática forense en un futuro no muy lejano, donde la evidencia digital dejara de estar almacenada en el dispositivo de uso diario y pasara a estar almacenada en distintos servidores localizados en cualquier lugar del mundo. Este artículo aborda el aspecto metodológico y las buenas prácticas referidas a la obtención de evidencia digital almacenada en la nube.

Palabras clave: Nube, análisis, forense, evidencia.

Abstract. Cloud computing is the trend in the digital transformation process most embraced by organizations of all sizes. The use of the information storage service in the cloud begins to take a large share in the discipline of computer forensics. The use of the cloud has allowed forensic computer scientists to remotely acquire and preserve digital evidence stored on any computer device, such as a mobile device. This has led not only to improve and optimize the justice service in terms of investigations where digital evidence is involved, but also to a paradigm shift for computer forensics in the not too distant future, where the evidence digital will no longer be stored in the device for daily use

Received December 2020; Accepted March 2021; Published June 2021

and will be stored in different servers located anywhere in the world. This article addresses the methodological aspect and good practices related to obtaining digital evidence stored in the cloud.

Keywords: Cloud, analysis, forensics, evidence.

1 Introducción

En la actualidad es habitual la utilización de servicios ofrecidos por distintos prestadores de internet para el almacenamiento de la información personal en la nube, desde correos electrónicos, distintos tipo de archivos multimedia fotos, videos, música, archivos de ofimática, posicionamientos de GPS, *backup* de un servicio de mensajería como ser whatsapp hasta copias de seguridad o *backup* de distintos dispositivos tecnológicos (dispositivos móviles, DVR, etc).

Las empresas que ofrecen estos servicios, brindan no solo seguridad para sus datos, sino también la posibilidad de acceder desde cualquier lugar y dispositivos a la vez. Esta información almacenada en la nube puede ser muy importante para una investigación judicial no solo del Fuero Penal sino también para el Fuero del Trabajo, Fuero Civil, Comercial, Minería y Sucesiones, Fuero de Familia.

La informática forense es una disciplina de las ciencias forenses que se dedica al análisis de la evidencia digital almacenada en cualquier dispositivo tecnológico. Para ello el informático forense sigue pautas, métodos y procedimientos bien definidos que permiten identificar, preservar, analizar y presentar dicha evidencia digital en una investigación Judicial.

En lo que respecta al informática forense en la nube, el Instituto Nacional de Estándares y Tecnología (NIST) [1], lo define como "*la aplicación de principios científicos, prácticas tecnológicas y métodos derivados y probados para reconstruir los eventos pasados de computación en la nube a través de la identificación, recolección, preservación, examen, interpretación y reporte de la evidencia digital*".
La adquisición de evidencia digital de entornos en la nube es más restrictivo porque las infraestructuras y los recursos no son propiedad de los usuarios de la nube sino que son proporcionados por los proveedores de servicios en la nube (CSP) Cloud Service Provider. Los usuarios tienen acceso limitado a los datos y no tienen conocimiento de dónde se encuentran físicamente [2].
Para ello es necesario establecer un procedimiento de buenas prácticas que permita identificar, preservar y adquirir la evidencia digital almacenada en la nube y garantizar la integridad de la misma.

2 Procedimiento de buenas prácticas para la obtención de evidencia digital en la nube

En función del estudio y pruebas de conceptos realizadas por el Departamento de Informática Forense Poder Judicial de Rio Negro, se ha elaborado una guía de buenas prácticas para la obtención de evidencia digital de proveedores de servicios en la nube. El objetivo de esta guía es otorgar un marco formal adecuado que permita ofrecer rigurosidad y control de calidad en la integración de los métodos y técnicas utilizadas. Para la elaboración de esta guía se siguieron los lineamientos propuestos por Scientific Working Group on Digital Evidence (SWGDE) [3].

2.1 Desafíos que se deben afrontar

Esta guía no es exhaustiva para las personas que no tienen experiencia en la adquisición de evidencia digital, para su utilización el investigador debe poseer una comprensión básica de la metodología.

