UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Plan de Investigación de fin de carrera titulado:

"Desarrollo de una herramienta forense bajo la normativa NIST 2001 para la recolección, validación y certificación de evidencia electrónica digital online en la red social Twitter"

Realizado por:

VALENCIA SASIL ADRIANA IVONNE

Director del proyecto:
MGS. LUIS FABIAN HURTADO VARGAS

Como requisito para la obtención del título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Quito, octubre de 2020

DECLARACION JURAMENTADA

Yo, ADRIANA IVONNE VALENCIA SASIL, con cedula de identidad # 1718185513, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría que no ha sido previamente presentado por ningún grado a calificación profesional y, que se ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Adriana Ivonne Valencia Sasil

C.C.: 1718185513

DECLARATORIA

El presente trabajo de investigación titulado:

"DESARROLLO DE UNA HERRAMIENTA FORENSE BAJO LA NORMATIVA NIST 2001 PARA LA RECOLECCIÓN, VALIDACIÓN Y CERTIFICACIÓN DE EVIDENCIA ELECTRÓNICA DIGITAL ONLINE EN LA RED SOCIAL TWITTER"

Realizado por:

VALENCIA SASIL ADRIANA IVONNE

Como requisito para la Obtención del Título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Ha sido dirigido por el profesor

ING. LUIS FABIAN HURTADO VARGAS, MGS.

Quien considera que constituye un trabajo original de su autor

_____

Ing. Luis Fabián Hurtado Vargas, MGS.

DIRECTOR

PROFESORES INFORMANTES

Después de revisar el trabajo presentado. Lo ha calificado como apto para su defensa oral ante el tribunal examinador.

_____

Ing. José Luis Medina Balseca, MGS

_____

Ing. Juan Xavier Játiva Álvarez, MGS

RESUMEN

El trabajo propuesto tiene como objetivo, la creación de un sistema forense en base a la normativa NIST 2001 para la recolección de evidencia electrónica digital de la red social Twitter, incluyendo la certificación de esta evidencia mediante firma digital y sellado de tiempo; evitando así la adulteración de la evidencia durante la judicialización de hechos delictivos. Considerando que los datos publicados en una red social solo existirán en un momento en el tiempo, trabajar en una copia de estos datos debe considerarse la mejor práctica habiendo extraído primero tanta información como sea posible. A través de las etapas definidas para el modelo que comprende dos entornos, uno físico y el digital se plantean diversas tareas a ser ejecutadas en cada uno de estos entornos, y a su vez como resultante de la propuesta dirigida hacia el entorno digital y apegados a la normativa ecuatoriana referente a temas como prueba documental, firmado digital y sellado de tiempo, se desarrolla una propuesta de script en python con diferentes herramientas como Tweepy, OSRFramework, Santoku, y otras librerías propias del lenguaje, para realizar la recolección de evidencia en la red social, a través de un código de programación simplista y comprensible que busca interpretar los datos y que cada elemento pueda ser verificable, haciendo que el proceso sea tan fácil de seguir como sea posible.

Claves: NIST, Prueba Documental, Hash, Testigo online, Evidencia digital, Twitter, Investigación Forense, Python, OSRFramework, Tweepy

ABSTRACT

The objective of the proposed work is to create a forensic system based on NIST 2001 regulations for the collection of digital electronic evidence from the social network Twitter, including the certification of this evidence by means of digital signature and time stamping; thus avoiding the adulteration of the evidence during the prosecution of criminal acts. Considering that the data published in a social network will only exist at one point in time, working on a copy of this data should consider the best practice of having extracted as much information as possible. Through the stages defined for the model that includes two environments, one physical and the digital, various tasks are proposed to be executed in each of these environments, and in turn as a result of the proposal directed towards the digital environment attached to Ecuadorian regulations regarding issues such as documentary evidence, digital signature and time stamping, a python script proposal is developed with different tools such as Tweepy, OSRFramework, Santoku, and other libraries of the language, to collect evidence on the network social, through a simplistic and understandable programming code that seeks to interpret the data and that each element can be verifiable, making the process as easy to follow as possible.

Key: NIST, Documentary Evidence, Hash, Online Witness, Digital Evidence, Twitter, Forensic Investigation, Python, OSRFramework, Tweepy

ÍNDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I
INTRODUCCIÓN

1.1Planteamiento del Problema

Las actividades ilícitas cometidas mediante el uso de sistemas informáticos o dispositivos de comunicación donde la informática es el instrumento para el cometimiento de un delito, se denomina delito informático o *ciberdelito,* estos delitos afectan los datos o información de un usuario considerados bienes jurídicos protegidos (Policía Nacional del Ecuador, 2015). En el COIP se define como sancionar estos delitos, cometidos con el uso de tecnología, los hechos registrados en la Internet pueden ser: estafa, calumnias, suplantación de identidad, fraude a cuentas bancarias, espionaje, entre otros.

Otro delito cibernético es el uso de niños o adolescentes con fines sexuales o pornográficos, para este tipo de delitos definidos como una forma de explotación el COIP sanciona conforme lo establecido en la sección tercera artículos 100, 103 y 104, con una pena privativa de libertad de entre 13 a 26 años.

Según la información publicada por la fiscalía, en marzo del 2015 se investigó una denuncia sobre la existencia de páginas web dedicadas a la comercialización de fotos y videos con contenido sexual de niños y niñas. De la investigación resultante se estableció como ubicación una vivienda del sector de San Rafael, se asoció la dirección IP con el origen de las publicaciones en varias cuentas de diferentes redes sociales. Este hecho derivó en la aprehensión de Víctor G. decomisándosele una computadora y una memoria, bajo la presunción de que su contenido correspondía a pornografía infantil, así como otras evidencias. El caso según los datos publicados por la web de fiscalía aún se encuentra en instrucción fiscal.

Las evidencias digitales poseen como características fundamentales las siguientes: Volátiles, Anónimas, Duplicables, Alterables y Eliminables. Según el perito experto Marques (2018) *"La evidencia digital corresponde a cualquier registro generado o almacenado en un sistema digital que pueda ser utilizado como prueba en un proceso legal."*

Los testigos online permiten recoger evidencias de múltiples elementos como:

- Páginas web, inclusive si estas requieren acceso mediante ingreso de datos como usuario y contraseña.
- Publicaciones de las diferentes redes sociales.
- Correos electrónicos, con sus datos embebidos como destinatario o archivos adjuntos.
- Documentos digitales tales como: facturas digitales, documentos tributarios, contratos, entre otros.

Los testigos online certifican evidencias digitales en una fecha y hora determinada. Este tipo de herramientas basan su funcionamiento en el uso de firmas digitales para acreditar de manera irrefutable una prueba. Gracias a una firma digital tomada por un

tercero de confianza (el testigo online), se podrá autenticar la integridad de la misma y que esta, además, tenga validez en un juicio.

1.1.1 Formulación del Problema

Actualmente, en un proceso de judicialización, la evidencia digital no es recolectada a tiempo o es recolectada sin la correcta metodología que garantice que la misma no va a ser alterada, duplicada o eliminada en el tiempo, debido a la falta de conocimiento de los peritos informáticos, así como de las herramientas que pueden garantizar que dicha evidencia sea almacenada y certificada en línea.

1.2 Objetivos

1.2.1 Objetivo General

Crear un sistema forense apoyado en la normativa NIST 2001 que permita la recolección de evidencia electrónica digital en la red social Twitter e incluya la certificación mediante firma digital y sellado de tiempo, evitando así la adulteración de la evidencia durante la judicialización de hechos delictivos apegado a la norma ecuatoriana.

1.2.2 Objetivos Específicos

- ✓ Realizar un estudio detallando el estado actual en materia de recolección y presentación de la evidencia digital en el país con la evaluación de la documentación obtenida de los repositorios de la Corte Nacional de Justicia y Consejo de la Judicatura estableciendo el panorama actual de las técnicas de recolección de evidencia.
- ✓ Detallar las normas, estándares y protocolos usados localmente y a nivel internacional para la recopilación y manejo de evidencia digital, identificando los procesos y fases más aceptadas en la actualidad determinando una estructura aplicada al entorno ecuatoriano.
- ✓ Establecer el mecanismo forense, mediante el estudio de herramientas open source, definiendo las más adecuadas que ayuden al proceso de certificación del proceso forense digital online de la red social *Twitter* en el entorno ecuatoriano.
- ✓ Evaluar la propuesta metodológica a través de pruebas realizadas en un caso de estudio práctico demostrando la fiabilidad del proceso y herramientas.

1.2.3 Justificaciones

Ante la ley existe información que se encuentra en la web o medios electrónicos que pueden ser presentada como prueba durante un juicio, entre estos se encuentran archivos, rastros de conexiones asociadas a la información IP, datos contenidos en mensajes de texto, correos electrónicos, chats o conversaciones en plataformas de mensajería, fotografías digitales obtenidas de teléfonos móviles, es decir toda aquella información enviada, recibida, almacenada o transferida por redes informáticas incluyendo la gran red, internet.

Actualmente la mayor parte de instituciones del estado otorgan validez a documentos generados en internet como actas de finiquito o registro de contratos del Ministerio de Trabajo, reglamentos internos de empresas, acceso a préstamos hipotecarios o prendarios con confirmación en línea de aceptación de intereses o las consecuencias de caer en mora; de igual forma empresas privadas hacen uso de estos documentos como es el caso del uso de fotografías de siniestros para aplicación de seguros vehiculares, notificaciones de mora por correo electrónico en tarjetas de crédito, etc.

En muchos delitos digitales, los procedimientos para llevar a cabo estudios forenses no son consistentes ni estandarizados varias personas han intentado crear directrices rudimentarias sobre esto los últimos años, pero fueron escritos con un enfoque en los detalles de la tecnología y sin consideración para un proceso generalizado.

En la actualidad el volumen digital de documentación que es procesada se torna inmanejable durante las actividades de obtención de pruebas en el laboratorio, tomando esto en consideración los peritos deben considerar la incorporación y aplicación de técnicas en línea con toda la ayuda que conlleva tener a la mano la tecnología para mitigar el problema de certificación de información.

Ante las situaciones expuestas es necesario que los peritos informáticos tengan acceso a una metodología adecuada para la obtención de pruebas y la respectiva certificación de la autenticidad de las mismas con herramientas de fácil acceso que se encuentren en internet. El presente trabajo se orienta a contribuir con una propuesta a dicha metodología para la inclusión de pruebas certificadas digitalmente, que puedan usarse durante el proceso probatorio del juicio sin que sean menoscabas o excluidas del mismo.

CAPITULO II

Marco Teórico y Estado del Arte

La literatura muestra que el concepto de análisis forense de redes sociales en el área forense digital ha tenido un rápido desarrollo en los últimos años, y hay muchas preocupaciones y problemas asociados con el análisis forense de redes sociales. No existe un modelo aceptado de estándares profesionales o herramientas estandarizadas que el investigador pueda usar en esta área. Es importante explorar las implicaciones de las redes sociales y desarrollar herramientas y pautas estándar para la investigación. Si bien algunas compañías de software privadas ofrecen programas de certificación para análisis forense digital y algunas funciones de investigación forense de redes sociales, no existe un organismo central o una junta disciplinaria que pueda usarse como modelo a seguir para el proceso de investigación. Tener una guía sólida y herramientas que los investigadores forenses puedan seguir será de gran valor para nuestra sociedad.

Analizando las implicaciones éticas y los dilemas en el área forense digital y los desafíos, problemas y oportunidades a los que expertos forenses digitales se enfrentan, es demasiado importante confiar los problemas éticos a cada experto forense individual. Las tecnologías cambian todo el tiempo y las herramientas, que pueden ayudar a los expertos forenses a hacer su trabajo, también tendrán un rápido desarrollo. Si bien es una noticia positiva que las tecnologías ayudarán a los expertos forenses a hacer un mejor trabajo, los expertos forenses digitales también deben desarrollar sus habilidades y mantener la ética y el conocimiento profesional en paralelo con las tecnologías que cambian rápidamente para mantenerse como expertos forenses digitales profesionales.

2.1 Forensia

Técnicas científicas utilizadas en relación en la investigación de delitos, que implica la aplicación de métodos científicos para la obtención de pruebas. (Piccirilli, 2015)

2.1.1 Forensia digital

Forensia digital es una ciencia relativamente nueva, su definición se ha ampliado para incluir al análisis de toda la tecnología digital. Mientras la informática forense se define como una compilación de herramientas y técnicas utilizadas para hallar evidencia en una computadora; la forensia digital está definida bajo métodos científicos contrastados que ayudaran en la preservación, recopilación, validación, identificación, análisis, interpretación, documentación y presentación de evidencia, contenida en fuentes digitales cuya finalidad es promover la reconstrucción de eventos delictivos, también

anticipa operaciones no autorizadas que podrían ser perniciosas en el funcionamiento de los sistemas.

2.1.1.1 Desafíos para la Investigación en Forensia Digital y la Gestión de Casos

En esta sección se analizan los desafíos destacados por los investigadores con respecto a los cuatro elementos fundamentales del proceso de investigación: recopilación, examen, análisis y presentación. Una revisión de los desafíos de la investigación muestra un vínculo cercano con los desafíos de la gestión de casos, especialmente los desafíos relacionados con fuentes heterogéneas, diversidad de datos, Big Data y eficiencias en el manejo del tiempo. Estos desafíos, ya sea por separado o de forma acumulativa, parecen suficientes para crear un retraso sustancial en la investigación y aumentar retrasos e incrementar las horas de trabajo.

a) Fuentes heterogéneas

Las fuentes heterogéneas se han convertido en un aspecto muy crítico a considerar. Los departamentos forenses digitales reciben anualmente una cantidad extraordinaria de dispositivos digitales. Por ejemplo, cada año, la Policía Metropolitana de Londres (MPS-DEFS, 2015) recibe más de 38,000 dispositivos digitales, que un equipo de aproximadamente 80 practicantes debe investigar (Overill, Silomon y Roscoe, 2013). Se requiere que los profesionales forenses obtengan datos correlacionados de diversas fuentes (Mohay, 2005). Las fuentes heterogéneas incluyen, entre otras, computadoras personales y corporativas, servidores, redes, páginas web de redes sociales, IoT, cloud computing y dispositivos integrados.

b) Computación en la nube

"*un modelo informático distribuido a gran escala impulsado por economías de escala, que proporciona la gestión abstracta, virtualizada, dinámicamente escalable y efectiva de la informática, el almacenamiento, la combinación de recursos y servicios, y un modelo a pedido a través de Internet para usuarios externos*" (Tian y Zhao, 2015): es un importante proveedor de datos para las investigaciones. Los dispositivos integrados (por ejemplo, teléfonos inteligentes, teléfonos móviles, relojes inteligentes y dispositivos de salud, etc.) transmiten datos a hogares inteligentes o sistemas de control industrial y crean datos. Las fuentes de datos solo aumentarán enormemente en el futuro.

c) Diversidad de datos

Los examinadores forenses también se enfrentan al desafío de la diversidad en los tipos, formatos y estándares de datos. Los investigadores podrían extraer datos de bases de datos, registros del sistema (por ejemplo, registro de eventos, registro del sistema Linux), registros de software (por ejemplo, registro de instalación, registro de

transacciones), documentos, hojas de cálculo, archivos de respaldo y muchos otros tipos y formatos de archivos. Además, los profesionales forenses no solo están interesados en extraer los datos estándar, sino que también están buscando datos corruptos, cifrados e inválidos para recuperar la mayor cantidad de evidencia posible.

Por lo general, los examinadores están buscando pequeñas piezas de evidencia digital o archivos, la mayoría de los cuales están ocultos en un entorno caótico. También es cierto que el crecimiento y la adopción de nuevas tecnologías (por ejemplo, contenido autodestructivo, comunicación anónima) están aumentando dramáticamente en comparación con el desarrollo limitado de herramientas forenses digitales.

Las herramientas forenses son incapaces de reconocer todos los tipos de datos, una limitación que probablemente se exacerbará con el tiempo (Garfinkel, 2012).

d) Big Data: volumen de evidencia digital

El volumen cada vez mayor de evidencia digital, lo que algunos han llamado "el tsunami digital" (Gogolin, 2010), y la espectacular caída de costos de los discos duros y las capacidades de almacenamiento en estado sólido han creado otro desafío: desempeño de la investigación. El rendimiento tiene implicaciones directas para el flujo de trabajo. El notable crecimiento de la capacidad de evidencia digital ha resultado en una acumulación creciente debido al tiempo requerido para obtener una imagen forense e investigar todos los datos en la evidencia. Debido a estos retrasos, los profesionales forenses están cada vez más presionados para mejorar el rendimiento, y se vuelven altamente dependientes de los "análisis forenses" automáticos para poder investigar pruebas a gran escala rápidamente.