Dada la gran cantidad de plataformas y proveedores de servicios en la nube, no es posible establecer un conjunto preciso de procedimientos para cubrir cada situación. El investigador debe seleccionar las acciones apropiadas en función de los recursos disponibles y su conocimiento y comprensión del caso investigado.

2.2 Evidencia digital en la nube

El almacenamiento en la nube se utiliza frecuentemente para aumentar la capacidad de almacenamiento, sincronizar información entre dispositivos u ofrecer servicios informáticos remotos.

Los dispositivos informáticos pueden sincronizar o hacer una copia de seguridad de los datos y configuraciones de los usuarios en los espacios de almacenamiento de los proveedores de la nube de forma predeterminada, lo que requiere poca interacción del usuario. Algunos dispositivos tienen por defecto una sincronización automática con servicios en la nube, WhatsApp, Redes Sociales, imágenes, videos, documentos del dispositivo, etc. El investigador debe tener en cuenta que los datos pueden existir en varios lugares.

Puede haber diferencias en el estado de cifrado entre un dispositivo local y los datos sincronizados con la nube. Los datos en el dispositivo local pueden estar encriptados o ser difíciles de decodificar, sin embargo, al solicitar datos al proveedor de la nube podría proporcionarlos de forma no encriptada o legible.

Un proveedor puede proporcionar información adicional asociada con esa cuenta, como dispositivos históricos, actividad del dispositivo y registros de usuario. Los datos históricos almacenados en la nube pueden ser más extensos y valiosos que los encontrados en un dispositivo local.

2.3 Métodos de adquisición y preservación de la evidencia digital

Se describen a continuación los métodos y etapas para la de adquisición y preservación de la evidencia digital:

- **Previo a la adquisición**: Identificar cual es la evidencia relevante a preservar, los períodos de tiempo, los proveedores de servicios en la nube involucrados y los servicios utilizados. Los registros de facturación y la información de la cuenta que identifiquen al proveedor y los servicios específicos. La mayoría de los proveedores publican políticas de privacidad en su sitio web que detallan los servicios que brindan, los tipos de información que recopilan y las circunstancias bajo las cuales recopilan esa información. Si corresponde, solicitar al proveedor que preserve la evidencia relacionada a la investigación;

- **Acceso mediante solicitud judicial**: La evidencia se obtiene mediante oficio judicial a los distintos proveedores de servicios. Existen dos tipos de solicitud, una consiste en los datos básicos de la cuenta que contienen fecha de alta/baja de la cuenta, números de teléfonos y correos electrónicos asociados, fecha y hora de inicios de sesión (IP de Conexión), dispositivos asociados, etc. otra información que se puede obtener es el contenido de la cuenta, ya sea comunicaciones y/o publicaciones. Para ambos casos se deben consultar las secciones legales de los proveedores para conocer cómo realizar el pedido y que información se puede obtener;

- **Acceso por usuario y contraseña**: La evidencia se obtiene ingresando las credenciales aportadas por la parte interesada, típicamente un nombre de usuario o cuenta de correo electrónico y su contraseña. También se pueden obtener credenciales de los dispositivos físicos que se encuentren bajo investigación. Algunos proveedores de servicios en la nube permiten el acceso a los datos almacenados con ellos y los metadatos asociados a través de aplicaciones cliente o API. Es posible que el acceso a los datos a través de estas API se pueda obtener desde un dispositivo en investigación que utiliza los servicios en la nube. En los casos que las credenciales no sean aportadas por las partes interesadas es necesario contar con la correspondiente autorización legal.

- **Procedimiento en la adquisición**: Documentar el proceso de adquisición, los métodos utilizados, cómo se reciben los datos. Tomar fotografías, filmar y capturas de pantalla o en algunos casos realizar una grabación de la sesión

utilizada. Determinar si los datos relevantes pueden adquirirse utilizando el método de adquisición planificado. Obtener los datos utilizando el método de adquisición seleccionado. Si surgen problemas para obtener los datos a través de métodos planificados, intentar métodos alternativos. Si todos los métodos fallan, considerar las capturas de pantalla o fotografías de los datos relevantes.

- **Una vez finalizada la adquisición**: Calcular y registrar valores *hash* para los datos adquiridos. Si un proveedor provee información firmada digitalmente o proporciona valores *hash*, verificar la firma o los valores *hash*. Verificar que se hayan adquirido todos los datos. Si los datos se proporcionaron en medios físicos documentar como se recibió. Seguir los procedimientos del área para almacenar los datos adquiridos, transferir los datos adquiridos a un medio adecuado de almacenamiento de evidencia, para ser entregados al área correspondiente.

3 Regulación del procedimiento de preservación de la evidencia digital en la nube

Resulta necesario establecer un marco normativo comprensible y viable de buenas prácticas respecto a la extracción de evidencia digital almacenada en la nube. En el caso del Poder Judicial de Río Negro, el marco normativo es establecido por la Acordada 8/2019 Superior Tribunal de Justicia [4] (ver texto completo en el Anexo). La intención de la Acordada es garantizar que la preservación de la evidencia se realice bajo un procedimiento metodológico y riguroso siguiendo los protocolos, procedimientos estándares y guías de buenas prácticas para ello.

Dentro de los considerandos, se establece que:

- Las preservaciones se realizan utilizando las credenciales de acceso a las correspondientes plataformas que pueden ser obtenidas de los dispositivos o aportadas por el propietario;

- Al no requerir acceso al dispositivo la preservación de evidencia se puede realizar a distancia independiente del dispositivo en el cual se haya originado, recibido o almacenado el dato pudiendo en determinadas circunstancias recuperar datos eliminados;

- La evidencia preservada de esta manera puede ser analizada utilizando las mismas técnicas y herramientas que para la evidencia tradicional;

En el contexto de la Acordada se brindó una capacitación a los operadores de justicia sobre la importancia de la obtención de este tipo de evidencia, se generó un protocolo de actuación en el cual se establecen los pasos a seguir por el operador que requiere el servicio. También se dotó a las oficinas de acceso a Internet a través de WIFI para los casos en que se requiera la sincronización de datos de un dispositivo con la nube.

4 Estandarización del procedimiento en la nube del Departamento de Informática Forense

Según lo establecido en el marco normativo de la Acordada 8/2019 del Superior Tribunal de Justicia para garantizar las buenas prácticas respecto del uso del almacenamiento de datos y extracción de evidencia digital almacenada en la nube, el Departamento de Informática Forense confecciono un Procedimiento Operativo Estandarizado (SOPs) donde se detallan los pasos y procedimientos a seguir. [5].

SOP. Preservación de la evidencia digital almacenada en la nube

Propósito:

El propósito de este procedimiento es la obtención de evidencia digital de proveedores de servicios en la nube, permitiendo ofrecer rigurosidad y control de calidad en la integración de métodos y técnicas utilizadas.

Alcance:

Este SOP describe los pasos a seguir a los efectos de obtener la evidencia digital que fuera generada, procesada por un dispositivo tecnológico y que fuera resguardada en un proveedor que brinda servicio de almacenamiento en la nube.

Equipamiento:

Hardware:

a Estación Forense

Software:

a Oxigen Forensic
b Axiom Cloud
c Navegador Web
d OSIRT
e Propios de la plataforma o proveedor.

Limitaciones:

Esta guía no es exhaustiva para las personas que no tienen experiencia en la adquisición de evidencia digital, para su utilización el investigador debe poseer una comprensión básica de la metodología.
Dada la gran cantidad de plataformas y proveedores de servicios en la nube, no es posible establecer un conjunto preciso de procedimientos para cubrir cada situación. El investigador debe seleccionar las acciones apropiadas en función de los recursos disponibles y su conocimiento y comprensión del caso investigado.

Procedimiento:

Los pasos del procedimiento deben ser documentados con suficiente detalle, de manera que permita a otro forense, competente en la misma área, ser capaz de identificar que se ha hecho y evaluar los resultados independientemente. Los pasos que se enumeraran deben adaptarse según la situación que se encuentren.