Con el tiempo, tales prácticas disminuirán la capacidad de los investigadores expertos y obligarán a los profesionales forenses a limitar su trabajo a esas herramientas forenses, en lugar de buscar soluciones y técnicas alternativas y creativas. Por lo tanto, es esencial que los departamentos forenses garanticen un equilibrio entre el botón y el análisis forense manual para mantener la base de la experiencia forense de los profesionales. Esto también es crucial para asegurar la calidad y la admisibilidad legal de la evidencia digital extraída (ISO -27037, 2012)

2.1.2 Metodología Forense

El análisis forense digital busca capturar evidencia digital de modo que la integridad forense de los datos se conserve para fines legales. En consecuencia, las políticas forenses deben abordar el requisito tanto para la captura como para la preservación de evidencias considerando los aspectos generales, de dicha evidencia digital planteados en la tabla 1.

Tabla 1 Aspectos a considerar de la evidencia digital

#	Aspectos generales de la evidencia digital	
1	La evidencia digital es desordenada	La evidencia digital no tiene orden y es una forma resbaladiza de evidencia cuyo manejo puede ser complicado.
2	Duplicabilidad y modificabilidad	La evidencia digital puede manipularse de forma fácil planteando nuevos desafíos al investigador digital. La evidencia digital se puede alterar, dañar o destruir fácilmente durante el proceso de recolección.
3	Imposible crear una reconstrucción completa	La evidencia digital es generalmente una abstracción de algún evento u objeto digital. Por lo tanto, todas las piezas del rompecabezas nunca están disponibles, lo que hace que sea imposible crear una reconstrucción completa del crimen.
4	La evidencia digital es circunstancial	La evidencia digital frecuenta ser ocasional dificultando la atribución de los hechos informáticos a un individuo. Es por ello que la evidencia digital solo podra ser considerada como parte en una causa de investigación sólida.
5	Cambios tecnológicos	Con el rápido desarrollo de las tecnologías, siempre hay nuevos ataques y diferentes formas de cometer el delito utilizando nuevas tecnologías. Los investigadores digitales deben seguir la tendencia de la tecnología y comprender el comportamiento de los atacantes en consecuencia con las tecnologías de vanguardia.
6	Sensible al tiempo	La evidencia digital es muy sensible al tiempo. Por ejemplo, la investigación del caso de robo de propiedad intelectual generalmente es urgente, ya que el tiempo de robo es información crucial
7	Cruzar fronteras geográficas y jurisdiccionales	El delito de Internet / red a menudo involucra componentes internacionales y la evidencia puede provenir de diferentes países. Las diferencias geográficas y jurisdiccionales entre cada país harán que el proceso de investigación digital sea mucho más complicado.

Fuente: (Del Valle, 2018)

Una metodología forense debe indicar claramente la funcionalidad forense de un sistema. Por lo tanto, en lugar de especificar lo que está permitido y lo que no está permitido, una metodología forense especificará los eventos que deben manejarse y los datos que rodean los eventos que deben conservarse. Los eventos que no se incluyen en esta lista no serán valiosos y los datos de estos incidentes no deberán conservarse por razones forenses. En consecuencia, una política forense divide el espacio de todas las posibles infracciones o actividades delictivas en un conjunto de eventos, que requieren acción forense, y aquellos que no lo hacen.

Un ejemplo de una metodología forense simple para un sistema comercial aborda las violaciones de seguridad de la red, los mecanismos de cumplimiento de esta metodología incluyen la forma de preservación de los registros de IDS, firewall y enrutadores, además de los registros del servidor web para el servidor web público. La forma de archivar dichos registros y el detalle de almacenamiento definiendo el período de tiempo configurable.

El siguiente proceso ayuda a definir una metodología forense:

a) Identificar los activos digitales que tienen valor.
b) Realizar una evaluación de riesgos para pérdidas potenciales y amenazas para esos activos.
c) Eliminar activos que no justifiquen el esfuerzo de recolección de evidencia.
d) Identificar los datos asociados necesarios para estos activos junto con las necesidades de recolección y almacenamiento.

e) Escribir la política forense en términos de activos digitales, eventos forenses, recolección de datos y almacenamiento.
f) Asegurar que se apliquen políticas forenses adecuadas.

2.1.2.1 Modelos de Investigación Forense Digital

Se han propuesto muchos modelos de proceso de investigación forensia digital pero todavía no ha surgido un modelo único como estándar global para la investigación (Pollitt, 2007). Los diversos modelos propuestos para la investigación generalmente consisten en los siguientes cuatro elementos fundamentales (Baryamureeba y Tushabe, 2004, Harrell, 2010):

1. Adquisición - Recolector
2. Identificación - Examinador
3. Evaluación - Analizador
4. Presentación

La recolección o adquisición es el proceso de usar procedimientos estandarizados y aceptados para mantener un duplicado de la evidencia digital. El examen o la identificación es el proceso de una búsqueda sistemática exhaustiva de evidencia electrónica relacionada con el presunto delito. El análisis o evaluación es el proceso en el que el examinador cuantifica y reconstruye fragmentos de datos para llegar a conclusiones lógicas basadas en la evidencia. La presentación es el proceso para resumir los hallazgos y aclarar las conclusiones para la admisión de evidencia.

En la práctica, puede haber cientos de variaciones del proceso de investigación, y cada organización posiblemente desarrolle sus propios procedimientos basados en los requisitos tecnológicos de la investigación. Debido a la variedad de delitos digitales, los investigadores probablemente seleccionarán el marco aplicable caso por caso, a menudo revisando la metodología para satisfacer las necesidades del caso (Sanya-Isijola, 2009). A continuación, se examinan algunos de los modelos de investigación propuestos y publicados. Ver la Tabla 2 a continuación.

Tabla 2 Modelos de investigación o marcos de referencia

Modelo o Marco de Referencia	Año	Investigadores	# Fases
Proceso Forense	2006	Kent, Chevalier, Grance y Dang	4 Procesos
Marco de Referencia en Investigacion	2006	Kohn, Eloff y Oliver	3 Estados
Modelo de proceso de clasificación en el campo cibernético	2006	Rogers, Goldman, Mislan, Wedge y Debrota	
Modelo FORZA para Forensia	2006	Leong	
Modelo de proceso común para incidentes e informática forense	2007	Freiling y Schwittay	4 Fases
Modelo de adquisición de datos en vivo y estático	2009	Perumal	
Modelo de reconstrucción relacional	2011	Preston, Imafidon y Ademu	
Big Data Framework	2016	Adedayo	

Fuente: (Sanya-Isijola, 2009)

Proceso Forense (PF)

Kent, Chevalier, Grance y Dang (2006) introdujeron un modelo de investigación de cuatro etapas llamado Proceso Forense (PF) con cuatro etapas que incluyen: (1) recopilación, (2) examen, (3) análisis y (4) informes. El proceso forense transforma los medios en evidencia digital mediante la extracción de datos en un formato compatible con herramientas forenses. El proceso transforma los datos en información a través de la fase de análisis, y en evidencia a través de la fase de informe.

Marco de Referencia en Investigacion (FI)

Kohn, Eloff y Oliver (2006) propusieron un modelo de tres etapas llamado Marco de Investigación (FI) que se basa en experiencias previas de investigadores en el campo. FI identifica tres etapas como requisitos mínimos para calificar bajo la definición de "forense". Estas tres etapas son: (1) preparación, (2) investigación y (3) presentación. Es importante destacar que FI destaca la necesidad de basar el marco en los requisitos legales relevantes antes del proceso de investigación, y la importancia de la documentación durante el proceso de investigación.

Modelo de proceso común para incidentes e informática forense (CPMICF)

El marco más reciente en esta revisión es uno para realizar pesquisas de delitos cibernéticos que fue propuesto por Freiling y Schwittay (2007) y lo llamaron el Modelo de Proceso Común para Incidentes e Informática Forense (CPMICF). Este es un proceso de investigación de delito cibernético que combina la respuesta a incidentes y la informática forense. Tiene como objetivo mejorar la investigación a través de un modelo basado en análisis que consta de las siguientes cuatro etapas: (1) Preparación previa al incidente, (2) Preanálisis, (3) Análisis y (4) Postanálisis.

Otros modelos de investigación

Otros modelos de investigación se enfocan en aspectos del proceso de investigación que podrían mejorarse o se enfocan en extender la aplicación del proceso de investigación a demandas tecnológicas únicas. Por ejemplo, Rogers (2006) propone en su Modelo de proceso de triaje de campo forense por computadora (CFFTPM), que se centró en un enfoque de campo para la identificación, análisis e interpretación en un corto período de tiempo, y abandonó el examen de laboratorio en profundidad o imagenología forense. Leong (2006) propuso el Modelo FORZA, un marco forense en la nube que no sigue los elementos típicos de investigación, sino que es un marco técnico dependiente. Asimismo, Perumal (2009) propuso un modelo que destaca la importancia de la adquisición de datos en vivo y estáticos en el proceso de investigación. Ademu (2011) propone el Modelo de Reconstrucción Relacional, que aborda la necesidad de reconstrucción e interacción, destacando la interacción regular de todos los recursos de investigación. Más recientemente, Adedayo (2016) propuso un Big Data Framework que contribuye a los marcos ya existentes mediante la introducción de técnicas más eficaces de recolección, preservación, análisis y presentación.

Se sugieren muchos procesos forenses digitales. Todos los procesos descritos se basan en la pericia de los autores y cada autor destaca sus perspectivas. Está claro que todos

los procesos sugeridos tienen una base legal relevante que es un aspecto importante a considerar antes de establecer un marco porque afectará todo el proceso de investigación. Además, los procesos muestran que deben tener los requisitos forenses básicos, como preparación, investigación y presentación. El objetivo de todos esos procesos y marcos sugeridos es establecer una guía clara de investigación.

2.1.3 ISO / IEC 27037: 2012 Normativa Internacional orientada a análisis forense digital

Esta normativa aporta las pautas para identificación, recopilación, adquisición y preservación de evidencia digital, el estándar fue publicado en 2012 y confirmado en 2018.

Acorde a esta normativa la evidencia digital tiene los siguientes fundamentos: relevancia, confiabilidad e idoneidad. Los principios básicos se identifican en la Figura 1 y se detallan a continuación:

a) Aplicación de Métodos

La evidencia digital será adquirida de una forma no intrusiva guiándose con el principio de preservación de la originalidad y respaldo de la información en forma de copias de seguridad.

b) Proceso Auditable

Las técnicas usadas conjuntamente con la documentación deben ser validados y contrastados bajo criterios de viabilidad técnica, proporcionando indicios y evidencias del trabajo ejecutado con sus respectivos resultados.

c) Proceso Reproducible

La metodología y procesos ejecutados serán reproducibles, verificables e impugnables por otros especialistas entendidos en la materia, quienes corroboraran y respaldaran las diligencias efectuadas.

d) Proceso Defendible

Se mencionarán todas las herramientas usadas y las mismas deben ser validadas para el cumplimiento del objetivo al cual han sido destinadas.

Figura 1 Fases de actuación pericial según ISO 27037

Fuente: (ISO/IEC 27037, 2012)

La evidencia digital se obtiene de la información de los dispositivos digitales y será interpretada durante el juicio de distintas maneras dependiendo de la jurisdicción; este estándar internacional aborda una metodología que permitirá ratificar la integridad y autenticidad de la evidencia digital, proporcionando orientación al detalle sobre la identificación, formas de recolección y almacenamiento, métodos para transporte y forma de preservación de pruebas electrónicas. Las etapas del procedimiento según la normativa ISO/IEC 27037 son:

a) Identificación

Primer proceso del tratamiento de la evidencia en el que se ubica e identifica el contenido potencial o elementos de prueba, en los estados físico y lógico, según le corresponda a cada evidencia.

b) Recolección y/o Adquisición

Segundo proceso, comprende el acopio de dispositivos (incautación) y recolección de documentación donde se sospeche se contenga información de la evidencia deseada, o la adquisición mediante copia del contenido de los diferentes dispositivos.

c) Conservación/Preservación

La cadena de custodia garantiza la originalidad e integridad de la prueba, es decir la evidencia debe ser preservada en su totalidad para que pueda ser admisible como elemento de prueba considerándose que todos los procesos fueron dirigidos para mantenerla original e integra.

La normativa se encuentra diseñada para tratar evidencia en los entornos mencionados a continuación:

- Computadoras
- Dispositivos conectados en red
- Dispositivos periféricos
- Medios de almacenamiento

- Sistemas de alta disponibilidad
- Dispositivos móviles

2.1.4 Enfoque NIST para probar herramientas forenses informáticas

Debido a la necesidad crítica de las fuerzas del orden público de garantizar la confiabilidad de las herramientas forenses digitales, agencia del Departamento de Comercio de los Estados Unidos representado por el Instituto Nacional de Estándares y Tecnología, ha propuesto enfoques para medir la viabilidad de las herramientas forenses informáticas. NIST ha resumido el enfoque para probar las herramientas forenses informáticas. La Figura 2 ilustra el enfoque utilizado según lo presentado por NIST para probar herramientas forenses informáticas

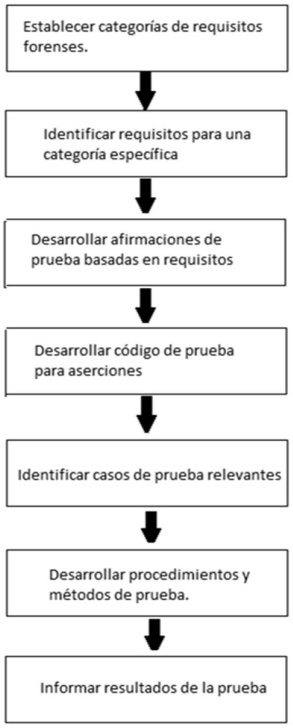


Figura 2 Metodología analítica para pruebas de herramientas forenses

Fuente: NIST, 2001

El enfoque de NIST tiene un vínculo directo con la investigación propuesta, ya que este enfoque considera no solo la precisión y confiabilidad de la funcionalidad del software sino que también considera los estándares internacionales existentes.

Las herramientas de software son solo parte del proceso forense, y el examinador debe tener el conocimiento suficiente para ir a un nivel mucho más allá del de un usuario simple con las mismas herramientas. Bryson y Stevens (2006). Al evaluar la capacidad de las herramientas con los procesos forenses básicos, este método puede ayudar a los investigadores a evitar el riesgo de pérdida de su credibilidad mediante el uso de herramientas inapropiadas.

2.2 Estrategias enfocadas al Ciberespacio

Para sentar las bases en el entorno digital los estados han definido estrategias y marcos normativos referentes a Ciberseguridad y Ciberespacio

2.2.1 Convenio de Budapest

Tratado internacional que aborda definiciones de ciberdelincuencia iniciado en el consejo de Europa en Estrasburgo y firmado en noviembre de 2001, orientado a definir la cooperación entre naciones para enfrentar los delitos informáticos en las infraestructuras y el internet mediante técnicas de investigación y cooperación. Se ratificó en octubre de 2010 con la firma de 30 estados. Dentro de su contenido se ha definido términos relacionados a los sistemas y datos informáticos, definiciones para proveedores de servicios como datos referentes al tráfico, uso de dispositivos, también pone en escena los términos asociados al acceso ilícito a datos o interceptación ilícita de los mismos, ataques de la integridad de datos y sistemas, fraude informático, delitos asociados a la pornografía infantil, delitos asociados a infracciones de la propiedad intelectual, también analiza en el ámbito del derecho procesal las condiciones para el conservación de datos informáticos, conservación de datos relativos al tráfico, confiscación de datos informáticos almacenados, interceptación de datos relacionados a contenido, y dirime los principios generales que regirán la cooperación internacional. (Consejo de Europa, 2001)

2.2.2 Ciberseguridad en la Constitución de la República del Ecuador

A fin de asociar el entorno de la ciberseguridad a la constitución y los deberes del Estado, a continuación, se mencionan los artículos a ser considerados cuando se habla de seguridad en el ámbito digital, “garantizar a sus habitantes el derecho a la seguridad integral” (Art.3, núm. 8); “al acceso universal a las tecnologías de información y comunicación” (Art. 16, núm. 2); “garantizar la seguridad humana... prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos.” (Art. 393).

2.2.2.1 Normativa existente para medios electrónicos en Ecuador - Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial Suplemento 557, emitida en el año 2002 contempla la existencia y uso del medio electrónico en las relaciones comerciales y de individuos en la sociedad ecuatoriana, legalizando aspectos como: reconocimiento de mensajes de datos, firmas electrónicas, autoridades competentes para la certificación electrónica de documentos, derechos al usuario de herramientas digitales, prueba y notificación electrónicas. Las pruebas digitales según lo ha establecido en esta Ley son instrumentos que servirán para exponer vínculos de comercio electrónico.

Señala disposiciones específicas para los medios electrónicos contemplando temas como emisión, recepción, aspectos referentes a la validez, etc.; de forma general se trata el desarrollo de internet y sus fines comerciales, educativos o culturales, el enfoque de

integración al empleo de medios electrónicos, como se regularán los actos civiles y transaccionales mediante el uso de la Red (internet). Esta ley tiene como objetivo regularizar la utilización de documentos electrónicos o mensajes de datos como análogos de documentos escritos que tengan soporte físico o respaldo en papel, para ello se utilizará obligatoriamente firmas electrónicas en lugar de manuscritas. Se establecen disposiciones que incluyen a los mensajes de datos y su inclusión como prueba en casos de juicio, el artículo 2 detalla los requisitos para que sean valorados como documentos electrónicos veraces. Se determina que los requisitos que deberán cumplir los documentos electrónicos y mensajes de datos son: accesibilidad, conservación o preservación e integridad.

a) Accesibilidad, el contenido íntegro de los documentos electrónicos y mensajes de datos podrá ser recuperado en cualquier momento.

b) Conservación y preservación de los datos correspondientes a la forma original, contenido de la información de envío, tipo de archivo, fecha y hora de realización, emisor, receptor, forma de procesamiento, forma de generación y medio de recepción.

c) Integridad, sustentar la inalterabilidad y totalidad de la información firmando electrónicamente.

Al encontrarse firmado electrónicamente el documento electrónico será considerado medio de prueba, caso contrario será considerado como un indicio, para que pueda ser usado y tener efecto dentro de un proceso judicial debe ser sometido a un examen pericial que lo certifique.

Conforme a lo descrito en el artículo 4 el documento desmaterializado, la copia certificada, el mensaje de datos y la información original, serán certificados con un Notario o similar mediante la firma electrónica o procedimiento autorizado, si las leyes lo determinan conforme al caso.

En el caso de que la ley lo exija o las partes lo acuerden, certificaran electrónicamente ante Notario o autoridad competente el documento desmaterializado mediante la inclusión de la firma electrónica, esta desmaterialización descrita en el artículo 5 comprende de un documento físico o electrónico solicitando la desmaterialización y ratificando la equivalencia entre el original y el desmaterializado. (Jara, 2010).

Firma electrónica

Medio de identificación personal que se encuentra constituido como un conjunto de datos de carácter electrónico, establecidos junto a otros datos o apuntados con ellos.

Sellado de tiempo

Acotación electrónica que se encuentra incorporada a un mensaje de datos, firmada electrónicamente, cuyos requisitos mínimos son: fecha, hora e identidad de la persona que apostilla dicha anotación

2.2.2.2 Documento electrónico en el proceso judicial

El Código Orgánico General de Procesos (COGEP, 2015) establece los instrumentos que servirán ante cualquier órgano jurisdiccional, en este se señala al documento público como aquel otorgado ante notario e incorporado en un registro público denominándolo como escritura pública; "*los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente."* Sin embargo, falta la definición adecuada para la interpretación de los medios electrónicos, es inexistente la definición de presentación, valoración, garantía de documentos digitales para la defensa en un proceso penal.

El artículo 54 de la Ley de Comercio Electrónico señala que se debe anexar el soporte informático o la transcripción de forma física del documento electrónico para ser incluido en el proceso judicial, también lo señala el COGEP en su artículo 159 indicando que la prueba electrónica se anunciará y se adjuntará al inicio del proceso judicial. Durante el juicio también se podrá incluir pruebas obtenidas de la desmaterialización de cualquier documento digital, por medio de la certificación de autenticidad signada por un Notario conforme lo determina el artículo 5 de la Ley, es decir el Notario certificará la autenticidad del documento electrónico original con una copia física (en papel).

Los documentos electrónicos se materializan es decir se integran al proceso judicial con la revisión durante la audiencia de juicio de los elementos encontrados en la página web implicada, o el dispositivo de almacenamiento de datos y su transcripción física (en papel), o mediante la certificación de copias ante un notario. (Ley Notarial, 2018)

Prueba documental

Durante el proceso judicial se exponen los hechos o circunstancias que se presentaron durante el ilícito, para exponer estos hechos se presentan las pruebas que durante esta etapa procesal podrán ser afirmados o negados por la contraparte. La prueba documental será incluida en la demanda, como parte de respuesta de la demanda, reprimenda y respuesta a la reprimenda. (COGEP, 2015)

El profesional del derecho reunirá las pruebas que serán presentadas con su demanda, es decir se integraran todos los documentos o diligencias que aporten al caso.

Prueba pericial para materialización de documentos

El Consejo de la Judicatura facultará la actuación de personas con experiencia en determinados ámbitos a los que se les denominará perito, en el ámbito judicial. El perito aportará con pruebas periciales ante el Juez, es decir la prueba pericial proviene de la opinión de personas expertas en determinada materia que concierne a los hechos del juicio. Es necesario el aporte de las pruebas periciales dado que el Juez no posee los conocimientos científicos, requeridos para la apreciación de toda la información que se plantea durante el litigio.

Conforme a lo establecido en el artículo 224 del COGEP la prueba pericial es entonces el hecho mismo, los peritos se encargan de explicarla y desglosan el contenido del informe pericial.

Se considerará al informe pericial realizado como prueba siempre que exista la declaración de su autor en audiencia de juicio, conforme a lo detallado en el artículo 222 del COGEP no será considerado en el caso de no comparecencia del perito.

2.2.2.3 Admisibilidad de la Prueba según el Código Orgánico General de Procesos

El COGEP (2015) en su contenido y acorde a lo indicado en el artículo 160 establece que la admisibilidad de la prueba se da cuando reúne los requisitos de pertinencia, utilidad, conducencia y será practicada acorde la ley. Se manifestará la improcedencia de la prueba si se determina que se ha obtenido con violación a la Constitución o la ley.

La prueba obtenida a través de simulación, dolo, fuerza física, fuerza moral o soborno será ineficaz, de igual manera la prueba actuada sin oportunidad de contradecir.

Acorde al contenido del artículo 227 la prueba pericial tendrá como propósito que expertos acreditados verifiquen hechos u objetos materia del proceso, las partes podrán presentar un informe del hecho o materia elaborado por el experto acreditado como perito.

2.2.2.4 Principales Delitos definidos en la normativa jurídica de Ecuador que pueden ser cometidos a través de Redes Sociales

Del análisis al Código Orgánico Integral Penal (COIP) contenido en el registro oficial del 10 de febrero de 2014 se determinan las infracciones y sanciones de los delitos informáticos en Ecuador, contenidos en los capítulos Segundo con un resumen detallado en la Tabla 3, capítulo Tercero resumido en la Tabla 4, capitulo Sexto detallado en la Tabla 5 y Séptimo resumido en la Tabla 6.

Tabla 3 Infracciones y Sanciones contenidas en el capítulo Primero del COIP

SECCION		ARTICULO	CONTENIDO	SANCION PRIVATIVA DE LIBERTAD
Tercera	Diversas formas de explotación	97	Publicidad de tráfico de órganos	7 – 10 años
		100	Explotación sexual de personas Si la conducta descrita se lleva a cabo sobre personas de grupos vulnerables o si entre la víctima y la persona agresora se mantiene o se ha mantenido una relación de pareja, familiar, de dependencia económica, laboral o de autoridad.	13 – 16 años 16 – 19 años
		103	Pornografía con utilización de niñas, niños o adolescentes	13 – 16 años

			Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable Si la persona infractora tiene grado de consanguinidad, es tutor, representante legal, o pertenezca al entorno íntimo de la familia.	16 – 19 años 22 – 26 años
		104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	10 – 13 años
Cuarta	Delitos contra personas y bienes protegidos por el Derecho Internacional Humanitario	127	Reclutamiento de niños, niñas y adolescentes	10 – 13 años

Fuente: Autor

Tabla 4 Infracciones y Sanciones contenidas en el capítulo Segundo del COIP

SECCION		ARTICULO	CONTENIDO	SANCION PRIVATIVA DE LIBERTAD
Segunda	Delitos contra la integridad personal	154	Intimidación	1 – 3 años
Cuarta	Delitos contra la integridad sexual y reproductiva	166	Acoso sexual Cuando la víctima sea menor de dieciocho años de edad o persona con discapacidad La persona que solicite favores de naturaleza sexual que atenten contra la integridad sexual de otra persona	1– 3 años 2 – 5 años 6 meses – 2 años
		168	Distribución de material pornográfico a niñas, niños y adolescentes	1 – 3 años
		173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1 – 3 años
		174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7 – 10 años
Quinta	Delitos contra el derecho a la igualdad	177	Actos de odio Si los actos de violencia producen la muerte de una persona	1 – 3 años 22 – 26 años
Sexta	Delitos contra el derecho a la intimidad personal y familiar	178	Violación a la intimidad	1 – 3 años
		179	Revelación del Secreto	6 meses – 1 año
Séptima	Delito contra el derecho al honor y buen nombre	182	Calumnia	6 meses – 2 años
Novena	Delitos contra el derecho a la Propiedad	185	Extorsión	3 – 5 años
		186	Estafa	5 – 7 años
		192	Intercambio, comercialización o compra de información de equipos terminales móviles	1 – 3 años
		194	Comercialización ilícita de terminales móviles	
		203	Comercialización de bienes de uso	3 – 5 años

			policial o militar hurtados o robados	
Decima	Delitos contra el derecho a la identidad	212	Suplantación de identidad	1 – 3 años

Fuente: Autor

Tabla 5 Infracciones y Sanciones contenidas en el capítulo Tercero del COIP

SECCION		ARTICULO	CONTENIDO	SANCION PRIVATIVA DE LIBERTAD
Tercera	Delitos contra la seguridad de los activos de los sistemas de información y comunicación	229	Revelación ilegal de base de datos	1 – 3 años
		230	Interceptación ilegal de datos	3 – 5 años
		231	Transferencia electrónica de activo patrimonial.	3 – 5 años
		232	Ataque a la integridad de sistemas informáticos. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana	3 – 5 años 5 – 7 años
		233	Delitos contra la información pública reservada legalmente La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información	5 – 7 años 3 – 5 años
		234	Acceso sin consentimiento a un sistema informático o de telecomunicaciones	3 – 5 años

Fuente: Autor

Tabla 6 Infracciones y Sanciones contenidas en el capítulo Sexto y Séptimo del COIP

CAPITULO		ARTICULO	CONTENIDO	SANCION PRIVATIVA DE LIBERTAD
Sexto	Delitos contra la seguridad pública	354	Espionaje	7 – 10 años
		348	Incitación a discordia entre ciudadanos	1 – 3 años
		363	Instigación	6 meses – 2 años
Séptimo	Terrorismo y su financiación	366	Terrorismo	10 – 13 años

Fuente: Autor

2.2.3 Estudios de metodologías forenses digitales en Latinoamérica

A nivel regional la problemática de metodologías forenses ya ha sido tratada y diferentes metodologías puestas en práctica para diversos entornos y sistemas operativos, a continuación, se listan varias investigaciones que abordan el tema.

"Los Laboratorios Informáticos Forenses deben estar preparados para poder abordar todas las competencias, en pos de garantizar una correcta reconstrucción del hecho investigado y cumpliendo con los principios del manejo de la evidencia digital establecidos en las normas ISO 27037 como son la relevancia, la confiabilidad y la

suficiencia" (Semprini, 2016, p.1). En este trabajo se aborda la importancia de los dispositivos tecnológicos usados para el estudio de la evidencia digital bajo el estándar ISO 27037, haciendo énfasis en las etapas de análisis con aplicación de métodos, técnicas y herramientas forenses que faciliten la obtención de información asociada a dispositivos con sistema operativo Windows.

En textos adoptados para la realidad Argentina, se propone las condiciones a considerarse para la obtención de las pruebas digitales y su uso en procedimientos judiciales; en base a la introducción de conceptos básicos y su relación con los principios de legalidad, libertad probatoria y el derecho a la intimidad. Abordando el *Cybercrimen* y la Convención de Budapest, analizando también los mecanismos de constitución del hecho (nube, correos electrónicos, celulares, redes sociales, imágenes digitales) y los tipos de pruebas que pueden obtener los expertos. "La relevancia social que presenta este tema, es para dar certeza jurídica a las partes intervinientes en los procesos o al estado para ejercitar el ius puniendi, que tendrá como interés la manera en que el dato electrónico o digital puede ser incorporado al proceso para probar la existencia del hecho" (Del Valle, 2018, p.8).

En un resumen realizado por la Asociación de Derechos Civiles (ADC, 2018), sobre el estado actual de la investigación forense digital en América Latina, se aborda la situación en el uso de herramientas de recolección de prueba digital en países como Argentina, Chile, Colombia y México; y la adherencia de dichos estados al Convenio de Budapest dando una imagen de lo que actualmente sucede en la región y las líneas de trabajo que especialistas de estos países usan para la práctica investigativa.

"El reto principal al que se enfrentan los investigadores en aplicaciones web, en la arquitectura más común cliente-servidor, es que gran parte de las buenas prácticas y guías dentro del análisis forense en entornos web, están enfocadas en su mayoría del lado del servidor, surgiendo otra problemática acerca de la ubicación de la información, puesto que en aplicaciones que alojan sus datos en la nube o en un servidor desconocido; la identificación, recolección y organización de la evidencia, en gran medida, depende del proveedor del servicio" (Coronel, 2018, p.17). El enfoque de este trabajo es hacia la propuesta de una metodología para la identificación, recolección, preservación, análisis y presentación de evidencia digital creada en un ordenador local mediante una aplicación web, detallando las herramientas y parámetros a ser utilizados durante la aplicación de la misma.

"El hecho de que la información haya dejado de estar en papel para almacenarse digitalmente en cualquier medio tecnológico deriva en Pericias Informáticas que son muy específicas y a la vez complicadas en la obtención de la evidencia" (Loarte, 2018, p.3). Este estudio brinda a los Peritos Informáticos referencias a normas, buenas prácticas internacionales especializadas que conlleven a la judicialización de delitos informáticos en equipos con sistema operativo MAC OS X.

2.3 Redes Sociales

Una red social anima a sus usuarios a comunicarse con otros usuarios que son parte de esa red, y crea un entorno para que los usuarios compartan contenido y se conecten a través de sus intereses similares. Muchos sitios de redes sociales ofrecen diferentes maneras para que los usuarios se comuniquen entre sí: mensajería instantánea, correo electrónico, video en tiempo real o chat de voz. Uno de los objetivos y, por lo tanto, una característica de una red social es un sentido de comunidad entre los usuarios. Los miembros de un sitio pueden distribuir y compartir su contenido entre sí, o pueden ser capaces de unirse a través de similares intereses y hobbies.

2.3.1 Evidencia almacenada en una red social

La tipología de datos encontrados en una red social corresponde a cinco categorías (Mumba y Venter, 2014), definidas a continuación:

a) Datos de servicio: datos que deben proporcionar los usuarios para continuar utilizando el sitio de la red social, ejemplos de los datos son el nombre del usuario, la fecha de nacimiento y los números de teléfono, etc.
b) Datos divulgados: cualquier dato publicado por el usuario de la cuenta, se puede presentar en cualquier formato, como imágenes, videos, enlaces, comentarios y estado de actualización.
c) Datos confiados: cualquier dato publicado por otra persona en una cuenta de usuario (amigos, suscriptores, seguidores, etc.), la diferencia entre los datos divulgados y los datos confiados es que el usuario no tiene control sobre los datos confiados una vez que se ha publicado.
d) Datos incidentales: los datos incidentales son lo que otras personas escriben en su cuenta sobre un usuario en particular. Los datos pueden ser cualquier contenido, imágenes, mensajes, videos, etc.
e) Datos de comportamiento: los datos recopilados por el sitio acerca de las prácticas y los hábitos de los usuarios. Grabando sus actividades, elecciones, hábitos regulares, puntos de vista, etc.