1 Pasos anteriores a la adquisición:

1.a Verificar la evidencia que hay que adquirir en base a lo solicitado;

1.b Verificar y constatar que las credenciales de la cuenta (usuario y contraseña) donde se almacenan y adquirirá la evidencia digital sean las correctas;

1.c Si es necesario validar y autenticar la estación de trabajo con el código de seguridad para poder acceder a la cuenta especifica.

2 Pasos durante la adquisición:

2.a Si fuera necesario, registrar mediante captura de video todo el procedimiento (utilización de software como, por ejemplo, OSIRT);

2.b Documentar si fuera necesario las características del dispositivo informático y/o prestador del servicio donde se encuentra la evidencia que hay que adquirir y preservar. Realizar capturas de pantalla;

2.c Identificar la evidencia que hay que adquirir, si se encuentra en un dispositivo informático local y no esta sincronizado en la nube, realizar la sincronización, copia de seguridad y/o respaldo necesario para almacenarlo en la cuenta de la nube donde se realizará la adquisición y preservación;

2.d Adquirir la evidencia y documentar el proceso de adquisición, los métodos utilizados, cómo se reciben los datos;

2.e Tomar fotografías y capturas de pantalla o en algunos casos realizar una grabación de la sesión utilizada;

2.f Si surgen problemas para obtener los datos a través de métodos planificados, intentar métodos alternativos y documentarlos;

2.g Si todos los métodos fallan, considerar las capturas de pantalla o fotografías de los datos relevantes.

3 Pasos posteriores a la adquisición:

3.a Calcular y registrar valores *hash* para los datos adquiridos;

3.b Si un proveedor provee información firmada digitalmente o proporciona valores *hash*, verificar la firma o los valores *hash*;

3.c Verificar que se hayan adquirido todos los datos;

3.d Seguir los procedimientos del área para almacenar los datos adquiridos, resguardar los datos en la carpeta del caso.

5 Aplicación del procedimiento en un caso real en el Poder Judicial de Rio Negro

En una investigación Penal se solicitó obtener datos de un dispositivo móvil para determinar la geolocalización en una fecha y rango horario determinado. En este caso en particular al no contar con el dispositivo móvil en el Laboratorio, se procedió a utilizar el “SOP de preservación de evidencia digital en la nube”.

Operaciones Realizadas:

1 Pasos anteriores a la adquisición:

- *Verificar la evidencia que hay que adquirir en base a lo solicitado*. Se procedió a realizar una comunicación telefónica con el operador judicial que se encontraba junto con el dueño del dispositivo móvil a los fines de realizar las operaciones necesarias para la adquisición de la evidencia digital y constatar que tenía el GPS activado en su dispositivo;

- *Verificar y constatar que las credenciales de la cuenta (usuario y contraseña) donde se almacenan y adquirirá la evidencia digital sean las correctas*. Se constató si el dispositivo contaba con una cuenta de Gmail asociada al dispositivo y se solicitó usuario y contraseña de la misma;

- *Si es necesario validar y autenticar la estación de trabajo con el código de seguridad para poder acceder a la cuenta*. Utilizando las credenciales aportadas, se accedió a la cuenta desde la estación forense. Eso permitió también realizar la adquisición con las herramientas forenses.

2 Pasos durante la adquisición:

- *Si fuera necesario, registrar mediante captura de video todo el procedimiento. (utilización de software como por ejemplo OSIRT).* Para este caso en particular se utilizó la herramienta FlashBack Express, para realizar una grabación de pantalla de la estación forense;

- *Documentar si fuera necesario las características del dispositivo informático y/o prestador del servicio donde se encuentra la evidencia que hay que adquirir y preservar.* Se realizaron capturas de pantalla de la configuración del dispositivo;

- *Identificar la evidencia que hay que adquirir, si se encuentra en un dispositivo informático local y no esta sincronizado en la nube, realizar la sincronización, copia de seguridad y/o respaldo necesario para almacenarlo en la cuenta de la nube donde se realizará la adquisición y preservación.* Se procedió a verificar la última copia de seguridad de whatsapp y que su fecha fuera posterior al hecho investigado, se verificó que tenga los puntos de geolocalización en Google Maps y las imágenes capturadas con el dispositivo, sincronizadas con la plataforma google photos;

- *Adquirir la evidencia y documentar el proceso de adquisición, los métodos utilizados, cómo se reciben los datos.*

A su vez, utilizando las credenciales aportadas:

- Se preservaron los recorridos registrados en la aplicación Google Maps para las fechas de interés;

- Se descargó una copia de seguridad del WhatsApp almacenada en la nube y se desencriptó con la herramienta Oxigen Forensics;

- Se descargó una copia de seguridad del dispositivo con el objetivo de obtener llamadas entrantes y salientes;

- Se realizó preservación de las imágenes que se encontraban en almacenadas en la plataforma google photos.

3 Pasos posteriores a la adquisición:

- Calcular y registrar valores *hash* para los datos adquiridos;

    - Se realizó el procedimiento de *hash* para todos los archivos adquiridos.

Del análisis de toda la información recolectada, se pudo determinar el recorrido realizado desde su casa al trabajo, fecha y hora aproximada de ingreso y egreso del lugar de trabajo.

Se obtuvieron además mensajes de whatsapp que incluían imágenes enviadas a contactos en el periodo de tiempo comprendido entre el ingreso y egreso del lugar de trabajo. Se compararon las imágenes enviadas por whatsapp con las que se preservaron de su cuenta en google photos para corroborar, mediante el análisis de los metadatos, que las mismas fueron capturadas desde dicho dispositivo y luego fueron enviadas por whatsapp a los diferentes contactos.

Este análisis permitió determinar que en la fecha solicitada el dispositivo se encontraba en el lugar de trabajo y estaba siendo utilizado por la persona investigada.

6 Conclusiones

El objetivo de este trabajo es proporcionar una guía de buenas prácticas para los laboratorios o profesionales dedicados a las disciplinas de las ciencias forenses, específicamente la Informática Forense, para la obtención de la evidencia digital almacenada en la nube.

Como se detalló a lo largo del trabajo, el laboratorio de Informática Forense perteneciente al Poder Judicial de Rio Negro, ha logrado aplicar el procedimiento operativo estandarizado a los efectos de obtener evidencia digital que fuera generada, procesada, almacenada en distintos dispositivo informáticos y luego sincronizada en un servicio de la nube.

Esto trajo como resultado la adquisición de evidencia digital aportada por una víctima, un testigo o cualquier persona que se encuentre realizando una denuncia en cualquier ciudad de la Provincia sin importar la distancia y optimizando los tiempos ya que no es necesario el traslado de los dispositivos hasta el laboratorio.

En lo que respecta a los Fueros de “Familia”, “Trabajo” y “Civil, Comercial, Minería y Sucesiones”, ha permitido poder dar un servicio pericial en todo el territorio de la Provincia, siendo posible en la mayoría de los casos, aplicar este

procedimiento de obtención de evidencia digital almacenada en cualquier dispositivo informático.

La elaboración del Procedimiento Operativo Estandarizado le permitió Departamento de Informática Forense del Poder Judicial de Rio Negro, no solo darle celeridad al proceso, sino también validación de información documental.

Referencias bibliográficas

[1] N. C. C. F. S. W. Group. NIST cloud computing forensic science challenges. Draft NISTIR 8006, 2014.

[2] Stavros Simou, Christos Kalloniatis, Stefanos Gritzalis, Haralambos Mouratidis: A survey on cloud forensics challenges and solutions. Security and Communication Networks, Noviembre 2016.

[3] SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers
Versión: 1.0 (Julio, 2019).

[4] Superior Tribunal de Justicia de la provincia de Rio Negro. Acordada 8/2019. Disponible en https://digesto.jusrionegro.gov.ar/bitstream/handle/123456789/9351/Ac008-19.pdf?sequence=1&isAllowed=y

[5] SWGDE for Computer Forensics Model SOP for Computer Forensics. (13/09/2012)

ANEXO

SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA DE RÍO NEGRO

ACORDADA No 8/2019

En la ciudad de Viedma, Capital de la Provincia de Río Negro, a los 26 días del mes de junio del año dos mil diecinueve, reunidos en Acuerdo los Señores Jueces y las Señoras Juezas del Superior Tribunal de Justicia, y;

CONSIDERANDO:

Que uno de los objetivos del Superior Tribunal de Justicia es el desarrollo de tecnologías informáticas que garanticen la accesibilidad, eficiencia, eficacia, inmediatez y seguridad en la recolección de información.