2.3.2 Fuentes de Datos en las redes sociales

La evidencia se puede difundir en una variedad de lugares, algunos de los cuales pueden ser inaccesibles. Hay muchos casos en los que las personas han utilizado las redes sociales en línea para revelar su admisión de cometer ofensas. Las redes sociales que las personas divulgan en línea también tienen los vínculos con otros que influyen en su comportamiento y aquellos con quienes ejercen influencia. Por supuesto que hay muchos puntos fuertes de la relación dentro de cualquier red social en línea, pero la naturaleza de la confianza y la aparente eliminación de las barreras habituales a la expresión permiten la divulgación de información importante.

Los tipos de evidencia pueden variar de una red social a otra dependiendo de su arquitectura y las características proporcionadas.

Las diferentes fuentes de datos que se pueden recopilar de las redes sociales en línea, se puede agrupar en cuatro áreas (Zainudin, Merabti y Jones, 2010)

i) Huella social con otros usuarios, incluidas listas de amigos, grupos conectados, que corresponden a los seguidores y usuarios seguidos.
ii) Métodos de comunicación entre los usuarios dentro del sitio, por ejemplo. Mensajes privados, mensajería instantánea, Comentarios, *likes*, comunicaciones grupales, y eventos.
iii) Fotos y videos publicados por los usuarios, y que fueron etiquetados en las imágenes, indicando tiempos de las actividades: cuando un usuario específico inició sesión en el sitio y qué tipo de actividades fueron realizado en un marco de tiempo específico.
iv) Las aplicaciones utilizadas por el usuario, así como la identificación del propósito de las aplicaciones y la información que se puede extraer.

2.3.3 Problemas en la forensia de redes sociales

Además de los problemas éticos, quedan muchos otros desafíos en las investigaciones forenses digitales en entornos de redes sociales. La siguiente sección resumirá algunos problemas y cuestiones asociadas con el análisis forense de las redes sociales:

Problema 1: Admisibilidad de evidencia

Identificar al autor de la publicación de comunicación y localizar evidencia potencial de redes sociales es muy difícil debido a la red distribuida de la red social. También es difícil encontrar todo en la red social, ya que la evidencia puede almacenarse en múltiples redes. Encontrar evidencia completamente precisa puede ser problemático y el riesgo de que falten datos es más común en el análisis forense de las redes sociales.

Problema 2: Interpretación o Percepción del investigador

El análisis de la red social brindará a los investigadores diferentes puntos de vista, diferentes pistas sobre qué mirar, cómo mirarlo y cómo se relaciona con otros. Es común interpretar cosas diferentes de una red social. Los investigadores podrían interpretar evidencia y presentar evidencia desde diferentes puntos de vista, y pueden presumir que la información que encontraron en los sitios de redes sociales está relacionada con actividades delictivas.

Problema 3: Diferencias jurisdiccionales

Como las redes sociales están sucediendo en el ciberespacio, la persona que cometió un delito a través de redes sociales puede estar ubicada en un país diferente al de la víctima. El Investigador forense digital encontrará dificultades si se publican pruebas de diferentes áreas jurisdiccionales.

Problema 4: Herramientas forenses de redes sociales

Se han desarrollado varias herramientas forenses digitales y de redes forenses para recopilar evidencia potencial del medio digital. Sin embargo, la recopilación de evidencia en redes sociales sigue siendo uno de los problemas más desafiantes en el

análisis forense. Cada herramienta está disponible individualmente y no hay muchos paquetes de software que estén específicamente diseñados para forensia de las redes sociales. Preservar adecuadamente la evidencia en la red social es la parte más crucial del proceso de investigación, que puede ser un desafío debido a las características sociales de las redes. No hay herramientas estándar todo en uno que los investigadores forenses puedan seguir. Para recopilar y analizar adecuadamente las pruebas, es necesario contar con herramientas desarrolladas para la investigación forense de las redes sociales, de modo que el investigador forense pueda recopilar y proporcionar evidencia relevante, que es admisible ante el tribunal de justicia.

Problema 5: Falta de estándares

Según el diccionario de Oxford, estándar significa algo utilizado como medida, norma o modelo en evaluaciones comparativas. La idea de tener un estándar es establecer un protocolo que todos entiendan y puedan seguir. Con la explosión del crimen digital, el análisis forense digital es cada vez más relevante. La disciplina forense digital se ha desarrollado bastante rápido, pero hasta la fecha, se ha desarrollado muy poca estandarización internacional con respecto a los procedimientos o la gestión. Es necesario elaborar un código de ética internacional estándar adecuado con las herramientas adecuadas para la investigación forense de redes sociales. También es necesario estandarizar la interacción con las áreas legales pertinentes, y el código de ética profesional contribuirá en gran medida a que nuestra sociedad clarifique la verdad sustantiva, lo que también puede minimizar los problemas y las cuestiones en el análisis forense de las redes sociales.

2.3.4 Estudios con enfoque en metodologías forenses aplicados a redes sociales

Se han logrado ubicar varios trabajos relacionados a la temática a explorarse a nivel mundial, a continuación, detallados, en contenido y fecha de realización.

Mazzini y Huber (2012) en su estudio discuten las fuentes de datos importantes y los métodos analíticos para el análisis forense de las redes sociales, muestran cómo se pueden evaluar las fuentes de datos de manera automatizada sin la ayuda de los operadores de redes sociales. Demostrando su viabilidad mediante un estudio de caso de Facebook. Estos autores presentaron otro enfoque en el mismo año para cosechar datos probatorios de sitios de redes sociales.

Con millones de usuarios alrededor del mundo, la extracción de datos forenses de las redes sociales se ha transformado en un importante problema de investigación. (Keyvanpour, 2014). Sin embargo, la recopilación de datos forenses está estrechamente relacionada con los operadores de redes sociales, lo que conduce a complicaciones relacionados con la integridad y la compatibilidad de los datos. Este artículo discutió el uso de forenses en redes sociales como medidas de ciberseguridad e identificó los problemas relacionados con la seguridad. Sin embargo, no discutió ningún problema técnico y legal relacionado con las redes sociales forenses.

Hubert (2014) en su trabajo sugiere algunas técnicas prácticas para recopilar, guardar y presentar evidencia de sitios de redes sociales que apoyen a la construcción de una línea

de tiempo del evento y permitan al investigador explicar lo que sucedió a la alta gerencia, a las agencias legales y policiales.

Los servicios de redes sociales (SNS) contienen información diversa, como conversaciones entre usuarios, información de ubicación del usuario, red personal y psicología del usuario. Se puede recopilar evidencia digital a través de un proceso forense digital apropiado, siendo esta información diversa, como la lista de amigos de un usuario de la red social, conversaciones y relaciones personales considerada como evidencia digital. Este documento sugiere un proceso forense digital para dispositivos digitales que utilizan redes sociales. Para analizar la evidencia digital este método propuesto se compone de procesos para clasificación de dispositivos digitales, recolección de evidencia digital y análisis. (Jang y Kwak, 2015).

2.3.5 Estudios de aspectos legales en relación al contenido de redes sociales en el entorno ecuatoriano y su valoración en etapas procesales.

Existen varios criterios acerca de la valoración de la prueba en las etapas de investigación previa y etapas procesales, en varios trabajos se ha dilucidado esta definición dando relevancia a la definición contenida en el Código Orgánico Integral Penal.

Los criterios de valoración determinados en el Código que debe cumplir la prueba documental con contenido digital, considerando la cadena de custodia y su influencia en un dictamen dada la validez probatoria son tratados en el trabajo de Dunn (2019) donde se indica que “aquellos elementos de convicción recopilados en la fase pre-procesal penal llamada investigación previa y los elementos de convicción recopilados en la primera Etapa procesal penal llamada Instrucción Fiscal se anunciarán como prueba en la audiencia de evaluación y preparatoria a juicio en caso de acusación. Tomarán el nombre de pruebas dentro de la etapa de juicio donde deberán ser debidamente practicadas” (p.17)

Los elementos por los cuales la cadena de custodia brinda la certeza de que un indicio no ha sido reemplazado por otro o vulnerado dando pautas para la tecnificación y realización de un reglamento que conlleve a la correcta valoración de la cadena de custodia, y las pruebas en la etapa de juicio por parte de los jueces de garantías penales se abordan en la investigación desarrollada por Vargas (2017), “La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación” (p.10)

Lorca (2017) dilucida el alcance del derecho ecuatoriano en el delito de violación de la intimidad realizado por medios informáticos y su tipificación en el Código Orgánico Integral Penal.

"Los delitos relacionados con medios telemáticos son: el *phishing*, robo de identidad, las injurias, las calumnias, la extorción, el acoso, la publicación de pornografía, la pedofilia, el *grooming*, difusión de malware, trata de blancas, sicariato, *happy slapping*, la estafa; son comunes pero su modus operandi, ha cambiado con el uso de medios telemáticos para sus operaciones, cuyo proceso en ocasiones no tiene la tecnología como fin" (Obregón, Ferruzola, Rodríguez, 2017, p.2). En este trabajo se muestra los conceptos de delitos, cometidos a través de las redes sociales. Se detallan métodos que usan los ciberdelincuentes en internet para aproximarse a sus víctimas.

La normativa procesal indica que existirán informes periciales conforme a lo solicitado por el juez o fiscal y se presentara de forma verbal y por escrito; acorde a lo definido en el Reglamento del Sistema Pericial Integral de la Función Judicial los requisitos mínimos obligatorios que todo informe pericial contendrá, serán: antecedentes donde se delimitara el objeto del peritaje, consideraciones técnicas o metodología a aplicarse, conclusiones y opinión técnica sin dar juicios de valor, inclusión de documentos de respaldo y anexos que sustenten las conclusiones técnicas mediante fotos, laminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc. (p. 7)

2.3.5.6 Juicios con sentencias ejecutoriadas en base a evidencias de redes sociales en Ecuador

La información aquí detallada se ha obtenido del sistema eSATJE administrado por el Función Judicial en representación del Consejo de la Judicatura y corresponde a los procesos judiciales penales en función de actores/ofendidos o demandados/procesados.

En el caso de Mónica Loor contra Hugo Garzón y Jessenia Zhunio por Violación a la Intimidad en el año 2013 en el Tribunal de Garantías Penales de Orellana, se emite sentencia según lo establecía el artículo 202.2 del Código Penal actualmente estipulado en el artículo 178 del Código Orgánico Integral Penal, el delito cometido se fundamenta en la publicación de fotografías y videos de índole personal de los encuentros íntimos mantenidos por la ofendida Mónica Loor y Hugo Garzón mediante publicaciones en la red social Facebook.

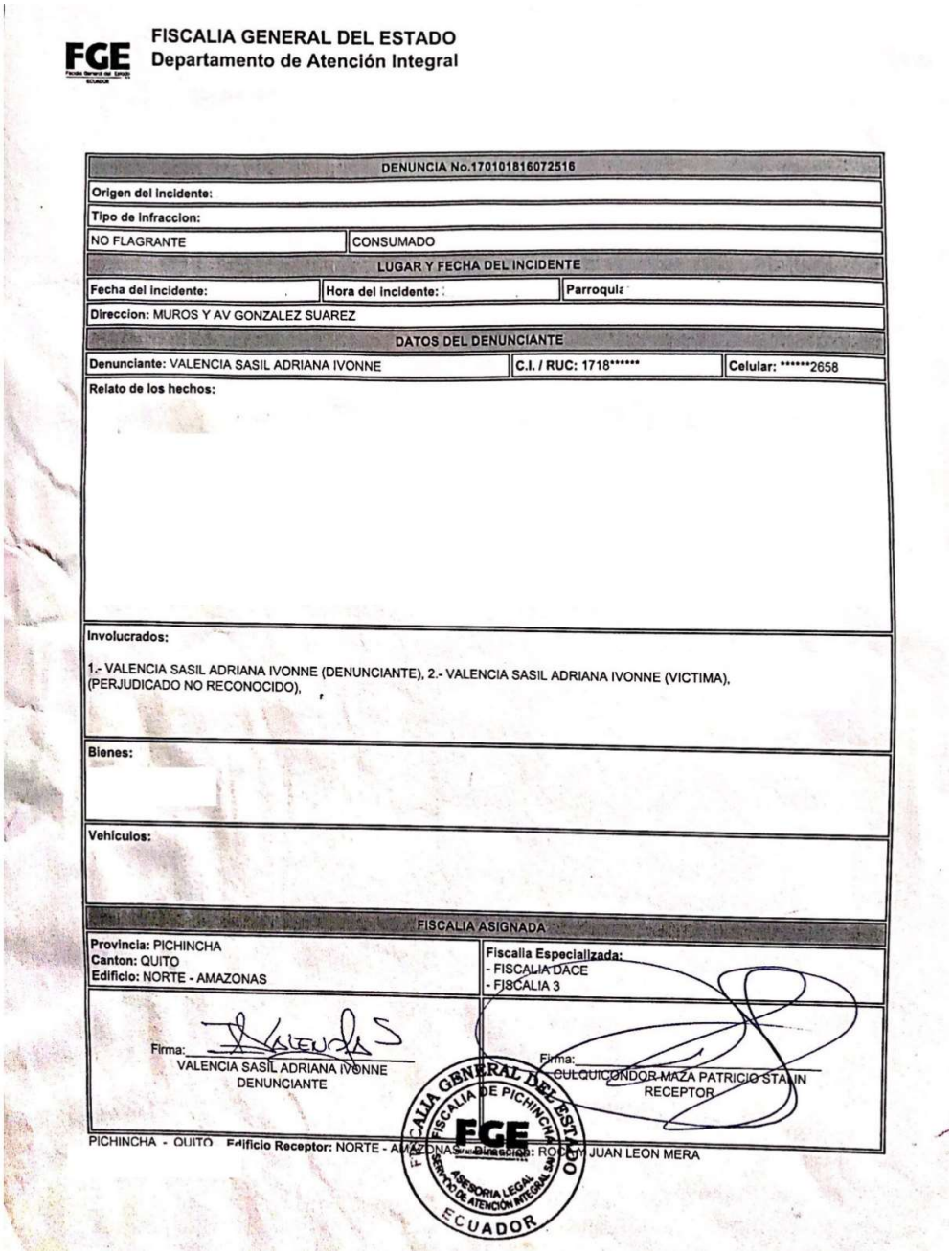
En el procedimiento ordinario establecido por Martinus Van Der Valk contra Sohar Romero en 2014 en la Unidad Civil del cantón de Guayaquil, por daños morales se aplica la materialización de las pruebas en portales de Facebook y Blogger debido a publicaciones que hacen referencia a una serie de delitos cometidos por Van Der Valk en Galápagos y cargadas a los portales mencionados por el usuario Sohar.

José Bolívar Castillo Vivanco vs la Concejal de la ciudad de Loja, Jeannine del Cisne Cruz Vaca, por las expresiones vertidas a través de la red social twitter, el día 21 de septiembre de 2015, en este juicio se señala que se ha procedido a realizar acciones atentatorias a la honorabilidad y buen nombre del accionante como persona y funcionario público, indicando en su mensaje: " Alcalde José Bolívar Castillo lo que pedimos las Lojanas es que deje de mentir y de robar"; se declaró la culpabilidad por haber infringido el numeral 1 del Art. 396 del Código Orgánico Integral Penal, con una multa del 25% de un salario básico unificado y una pena de 30 días de privación de libertad.

2.4 Métodos vigentes para recolección de evidencia digital en la denuncia de delitos afines a redes sociales en Ecuador

Para denunciar hechos de delitos en redes sociales, el afectado o víctima debe realizarlo en el Servicio de Atención Ciudadana de la Fiscalía próxima a su sitio de residencia, conocidas como Unidades de Servicio de Atención Integral (SAI), según la página de la Policía Nacional.

Allí, los funcionarios recibirán la denuncia que será redactada de forma manual en el formato indicado en la Figura 3, al concluir la toma de versión se asesorará al afectado con el proceso a seguir de acuerdo a su caso.