Que en virtud de la constante evolución surgen nuevas formas de almacenamiento de la evidencia digital, lo cual hace que se deban implementar nuevos métodos y técnicas de adquisición y preservación que respeten los principios enunciados en las normas estándares (ISO-IEC-27037 -Relevancia, Suficiencia y Fiabilidad).

Que así, aparece el “almacenamiento en la nube” como un modelo de servicio en el cual los datos contenidos en un dispositivo informático se almacenan, administran y se respaldan de forma remota, típicamente en servidores que están en internet y que son administrados por un proveedor del servicio.

Que algunos de estos datos son: fotos sincronizadas con algún servicio de almacenamiento en la nube, backups de dispositivos y de programas de mensajería, recorridos georreferenciados, actividad y comunicaciones en redes sociales, etc.

Que dichos datos almacenados en la nube pueden contener evidencia digital, la cual puede ser preservada y analizada en el contexto de una pericia informática realizada en el marco de cualquiera de los fueros judiciales.

Que esa preservación se realiza utilizando las credenciales de acceso a las correspondientes plataformas que pueden ser obtenidas de los dispositivos o aportadas por el propietario.

Que la indicada preservación de evidencia en la nube tiene ventajas, a saber: a) no requiere acceso al dispositivo, incluso puede hacerse a distancia; b) se puede obtener evidencia en tiempo real; c) es independiente del modelo del dispositivo en el cual se haya originado, recibido o almacenado el dato; d) se pueden recuperar datos eliminados en determinadas circunstancias.

Que el Departamento de Informática Forense recomienda la preservación de datos en la nube para los casos en que la evidencia digital sea aportada por un denunciante, testigo, posible imputado, las partes y otros, sin necesidad de retener el dispositivo de origen.

Que la evidencia allí almacenada puede ser analizada utilizando las mismas técnicas que para la evidencia tradicional.

Que de la evidencia digital recolectada en la nube se pueden obtener datos de geolocalización desde los recorridos y las imágenes, comunicaciones desde las distintas redes sociales y mensajeros instantáneos, información de contactos, historiales de navegación, búsquedas en internet, actividades del dispositivo, etc.

Que resulta necesario establecer un marco normativo comprensible y viable de buenas prácticas respecto del uso del almacenamiento de datos y extracción de evidencia digital de información almacenada en la nube.

Por ello, y en uso de la facultades otorgadas por el artículo 43 incs. a) y j) de la ley 5190,

EL SUPERIOR TRIBUNAL DE JUSTICIA

RESUELVE:

Artículo 1°.- Establecer que la preservación de toda evidencia digital almacenada en la nube relacionada a causas penales, civiles, laborales y de familia se efectuará con la intervención de los profesionales del Departamento de Informática Forense.

Artículo 2°.- Realizar la preservación de la evidencia digital almacenada en la nube siguiendo los protocolos, procedimientos estándares y guías de buenas prácticas para el tratamiento de la evidencia digital.

Artículo 3°.- Capacitar a los Magistrados y Funcionarios del Poder Judicial y del Ministerio Público sobre los aspectos aquí tratados, a través del Departamento de Informática Forense en conjunto con la Escuela de Capacitación Judicial.

Artículo 4°.- Establecer que el Comité de Informatización de la Gestión Judicial arbitre los medios necesarios para que las áreas correspondientes faciliten técnicamente las medidas necesarias para brindar dicho servicio.

Artículo 5°.- Regístrese, notifíquese y oportunamente archívese.

Firmantes:

ZARATIEGUI - Presidenta STJ - PICCININI - Jueza STJ - APCARIÁN - Juez STJ - MANSILLA - Juez STJ - BAROTTO - Juez STJ.
MUCCI - Secretaria de Gestión y Acceso a Justicia STJ.