FISCALIA GENERAL DEL ESTADO
Departamento de Atención Integral

DENUNCIA No.170101816072516		
Origen del incidente:		
Tipo de infraccion:		
NO FLAGRANTE	CONSUMADO	
LUGAR Y FECHA DEL INCIDENTE		
Fecha del incidente:	**Hora del incidente:**	**Parroquia**
Direccion: MUROS Y AV GONZALEZ SUAREZ		
DATOS DEL DENUNCIANTE		
Denunciante: VALENCIA SASIL ADRIANA IVONNE	**C.I. / RUC:** 1718******	**Celular:** ******2658
Relato de los hechos:		
Involucrados: 1.- VALENCIA SASIL ADRIANA IVONNE (DENUNCIANTE), 2.- VALENCIA SASIL ADRIANA IVONNE (VICTIMA), (PERJUDICADO NO RECONOCIDO),		
Bienes:		
Vehiculos:		
FISCALIA ASIGNADA		
Provincia: PICHINCHA **Canton:** QUITO **Edificio:** NORTE - AMAZONAS	**Fiscalia Especializada:** - FISCALIA DACE - FISCALIA 3	
Firma: VALENCIA SASIL ADRIANA IVONNE DENUNCIANTE	Firma: CULQUICONDOR MAZA PATRICIO STALIN RECEPTOR	

PICHINCHA - QUITO **Edificio Receptor:** NORTE - AMAZONAS **Dirección:** RODOLFO JUAN LEON MERA

FISCALIA GENERAL DEL ESTADO
FISCALIA DE PICHINCHA
FGE
ASESORIA LEGAL
SERVICIO DE ATENCIÓN INTEGRAL SAI
ECUADOR

Figura 3 Formato para recepción de denuncias

Fuente (Fiscalía General del Estado, 2020)

Actualmente para aquellos casos relacionados con violencia de género o intrafamiliar también se ha habilitado la opción de denuncia en línea detallada en la Figura 4 en el sitio web de la Fiscalía

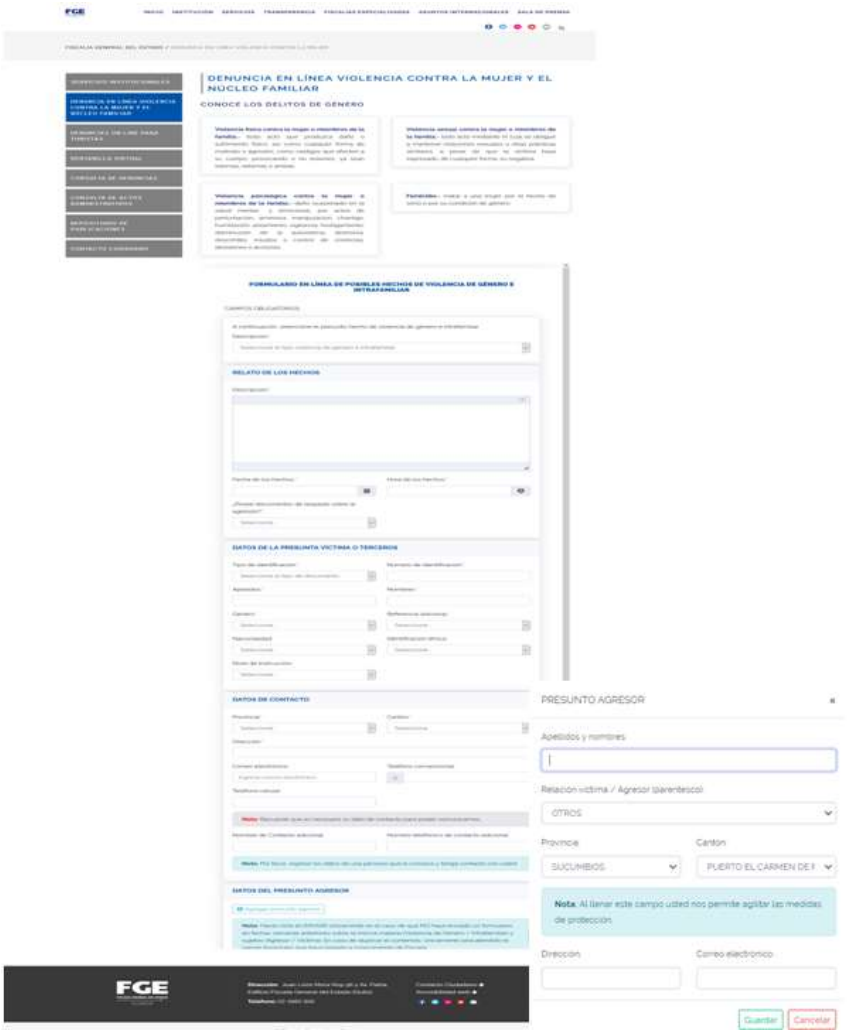


Figura 4 Formato de denuncia en línea

Fuente: Pagina Web Fiscalía General del Estado Opción Denuncia en Línea

De igual forma corresponde a un llenado manual de diferentes datos entre los que consta el relato de los hechos, solicita la confirmación de existencia de documentos de respaldo sobre la agresión como fotos, videos u otros pero no existe opción para cargar los mismos y en su última sección permite ingresar los datos del presunto agresor, acorde a la información detallada en la Figura 4.

Los entes gubernamentales también realizan procesos de denuncia en Fiscalía, como se puede ver en la Figura 5, dichas denuncias son presentadas a través de un llenado manual de datos donde se describe textualmente el texto contenido en la red social Twitter, se denomina al usuario de Twitter de la siguiente forma "*se encuentra una página que se denomina*", se identifica al usuario por el nombre de pantalla aduciendo desconocimiento de nombres y apellidos, finalmente, la captura de pantalla del contenido también se adjunta por un Telegrama interno.

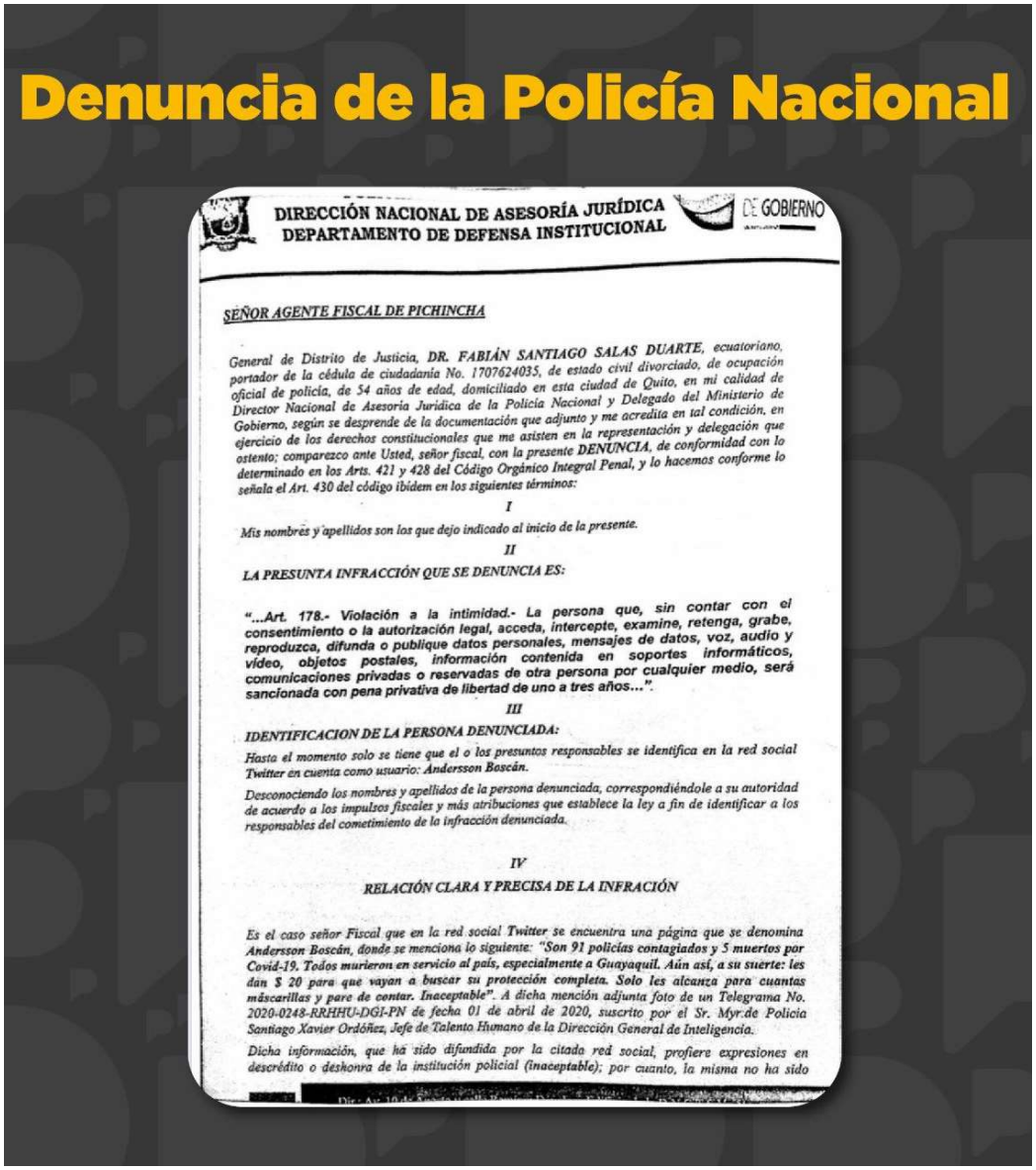


Figura 5 Formato de Denuncia Policía Nacional

Fuente: Twitter La Posta Ec

2.5 Adopción perspectiva teórica

En el seguimiento de los delitos tecnológicos un punto crítico corresponde a la cadena de custodia de donde se va a realizar el peritaje, en la cual mediante documento elevado a público se debe asegurar el estado de la prueba, determinando que en el proceso de obtención y análisis la prueba no ha sido contaminada. Considerando que la constante evolución y el surgimiento de nuevas formas de exposición de la evidencia digital, deriva en la implementación de nuevos métodos y técnicas de adquisición y preservación que respeten los principios dispuestos en la normativa ISO-IEC 27037 respecto al manejo de la información: Relevancia, Suficiencia y Fiabilidad.

Con el surgimiento del almacenamiento en la nube como modelo de servicio, los datos contenidos en un medio informático se almacenan, administran y preservan remotamente, gestionados por un proveedor de servicio externo en servidores que están en internet. La información a la que hacemos referencia corresponden a: fotos de los diversos servicios de almacenamiento en la nube, *backups* de programas de mensajería, *backups* de dispositivos, mapas de recorridos geo-referenciados, comunicaciones desde las distintas redes sociales y programas de mensajería instantánea, información de contactos, historiales de navegación, búsquedas en internet, actividades del dispositivo, etc.; cualquiera de los datos antes mencionados se puede considerar evidencia digital.

Los contenidos publicados en las redes sociales se usan como evidencia directa para indicar la participación de un individuo en un delito o su mala conducta, el material publicado en las plataformas en línea revela el estilo de vida, el estado financiero y las preferencias de relacionamiento con determinadas personas, esta información es invaluable en casos de divorcio y custodia.

Los datos de las redes sociales ofrecen suficiente información para realizar verificaciones de antecedentes de sospechosos, víctimas y testigos. También es adecuado para fines de perfilado. Además, estos datos proporcionan hechos específicos sobre los individuos y sus asociaciones con otra gente; estos puntos ayudan a determinar el motivo y la oportunidad del involucrado en un crimen. Las vías de comunicación pueden conducir a cómplices adicionales. El hallazgo de evidencia adecuada en las redes sociales incluso puede ayudar a determinar una decisión de culpable versus no culpable.

La preservación de evidencia mediante la introducción de las herramientas en línea denominadas testigos online tiene ventajas: a) no requiere acceso a dispositivos finales, tiene opción de realizarse a distancia; b) se puede obtener en tiempo real; c) no depende del modelo del dispositivo en el cual se haya originado, recibido o almacenado la evidencia; d) se puede recuperar información eliminada en determinadas circunstancias.

Como resultante de la investigación se desarrollara una propuesta de sistema que contendrá un script con diferentes herramientas para realizar recolección de evidencia digital en la red social Twitter, este desarrollo se efectuara bajo la normativa NIST e incluirá la certificación de la evidencia por terceros de confianza también denominados testigos online, mediante esta propuesta se pretende socializar con los interesados profesionales, estudiantes, organizaciones civiles en la obtención de evidencia electrónica con una metodología apropiada para la red social Twitter.

CAPÍTULO III

MÉTODO

3.1. TIPO DE ESTUDIO

Para el desarrollo del proyecto de titulación se usará el método exploratorio y descriptivo.

Exploratoria

Se empleará esta metodología ya que se detallará la información necesaria para la documentación y certificación de pruebas a peritos o personas que requieran la obtención de evidencia en delitos perpetrados a través de la red social Twitter.

Descriptiva

De forma descriptiva se planteará un procedimiento para la recolección de pruebas de información en línea obtenida en la red social Twitter y certificada digitalmente.

3.2. MODALIDAD DE INVESTIGACIÓN

Documental

Esta investigación se plantea de forma documental basada en:

Lectura sobre procedimientos actuales para obtención de evidencia en delitos informáticos en redes sociales.

Lectura de bibliografía concerniente a tesis y publicaciones que presenten la situación de delitos informáticos en redes sociales.

Lectura de estándares internacionales establecidos por organismos como IEEE y organismos Europeos a través de sus normativas.

Lectura y comprensión del Código Orgánico Integral Penal y la determinación de vacíos legales.

3.3 LEVANTAMIENTO DE INFORMACION

El objetivo del presente trabajo es desarrollar un modelo específico para la investigación de la red social Twitter en línea y luego se desplegará un prototipo que refleje el proceso de investigación forense basado en el modelo que se ha desarrollado anteriormente.

Un hash, utilizado en métodos forenses informáticos tradicionales, reduce una entrada binaria grande o flujo de bits en un valor de tamaño fijo, normalmente mostrado como un valor hexadecimal y realiza la tarea de verificar que una copia sea exactamente igual que el original, habitualmente utilizando MD5 y SHA-256; actualmente existen una serie de aplicaciones de código abierto disponibles que permiten el hash de archivos.
Sin embargo, tanto los perfiles de usuario como los estados tienen propiedades que cambian con el tiempo y se sobrescriben, lo que hace que el hash de datos directamente de la red social sea casi imposible.

3.3.1 Twitter

Twitter considerada como una de las redes sociales más populares que proporcionan una red social de usuarios que publican mensajes compuestos de hasta 280 caracteres llamados "tweet". Twitter permite a los usuarios compartir sus mensajes sobre todo lo relacionado con la vida real, incluyendo noticias, eventos, celebridades, política. De acuerdo con el sitio de estadísticas Statista, esta red social tiene 326 millones de usuarios activos mensuales (MAU), los usuarios activos se calculan utilizando los datos en función de usuarios únicos que realizan acciones específicas que se consideran un signo de actividad; alcanzando los 500 millones de tweets por día que equivalen a 350,000 tweets por minuto (Statista. 2020), un usuario en promedio establece una sesión de 3.39 minutos dentro de la red social.

En una cuenta de Twitter podemos encontrar el contenido detallado en la Figura 6, cuyas definiciones serán tratadas más adelante.

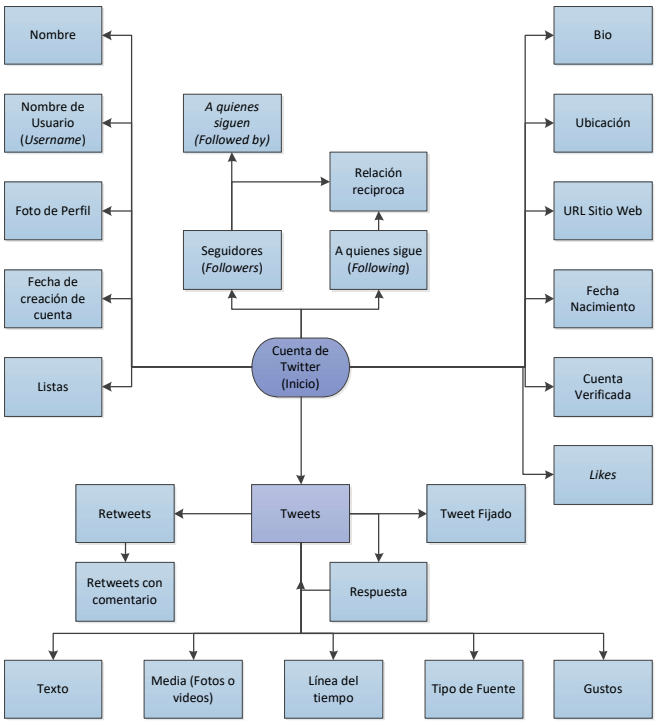


Figura 6 Contenido red social Twitter

Fuente: Autor

Twitter determina los temas más comentados en un momento dado y los llama "Temas de tendencias (TT)" para que los usuarios estén al tanto de la mayoría temas populares en Twitter.

"Hashtag" es un término que comienza con el carácter "#" se usa comúnmente para mencionar el tema del tweet y permite a los usuarios seguir los temas que les interesan. Gracias a su popularidad y diseño, Twitter inmediatamente refleja eventos notables en tiempo real. Esta estructura de Twitter permite sistemas de búsqueda en tiempo real, servicios de minería de tweets en tiempo real para averiguar qué está sucediendo en el mundo con un retraso mínimo.

El análisis de sentimientos permite llegar a una conclusión sobre temas en Twitter lo que convierte a Twitter en un sistema de encuestas en tiempo real. El éxito de esos servicios depende completamente del filtrado de usuarios legítimos.

Twitter permite que las cuentas "sigan" otras cuentas. A diferencia de otras plataformas de redes sociales, la relación entre usuarios es bidireccional en lugar de enlaces unidireccionales que significan que un usuario puede no estar siguiendo a uno de sus seguidores. El usuario puede seleccionar "me gusta" o "retweet (RT)" a un tweet que significa que compartirá ese tweet con sus "seguidores".

Cada usuario tiene un nombre de usuario de Twitter único, y los usuarios pueden publicar tweets que refieren a otros agregando sus nombres de usuario al comenzar Carácter "@" que se llama "mención" en Twitter. Los usuarios son informados inmediatamente con notificaciones cuando una mención, me gusta, o RT le sucede a uno de sus tweets. Un resumen de esta estructura de datos se presenta en la Tabla 7.

Tabla 7 Estructura de datos en Twitter

Tweet	User	Entity	Place
Elemento fundamental que conforma los tweets, comprendido por un identificador único (ID), y el texto del tweet; devuelve atributos como lenguaje, autor, coordenadas, marca de tiempo, etc.	Una cuenta activada en Twitter tiene un elemento user asociado; conformado por campos como el nombre, fecha de creación de cuenta, descripción de intereses, imagen de perfil, idioma preferido, usuarios a los que sigue, seguidores, entre otros.	Contiene metadatos de los elementos tweet y user. Sus atributos reseñan las menciones a otros usuarios (@usuario), hashtag o etiquetas (#etiqueta), contenido multimedia o enlaces http.	Corresponden a los lugares o sitios que han sido incluidos en un tweet. Compuesto por atributos como dirección, coordenadas, etc.

Fuente: Autor

Otra característica de Twitter es permitir a los usuarios crear usuarios públicos o listas privadas para organizar sus intereses agrupando usuarios cuyos intereses son iguales o similares. Del mismo modo, es posible administrar listas agregando usuarios a las listas o eliminar usuarios de las listas de las cuales es propietario.

Acorde a la información de la organización Pew Research que realizo una encuesta en Estados Unidos a usuarios adultos de Twitter en 2019, concluye que existe una diferencia abismal en la cantidad de contenido que produce un usuario asiduo de Twitter y un usuario promedio, mientras un usuario promedio publica contenido propio 2 veces al mes y añade como favorito solo un tweet por mes, el usuario más asiduo de la plataforma produce una mediana de 138 tweets mensuales y añade como favorito a 70 tweets por mes, información detallada en la figura 7. En esta estadística no se consideran cuentas institucionales.

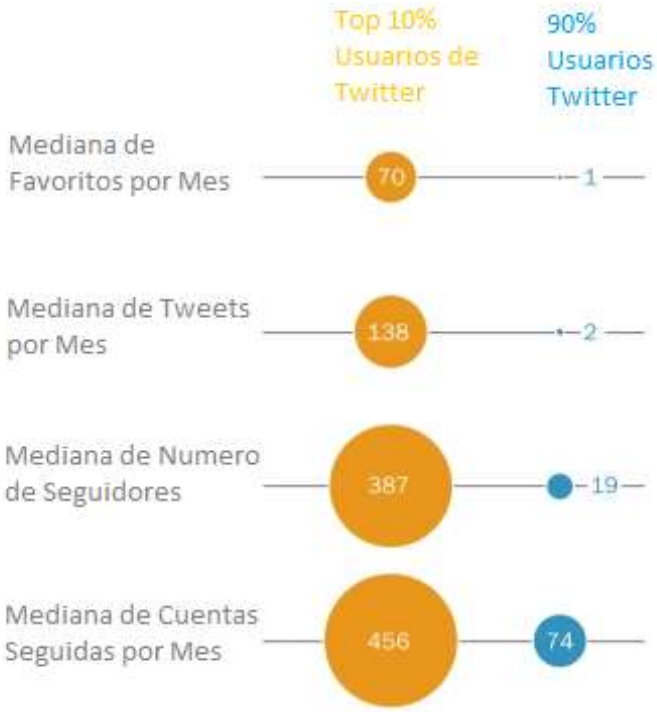


Figura 7 Evaluación de los usuarios de Twitter

Fuente: Pew Research Center

3.3.1.1 Metadatos para elementos individuales en Twitter

La autenticación de la evidencia de las redes sociales puede presentar desafíos importantes cuando se recopilan capturas de pantalla, impresiones o feeds html sin procesar desde una herramienta de archivo. Esta es solo una de las razones por las cuales los datos de las redes sociales deben recopilarse, conservarse, buscarse y producirse adecuadamente de manera coherente con las mejores prácticas. Cuando las redes sociales se recopilan con una cadena de custodia adecuada y se conservan todos los metadatos asociados, la autenticidad puede ser mucho más fácil de establecer. Como ejemplo, los campos de metadatos señalados en la Tabla 8 son clave para elementos

individuales de Twitter (Chemerkin, 2012) que proporcionan información importante para establecer la autenticidad del tweet, si se recopila y preserva adecuadamente:

Tabla 8 Metadatos obtenidos del objeto Tweet

Entity	Definición	Tipo de Dato
ID	Representacion del identificador unico asignado al Tweet cuando ha sido posteado en la red. No puede ser Nulo.	Constante
created_at	Fecha y hora de publicacion del tweet (AAAA-MM-DD HH:MM:SS) en formato UTC, no se puede modificar. No puede ser Nulo.	Constante
coordinates	Permite ubicar al usuario en el sitio de la publicacion de Twitter, este campo puede ser habilitado por el usuario por lo tanto puede ser Nulo.	Constante
in_reply_to_screen_name, in_reply_to_status_id	Estos campos retornan ID y nombre de usuario destinatario si el tweet es una repuesta. Resulta de utilidad si se está monitorizando la actividad entre usuarios. Puede ser Nulo.	Constante
lang	Hace posible obtener información relacionada al sistema del usuario. Mediante el identificador de lenguaje del equipo desde el que se genero el Tweet.	Constante
place	Indica si el tweet se publicó de un sitio concreto permitiendo la ubicación del usuario. Se puede señalar un lugar cualquiera, por lo que no es determinante. Puede ser Nulo.	Variable
source	Permite obtener información sobre qué dispositivos utiliza un usuario para el acceso a la aplicación, indicando la fuente de origen desde donde se ha publicado el tweet. No puede ser Nulo.	Constante
text	Contenido publicado en formato UTF-8 de maximo 280 caracteres. Permite la filtracion por palabras clave. No puede ser Nulo	Constante
contributors	Grupo de identificadores de usuario, que indica quién contribuyó a la autoría del tweet. Puede ser nulo.	Constante

Fuente: (Chemerkin, 2012)

La actividad de datos del objeto Tweet se refiere a los datos registrados para cada acción realizada por el usuario, como la hora y el lugar asociado con publicaciones. Estos datos son el subproducto de la actividad del usuario, la información de la actividad se basa en eventos. Por lo tanto, esta información es más confiable ya que se genera automáticamente.

Los metadatos mantenidos por las redes sociales ayudan a las investigaciones y autentican la evidencia. Técnicamente, son datos sobre datos; actúan como una directiva para los motores de búsqueda y muestran el contenido a los usuarios.

Las marcas de tiempo y etiquetas de ubicación asociadas con interacciones en línea pueden ser usadas para encontrar el paradero de una persona. Esta información también permite corroborar una coartada o es la evidencia de que un individuo estaba en otro sitio cuando se cometió un delito. En la Tabla 9 se encuentran detallados los metadatos obtenidos del perfil de usuario.

Tabla 9 Metadatos obtenidos del objeto User

Entity	Definición	Tipo de Dato
id	Valor entero de 64 bits que es considerado el identificador unico para el usuario.	Constante
default_profile, default_profile_image	Variable que indica si se ha realizado un cambio en el perfil o la imagen de perfil.	Variable
screen_name	Alias asociado a la cuenta, permitira comparar o buscar el mismo nombre de usuario o alias en diversas plataformas.	Constante
name	Nombre de usuario de la cuenta.	Variable
created_at	Fecha de creación de la cuenta.	Constante
description	Es un campo opcional, breve reseña sobre el usuario.	Variable
followers_count	Variable que contiene el número de seguidores asociada a la popularidad de la cuenta.	Variable
friends_count	Permite conocer la cantidad de usuarios a los que sigue la cuenta.	Variable
lang	Variable que almacena los datos del lenguaje indicado por el propio usuario.	Variable
location	Localización geográfica publicada por el usuario.	Variable
time_zone	Zona horaria publicada por el usuario.	Variable

Fuente: (Chemerkin, 2012)

3.3.1.2 Acceso mediante APIs a información de Twitter

La API de Streaming de Twitter recopila datos producidos en tiempo real, mientras la API REST tiene el propósito opuesto es decir recabar datos que se produjeron antes del momento de la recopilación, es decir información histórica.

Usando esta API podemos recopilar tweets antiguos que contienen ciertas palabras clave, pero también podemos recopilar otra información que sea relevante para la plataforma, como amigos y seguidores de diferentes cuentas de usuario, retweets de una determinada cuenta, o retweets de un tweet determinado.

Para crear una conexión con la API REST se deben ejecutar las líneas de comando indicadas en la tabla 10 en base a las credenciales personales obtenidas en modo developer de la red social Twitter.

Tabla 10 Líneas de comando conexión API REST Twitter

```
auth = tweepy.OAuthHandler(consumer_key, consumer_secret)
auth.set_access_token(access_token, access_token_secret)
api = tweepy.API(auth)
```

Fuente: Twitter (2020)

Los usuarios dentro de las API de Twitter se identifican mediante dos variables diferentes:

El usuario o screen_name, que es el nombre de Twitter antepuesto al símbolo @ y el user_id, que es un identificador numérico único para cada usuario de Twitter.

En el proceso de recopilación de datos, cuando queremos especificar el usuario del que queremos recopilar datos, podemos hacerlo utilizando el screen_name o el user_id de dicho usuario.

La línea de tiempo de un determinado usuario son los tweets anteriores que ha publicado o retuiteado. Es útil recopilar esta información para tener una idea de la actividad previa de una determinada cuenta dentro de la red social.

Sin embargo, debemos saber que el método que se utilizará solo puede devolver los últimos 3200 tweets de un usuario específico, por lo que, si estamos recopilando publicaciones de una cuenta muy activa y queremos tweets de hace mucho tiempo, no podrán ser obtenidos por una cuenta Standard, sin embargo, el uso de una cuenta Entreprise permite acceder al producto Full-Archive Search API que brinda un acceso instantáneo a todo el histórico de Twitter.

3.3.1.3 Tweets Eliminados

Al eliminar un tweet el contenido será desagregado del timeline del usuario, de las cuentas que sigan al usuario y los resultados de búsquedas en los motores de búsqueda propios de Twitter como son: twitter.com, Twitter para iOS y Twitter para Android, el proceso de eliminación considera los siguientes aspectos:

- El usuario solo podrá eliminar el contenido de su propio timeline, no los tweets de otras cuentas.
- Los retweets también será eliminados sin embargo si se encuentran retwiteados por otros usuarios con su comentario propio, ese contenido no se eliminará.
- Si otros usuarios realizaron una copia y luego pegaron el tweet o parte de el en su propio tweet tampoco se eliminará dicho contenido.
- Twitter garantiza la eliminación del contenido en sus propios motores de búsqueda, pero también menciona la posibilidad de que dicha información puede ser susceptible a quedar almacenada en cache de sitios web así también como aplicaciones u otros motores de búsqueda de terceros.

Al postear un tweet este se asocia a un identificador único, este identificador corresponde a un número y se encuentra dentro de la URL del tweet, de esta forma se puede considerar que al buscar la URL con el ID del Tweet la información que retorna será única y contendrá la información del posteo, ver figura 8.

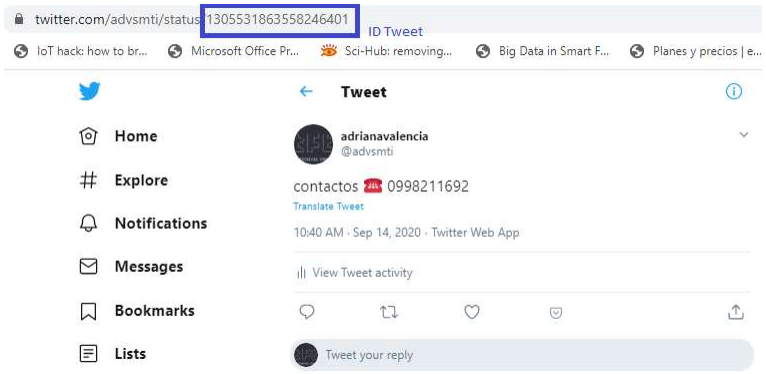


Figura 8 URL Twitter con ID del Tweet

Fuente: Twitter (2020)

A continuación, se presentan dos métodos que permitirían acceder a la información del tweet eliminado en base a la búsqueda por URL del Tweet o búsqueda por nombre de usuario en una API.

Internet Archive

Se pueden recuperar tweets personales o de otras cuentas según la asociación antes expuesta en el motor de búsqueda Internet Archive. En la página web solicita la información de la URL a la que se desea acceder, en caso que encuentre información de dicha búsqueda indicara en la sección *Saved* la fecha de la que contiene resultados, verificar figura 9.

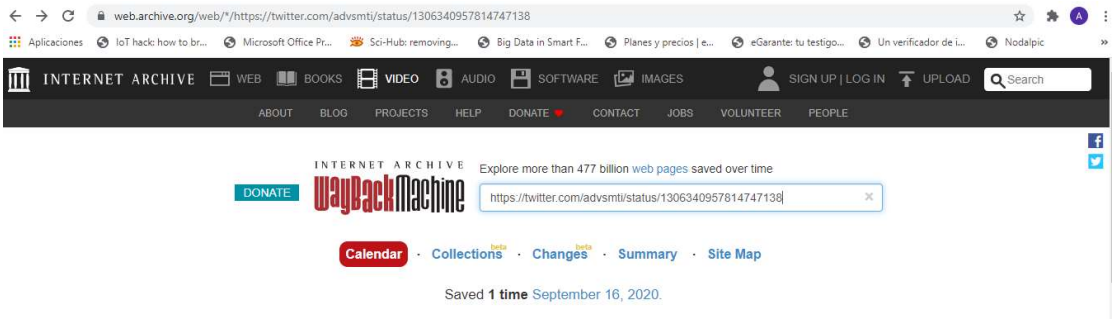


Figura 9 Búsqueda por URL de contenido de Internet antiguo

Fuente: Motor de Búsqueda webarchive.org

Al dar click en la fecha se obtiene acceso a la información del contenido de dicha publicación a la fecha indicada como se puede evidenciar en la figura 10.

Figura 10 Resultado contenido en el motor de búsqueda Wayback Machine

Fuente: Motor de Búsqueda webarchive.org

API Tweepy

A través de la API Tweepy y mediante la ejecución de comandos, también se puede acceder a la búsqueda de contenido de un timeline de hasta 3200 tweets antiguos, esta búsqueda arrojara tanto información que se encuentra publicada actualmente, así como información antigua que se encuentre cacheada; por lo tanto, como en el caso antes mencionado no se puede asegurar que recuperara toda la información borrada sino solo aquella que haya sido cacheada en su sistema.

```
advsmti,1311862730274594817,2020-10-02 02:57:02,video prueba acoso @Adriana_ee1311 https://t.co/tYcHf7m1UM
advsmti,1306360247439761409,2020-09-16 22:32:08,prueba acoso sexual
advsmti,1306340957814747138,2020-09-16 21:15:29,@DaloBucaram10  loco contactame  0998211692
advsmti,1306340210192547840,2020-09-16 21:12:31,#robolucion con correa
advsmti,1305532006093197313,2020-09-14 15:41:00,acoso sexual prueba
advsmti,1305531921406013440,2020-09-14 15:40:40,prueba tesis n
advsmti,1305531863558246401,2020-09-14 15:40:26,contactos  0998211692
```

Figura 11 Búsqueda de Contenido de Timeline por Usuario de Twitter a través de la API Twitter

Fuente: Autor

3.3.1.4 Análisis de herramientas en línea para procesamiento y recopilación de datos en Twitter

En detalle se recopila un análisis de las herramientas en línea disponibles actualmente y su relación con la información recopilada de la red social Twitter.

Tinfoleak

Herramienta diseñada para el análisis de inteligencia de Twitter que proporciona una salida de archivo HTML. Está incluido en varias distribuciones de Linux entre ellas Kali. Considerada como una herramienta de código abierto completa.

La siguiente información es extraída con esta herramienta:

- Conversaciones

- Información de la cuenta como: actividad del usuario, cuentas protegidas, relaciones con el usuario
- Aplicaciones de origen o Dispositivos de usuario y su frecuencia de uso
- Hashtags, Menciones, Favoritos
- Análisis de texto por frecuencia de palabras, medios y metadatos
- Lugares visitados por el usuario como ubicaciones principales
- Redes sociales e Identidades digitales
- Usuarios geolocalizados o Usuarios etiquetados
- Seguidores y Amigos
- Listas

TweeterID

Mediante el uso de cualquier ID de Twitter o @nombredeusuario, se convertirá en el ID o nombre de usuario correspondiente.

Who Tweeted it first

Herramienta que mediante el uso de palabras clave de búsqueda, o un enlace, encontrará el primer tweet que contenga determinado término. Realiza la búsqueda mediante operadores o usando toda una frase entre "comillas dobles" para una coincidencia exacta.

Twitter Búsqueda Avanzada

La búsqueda en Twitter se puede realizar usando una gran variedad de filtros como palabras, ver Figura 12, o por datos de la cuenta, ver Figura 13. Las búsquedas resultantes se pueden guardar, así como ajustar dentro del cuadro de búsqueda o la URL.

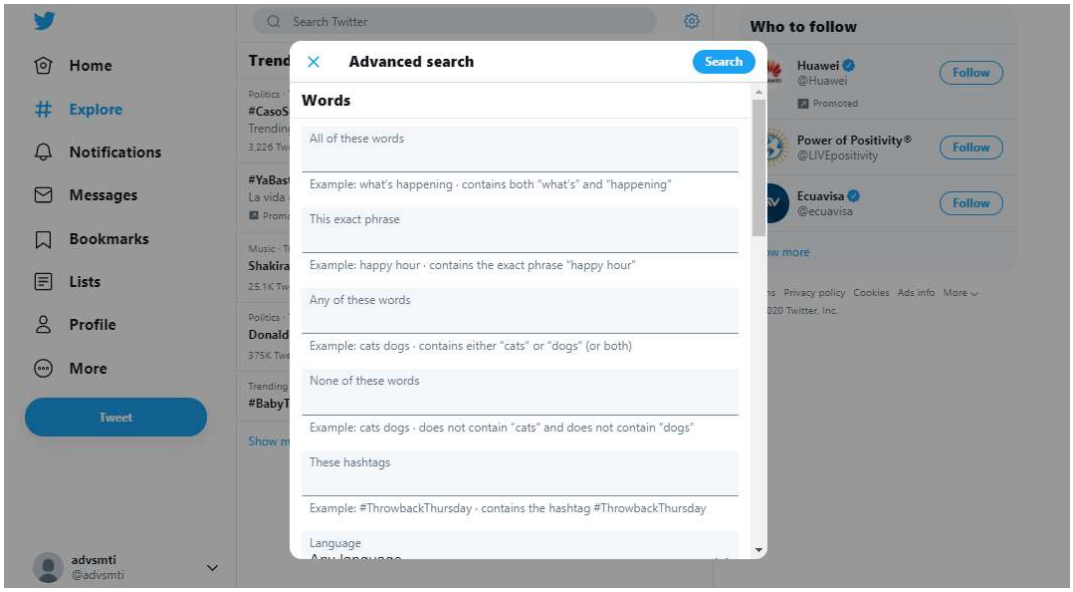


Figura 12 Datos necesarios para la opción búsqueda avanzada por palabras en Twitter

Fuente: (Twitter, 2020)

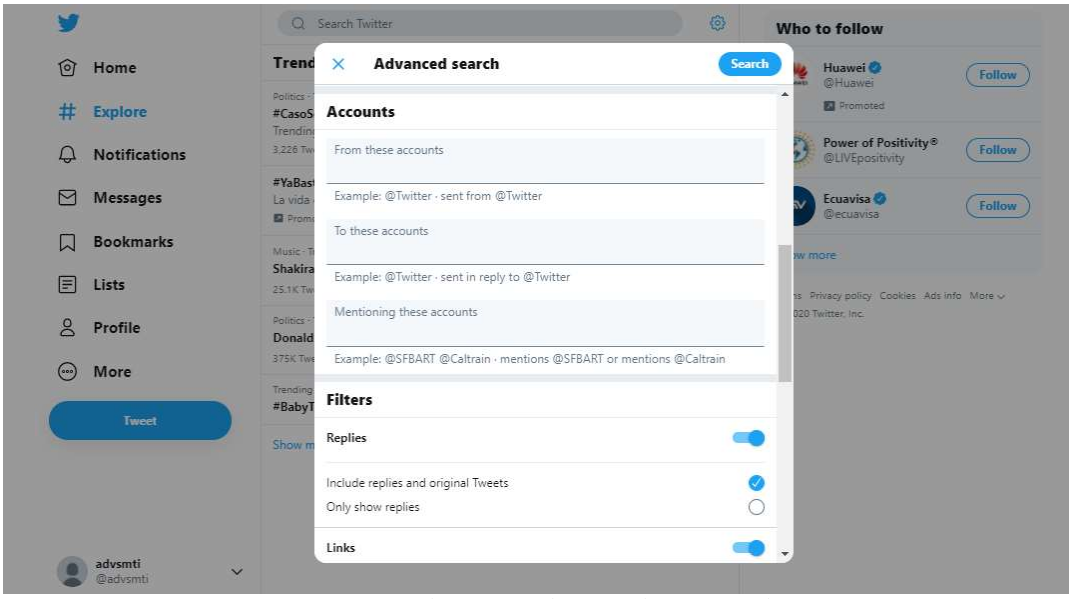


Figura 13 Datos necesarios para la opción búsqueda avanzada por cuenta en Twitter

Fuente: (Twitter, 2020)

La búsqueda avanzada de Twitter es una herramienta poderosa para encontrar Tweets comprometedores o lamentables que podrían usarse en una investigación.
Por ejemplo en la Figura 14 se realiza una búsqueda con el filtro filter:native_video coincide con los tweets que contienen videos nativos de Twitter, subidos directamente a Twitter. Esto no coincidirá con los videos creados con Vine, Periscope o Tweets con enlaces a otros sitios de alojamiento de videos.

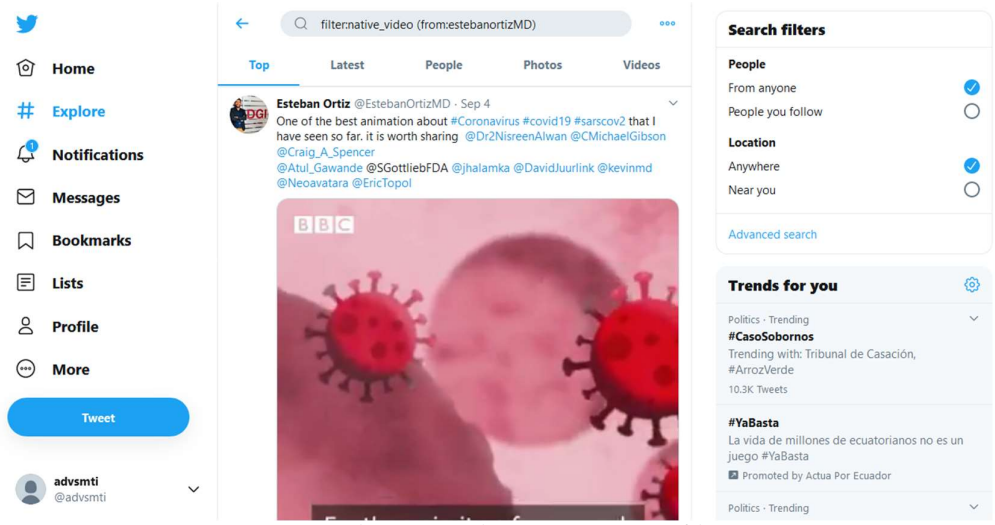


Figura 14 Búsqueda avanzada por usuario y filtro en Twitter

Fuente: (Twitter, 2020)

Followerwonk

Herramienta de análisis de cuentas, útil para explorar biografías de Twitter para encontrar cuentas de intereses comunes.

Esta herramienta también permite comparar en un máximo de 3 cuentas, entre quienes son seguidores o a quienes siguen, con un límite de 50000 interacciones, si supera dicho límite debe realizarse mediante funciones de pago.

Spoonbill

Permite ver los cambios de perfil de los seguidores en Twitter u otras redes sociales, como nombre, datos de la biografía, cambios en el nombre de la web.

Twitter List Copy

Herramienta que permite copiar listas completas de Twitter para crear unas propias. Creado por Noah Liebman. También disponible en Github para modificarlo y adaptarlo a nuestros propósitos, en este caso permite añadir los intereses de una cuenta de Twitter a la nuestra.

TweetBeaver

Interfaz fácil de usar que ofrece análisis de cuentas, incluso para interacciones entre cuentas.

Hay muchas herramientas útiles como convertir un nombre de usuario de Twitter a ID, descargar la línea de tiempo de un usuario, encontrar seguidores en común de dos cuentas, descargar la lista de amigos de una cuenta, etc.

Foller.me

Información sobre cualquier perfil público de Twitter. Recopila la información del perfil del usuario solicitado y los últimos tweets. Analiza el contenido del tweet e informa sobre el uso de temas en forma de "nubes de etiquetas" para mejorar la comprensión de las palabras que fueron las más populares.

También permite verificar datos que no se muestran en las páginas públicas de Twitter, como la fecha de ingreso, la zona horaria y la proporción de seguidores.

OneMillionTweetMap

Mapa en tiempo real de los últimos tweets geolocalizados entregados resultado de la búsqueda por determinado tópico.

En resumen, se tienen las funcionalidades detalladas en la Tabla 11 de cada herramienta disponible para análisis de datos de Twitter

Tabla 11 Resumen de funcionalidades que prestan las herramientas de análisis de datos de la red social Twitter

	Tinfoleak	*TweeterID*	*Who Tweeted it first*	*Twitter Búsqueda Avanzada*	*Followerwonk*	*Spoonbill*	*Twitter List Copy*	*TweetBeaver*	*Foller.me*	*OneMillionTweetMap*
Nombre Usuario	✓				✓			✓	✓	
Fecha Creacion Cuenta	✓				✓			✓	✓	
Twitter ID	✓	✓						✓	✓	
Ubicación	✓				✓			✓	✓	✓
Siguiendo	✓				✓			✓	✓	
Seguidores	✓				✓			✓	✓	
Numero Tweets	✓			✓	✓			✓	✓	
Contenido Tweets	✓		✓	✓				✓	✓	✓
Historico de cambios						✓				
Contenido Listas							✓	✓	✓	

Fuente: Autor

3.3.1.5 Análisis de herramientas OSINT

Existen varias herramientas para la recopilación de información pública de un usuario de Internet denominadas Inteligencia de Fuentes Abiertas, a continuación, se describen brevemente varias que se encuentran vigentes para procesos de SOCMINT (Inteligencia de Redes Sociales).

UserRecon

UserRecon es un script que acelerará el proceso de búsqueda de usuarios en 75 redes sociales. Herramienta escrita en Python una vez ejecutada escaneara las diferentes redes sociales y al finalizar generara un reporte con formato .txt.

Userrecon-py

Permite realizar la búsqueda de nombres de usuario en 187 plataformas diferentes, herramienta escrita en Python con un archivo de salida en formato json que contiene los resultados.

Little Brother

Herramienta OSINT que permite recolectar información de personas localizadas en la región de Francia, Bélgica, Luxemburgo y Suiza, sin embargo, algunas de sus funcionalidades se pueden usar para investigaciones generales. Desarrollada en Python que permite la extracción en archivos o visualización de los datos en su base.
Características: Búsqueda de Teléfono, correo, nombre y apellido, dirección, ubicación IP correo, IP, Bssid, lectura de exif, búsqueda en google, Twitter, Instagram, Facebook, Linkedin, fuerza bruta al Hash, administrador de base de datos y elaboración de un perfil.

Sherlock

Herramienta desarrollada en Python que verifica en alrededor de 300 redes sociales y sitios populares si un usuario con el nombre de usuario especificado está registrado allí, es decir, si hay una cuenta con ese nombre de usuario (nickname). Permite la descarga de la información recabada en archivos de tipo .txt o .csv. También dispone de un servicio en línea para realizar la búsqueda sin el uso de líneas de comando.

IKY I know You

A partir de un correo electrónico recolecta datos de un usuario, para convertir esta información en imágenes mejorando la interpretación del cerebro de los datos obtenidos. Requiere de API keys para conexión en Linkedin, Instagram, Twitter, leaklookup, peopledatalabs, fullcontact, con la información obtenida puede generar informes del perfil encontrado.

Maltego

Acepta como datos de entrada un teléfono, nombre de dominio, nombre de usuario, correo, palabras, ubicaciones geográficas, IPs. Como resultado se pueden generar nodos o arboles de datos, relacionados y representados de forma gráfica permitiendo una mejor interpretación para seguir profundizando en la obtención de información de un usuario.

OSRFramework

Es un conjunto de bibliotecas de código abierto que permite ejecutar tareas de inteligencia como validación por nombres de usuario, búsqueda deepweb, entre otros. Mediante transformaciones ad-hoc de Maltego, OSRFramework permite realizar consultas gráficamente y brinda interfaces de interacción como OSRFConsole o una interfaz web.

En resumen, se tienen las funcionalidades detalladas en la Tabla 12 de cada herramienta disponible para análisis OSINT

Tabla 12 Resumen de funcionalidades que prestan las herramientas de análisis OSINT

	UserRecon	Userrecon-py	Little Brother	Sherlock	I know you	Maltego	OSRFramework
Búsqueda por nombre de usuario	☺	☺	☺	☺		☺	☺
Búsqueda por correo electrónico			☺		☺	☺	☺
Búsqueda por numero telefónico			☺			☺	☺
Búsqueda por otras entradas			☺			☺	☺
Descarga de informacion obtenida	☺	☺	☺	☺	☺	☺	☺
Almacenamiento en base de datos			☺		☺	☺	
Presentación de resultados en forma grafica					☺	☺	☺
Generación de informe			☺		☺	☺	
Servicio web				☺	☺	☺	☺

Fuente: Autor

CAPITULO IV

DISEÑO DE LA SOLUCION

Aunque hay una serie de modelos de investigación forense digital desarrollados, no existe un modelo estándar y consistente, solo conjuntos de procedimientos y herramientas, por lo que muchas investigaciones penales digitales se realizan sin las pautas adecuadas. Además, no existe un modelo creado específicamente para la red social Twitter.
Los datos probablemente solo existirán en un momento en el tiempo y luego casi inevitablemente se perderán; se debe hacer todo lo posible para recuperar tanto como sea posible. Por lo tanto, trabajar en una copia de estos datos debe considerarse la mejor práctica habiendo extraído primero tanta información como sea posible.
Se deben conocer todas las herramientas utilizadas y se debe hacer todo lo posible para hacer que cualquier código de programación simplista y comprensible pueda interpretar los datos y que cada elemento se pueda inspeccionar, haciendo que el proceso sea tan fácil de seguir como sea posible.

4.1 MODELO GENERAL PROPUESTO

El modelo comprende todo el proceso de investigación de redes sociales en línea. La Figura 15 muestra el modelo de investigación forense digital propuesto. Por lo tanto, hemos dividido todo el proceso de investigación en dos entornos.
El entorno físico consiste en actividades realizadas antes de la investigación. Estas son actividades preliminares que incluyen la notificación del cuerpo de ejecución, la planificación de cómo llevar a cabo la investigación y también inspeccionar la escena o evidencia presente. Una vez que se hayan completado estas actividades, los investigadores procederán al entorno digital donde llevarán a cabo la investigación y el análisis de la red social en línea utilizando el prototipo de aplicación que se desarrollará. La siguiente actividad volverá al entorno físico donde tiene lugar todo el proceso de evaluación.
Las explicaciones de cada proceso son las siguientes:

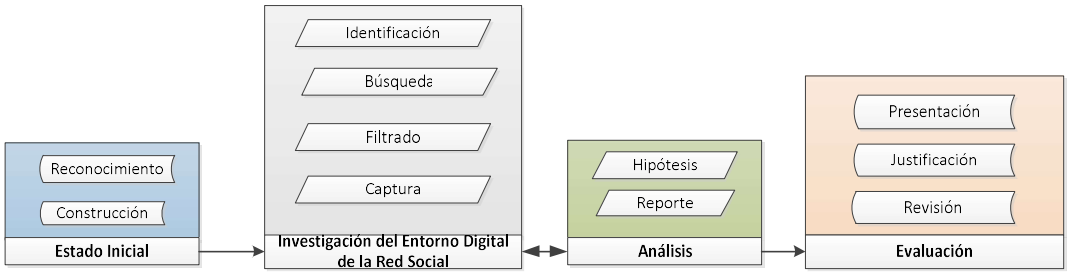


Figura 15 Modelo de investigación forense digital para la red social Twitter

Fuente: Autor

A. Estado Inicial

Este es el primer proceso en el modelo que consiste en:

1) Reconocimiento: Este es el primer paso de una investigación forense de redes sociales, el proceso consiste en establecer detalles de un evento y lo que se espera de la investigación. No hay ningún componente técnico en este proceso.

2) Construcción: después de que se recopilan todos los detalles, se debe construir un plan completo. La planificación incluirá operaciones, infraestructura y autorización de personas u organizaciones relevantes. En nuestro modelo el investigador necesita determinar si hay datos, incluido el perfil del sospechoso o la víctima, o cualquier otra información que pueda ser recopilada de la red y que se puede usar en el proceso de investigación.

B. Investigación

1) Identificación: esta actividad se llevará a cabo mediante la implementación del prototipo a desarrollar. Primero identificaremos cualquier evidencia o información asociada que pueda estar disponible en la red social en línea. Por ejemplo, con el nombre de usuario de un sospechoso o de la víctima se puede realizar una investigación exhaustiva de un caso.
2) Búsqueda: En base a los datos relevantes recopilados del proceso de investigación, realizaremos una búsqueda exhaustiva que nos permita descubrir datos relevantes automáticamente. Hay una gran cantidad de diferentes tipos de datos que se pueden recopilar y utilizar como evidencia o información de respaldo que se podría extraer de la red social.
3) Filtrado: la actividad de filtrado se reducirá y enfocará la investigación en información y descartar cualquier información irrelevante.
4) Captura: La información recopilada a través del filtrado se capturará de la mejor manera garantizando de esta forma la integridad de los datos. Estos datos en sí serán analizados en el siguiente proceso.

C. Análisis

Se realizará un análisis exhaustivo basado en la información recopilada de las actividades anteriores. Esta actividad será apoyada por un módulo en el prototipo a desarrollar.

1) Hipótesis: esta actividad consiste en desarrollar una hipótesis para el caso que respalde cualquier evidencia descubierta y se formula en base a las preguntas expuestas en la Figura 16.

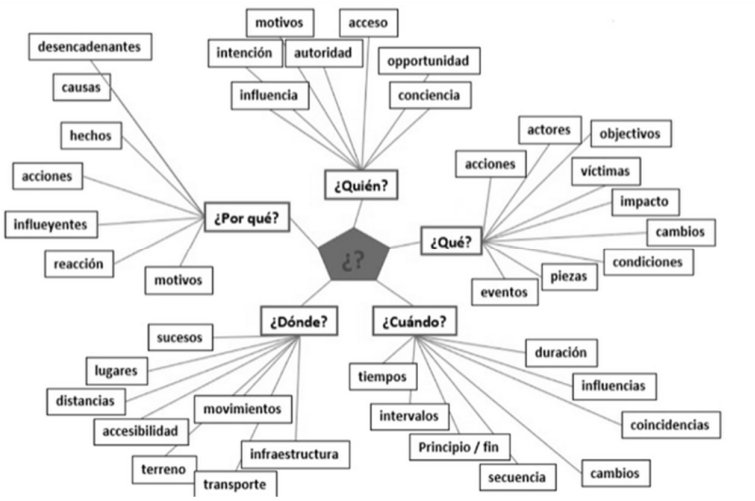


Figura 16 *Elementos a considerar para la generación de hipótesis*

Fuente: Autor

2) Informes: la actividad de informes implicará documentar los datos analizados y la evidencia recopilada del proceso anterior, así como generar un informe detallado de un sospechoso y otros relacionados con el caso.

D. Evaluación

1) Presentación: El informe que se ha preparado en la actividad anterior se presentará a las personas relevantes. Por ejemplo, si se ejecuta un caso policial, el informe se presentará al jurado. Si se trata de una investigación particular, el informe podría presentarse al solicitante.
2) Justificación: En esta actividad, los investigadores deberán racionalizar la validez de la evidencia y deberán defenderla contra cualquier duda o desafío.
3) Revisión: si la evidencia presentada tiene alguna duda razonable, la investigación será revisada. Los investigadores decidirán si deben volver a una de las actividades anteriores para descubrir más evidencia. De lo contrario, esta actividad se puede omitir.

4.1.1 Requisitos para la implementación del modelo propuesto

Se ha de considerar las características que se pueden aplicar en el desarrollo de nuestro prototipo de herramienta. Sobre la base del enfoque de la normativa NIST y en cumplimiento de los requisitos que esta menciona: se debe establecer categorías de requisitos forenses e identificar los requerimientos para una categoría específica, se desarrollara un prototipo que refleje el proceso de nuestro modelo, debe ser capaz de cumplir con los requisitos a continuación detallados para producir una herramienta eficiente para la investigación forense en línea de la red social Twitter.

El prototipo tendrá varias funciones. Para llevar a cabo el proceso crucial de una investigación forense, con las funcionalidades detalladas a continuación:

1) Generación automática: el prototipo de la aplicación será capaz de generar datos basados en consultas realizadas por los investigadores, a partir de entonces hará

el resto del proceso de búsqueda, análisis y reporte de un examen en particular. Por lo tanto, habrá una mínima participación humana en la aplicación del prototipo.

2) Capacidad para buscar y filtrar datos: se desarrollará una técnica para buscar datos automáticamente de acuerdo con las condiciones específicas exigidas. Posteriormente, los datos buscados se filtrarán para descubrir datos relevantes del proceso de búsqueda.
3) Capacidad para informar de manera integral: el prototipo que se desarrollará será capaz de crear un informe basado en el proceso anterior y proporcionará información significativa de la investigación.
4) Capacidad para proporcionar un prototipo eficiente en el tiempo: se centrará en las técnicas para cumplir pasos dentro de la investigación forense digital que tienen la complejidad adecuada. El objetivo es garantizar que se puedan usar en escalas de tiempo realistas.
5) Capacidad para ejecutar y realizar análisis de búsquedas múltiples de las cuentas de redes sociales o correo electrónico: el prototipo podrá buscar y analizar diferentes repositorios de redes sociales para aumentar la cantidad de información que se pueda recopilar.
6) Capacidad para almacenar información: el prototipo deberá contar con una base de datos con dos propósitos, el almacenamiento del contenido de la red social en caso de que a futuro se requiera una auditoria de esta información y la misma haya sido borrada de la red social; también se debe tener en cuenta que el acceso a la información en línea, con el paso del tiempo, se limita a cierto número de publicaciones no a todo el historial de un usuario.

4.1.2 Descripción del funcionamiento del modelo a implementar

A continuación, se sintetizará la forma en que funcionará el script, en base a lo propuesto por la normativa NIST en este punto desarrollaremos afirmaciones basadas en los requisitos expuestos en el punto anterior.

El modelo se divide en dos entornos: el físico y el digital; y, a su vez los procesos en el entorno digital lo componen dos módulos que son: investigación y análisis.

Del entorno físico se obtendrá un usuario de Twitter es decir el nombre de usuario de la red social del que se requiere recopilar información, a este usuario que se encuentra bajo investigación se le atañen la autoría de publicaciones que derivan en la infracción de alguno de los delitos tipificados en el COIP.

Las siguientes afirmaciones se implementarán en lo que consideramos el entorno digital de nuestro modelo.

1. En primera instancia se verificará el post realizado por un usuario y la relación que podría tener con el denunciante, o, ciertas expresiones consideradas controvertidas.

2. La información filtrada por nombre de usuario, fecha de publicación del tweet y mención al denunciante será almacenada en un producto denominado *usuario*_tweet.csv, la información sin ningún tipo de filtro contenida en el muro de publicaciones del usuario será almacenada en la base de datos bd_tweepy

tabla tbl_respaldo con la finalidad de garantizar el acceso posterior en caso de una auditoria o revisión del caso.

3. Con la constatación del hecho se procederá a recabar información de este usuario en base al contenido de su perfil de Twitter. Obteniendo como resultado un producto denominado *usuario*_perfil.csv

4. También se requiere la información concerniente a la búsqueda del usuario bajo investigación y su interacción en otras redes sociales o plataformas. Datos que serán almacenados en un producto llamado *usuario*_profiles.csv

5. Del mismo usuario se obtendrá un correo electrónico que se encuentra asociado a la cuenta de la red social Twitter, información contenida en el archivo *usuario*_mails.csv

6. Para poder llevar a cabo una investigación que desanonimice al usuario ya que la información del perfil o nombre de usuario pueden ser convenientemente creados para inculpar a terceros, se realizara una búsqueda del número telefónico asociado a la cuenta de Twitter. Deriva en el producto *usuario*_fono.csv.

7. Se garantizará que los archivos .csv generados en los procesos antes mencionados no serán alterados creando un hash de la información contenida en cada uno de ellos y almacenando este dato en la base de datos bd_tweepy tabla tbl_respaldo_hash

8. Antes de la generación del informe se ejecutará un código de revisión del hash de los archivos .csv que se planea usar para la realización de este informe, en caso de que se hayan alterado el resultado del hash no será concordante con el almacenado en la base datos y no permitirá la ejecución del siguiente paso.

9. La información debe estar contenida en un documento con validez procesal, es decir firmado electrónicamente y con un sello temporal que reunirá la información antes obtenida en un solo archivo y contendrá los datos del solicitante de dicho informe y los datos de la persona que lo elaboro expresados a través la firma electrónica. Producto final formato PDF.

La funcionalidad del modelo propuesto nace de que los puntos mencionados no son concatenados se pueden ejecutar individualmente en base a que el proceso de investigación es reiterativo y puede manejar varias hipótesis, se busca que se puedan realizar búsquedas independientes del resultado obtenido del módulo anterior.

4.1.2.1 Tipos de datos a ser recolectados

La adquisición de datos fidedignos es crucial, para el proceso de recolección de evidencia forense en Twitter, considerando la estadística del año 2019 publicada por Pew Research y detallada en la sección de Levantamiento de Información, el número de publicaciones de un usuario asiduo de la red social tiene como media 138 posteos mensuales, bajo esta premisa se espera recabar información de al menos 1656 publicaciones que corresponderían a la información posteada un año previo a la

denuncia, considerando que la API REST de Twitter tiene una capacidad definida de extracción para una cuenta developer estándar de 3200 publicaciones como número máximo de descarga de tweets, se establece que el nivel de extracción de información es suficiente e inclusive supera el límite requerido.

Los siguientes requerimientos serán considerados como requisitos mínimos:

1. Acceso a la información contenida en la red social Twitter, esta información comprende tweets, información del usuario, sobre todo los nombres de usuario conocidos como '*username'*. Acorde a lo detallado en la Tabla 13.

Tabla 13 Información a ser recolectada de Twitter

User	name
	screen_name
	description
	location
	created_at
	Friends
	Followers
Tweet	tweet_ID
	created_at
	text
	URL Tweet

Fuente: Autor

2. Búsqueda de cuentas que usen el mismo nombre de usuario en otras redes sociales, plataformas digitales, sitios web, foros, etc.; procurando otras fuentes de investigación.

Tabla 14 Información a ser recolectada de usuario en otras plataformas

Plataforma	username	URL Validacion Plataforma

Fuente: Autor

3. Localización de direcciones de correo electrónico contenidas en servidores públicos asociadas al '*username'* y que realizan procesos de autenticación en la plataforma Twitter.

Tabla 15 Información a ser recolectada de correos electrónicos y plataformas de autenticación asociadas

Correos electronicos	Mail	Plataforma de Autenticacion

Fuente: Autor

4. Búsqueda de números telefónicos en el historial de publicaciones de Twitter, ver Tabla 16, y, conexión a una fuente de datos que contenga los números celulares recabados del dispositivo móvil del afectado ver Tabla 17.

Tabla 16 Información a ser recolectada de Twitter

Tweet	username
	tweet_ID
	created_at
	text

Fuente: Autor

Tabla 17 Información que se espera de dispositivo móvil

Dispositivo Movil	Contactos
	Numeros Celulares de Llamadas
	Numeros Celulares de Mensajes

Fuente: Autor

5. Los datos contenidos en los archivos antes mencionados serán sometidos a un proceso de hashing garantizando así su autenticidad y no modificación.

Tabla 18 Información que se espera de archivos .csv

Archivos .csv	Hash

Fuente: Autor

4.1.2.2 Acceso a datos de Twitter

Para acceder a la información de Twitter se usará Tweepy que es una biblioteca de Python. Es ideal para la automatización simple o la creación de bots de Twitter. Tweepy puede extraer los metadatos de:

- Tweets
- Perfil de usuario
- Retweets
- Entidades
- Mensajes directos
- Seguidores

Tabla 19 Resumen Tweepy

Source	https://github.com/tweepy/tweepy
Autor	Joshua Roesslein
Licencia	GPLv2

Fuente: Autor

Antes de poder acceder a las credenciales de API de Twitter, se debe realizar una solicitud de una cuenta de desarrollador en Twitter. Una vez aprobada la aplicación, se podrá obtener acceso a las claves Access Token, Access Token Secret y de usuario Consumer Key (API Key), Consumer Secret (API Secret). A través de la autenticación de forma segura con el protocolo OAuth (Open Authorization), el usuario se conectará sin compartir su información

4.1.2.3 Almacenamiento del contenido de Twitter en base de datos

Para el almacenamiento de las publicaciones del timeline del usuario investigado se utilizará la base de datos relacional MariaDB Server realizada por los desarrolladores originales de MySQL. Es predeterminada en la mayor parte de las distribuciones de Linux.

Por sus características de compatibilidad con Oracle Database y Temporal Data Tables, permite consultar los datos tal como estaban en cualquier momento del pasado.

Tabla 20 Resumen Youtube Video Downloader

Source	https://downloads.mariadb.com/MariaDB/mariadb_repo_setup
Autor	MariaDB Team
Licencia	GPLv2

4.1.2.4 Descarga de imágenes y videos contenidos en Tweet

A través del programa de línea de comandos youtube-dl se puede realizar la descarga de vídeos o extraer audio de sitios de streaming. Porgrama desarrollado en Python, que lo hace multiplataforma. Administrable bajo dominio público no licenciado.

Tabla 21 Resumen Youtube Video Downloader

Source	https://github.com/ytdl-org/youtube-dl
Autor	Ricardo García
Licencia	GPLv3

Fuente: Autor

Mediante el uso del módulo *requests* de Python y el módulo *wget* de Python también se puede usar para descargar la imagen de la URL en un archivo local fácilmente.

Tabla 22 Resumen Requests

Source	https://github.com/psf/requests
Autor	Kenneth Reitz
Licencia	Apache 2.0

Fuente: Autor

4.1.2.5 Acceso a URL de Twitter e Impresión de pantalla

Selenium Webdriver es una versión mejorada de Selenium RC y la herramienta más utilizada. Acepta comandos a través de la API del cliente y los envía a los navegadores. En pocas palabras, Selenium Webdriver es un controlador específico del navegador que ayuda a acceder y ejecutar los diferentes navegadores. Proporciona una interfaz para escribir y ejecutar scripts de automatización. Cada navegador tiene diferentes controladores para ejecutar pruebas.

Tabla 23 Resumen Selenium

Source	https://www.selenium.dev/downloads/
Autor	Jason Huggins
Licencia	Apache 2.0

Fuente: Autor

Chromedriver permite realizar pruebas automatizadas de aplicaciones web en diferentes navegadores. Implementa el estándar W3C WebDriver como servidor independiente. Está habilitado para Chrome en Android y Chrome de escritorio en diversos sistemas operáticos incluido ChromeOS.

Tabla 24 Resumen Chromedriver

Source	https://chromedriver.chromium.org/downloads
Autor	Google
Licencia	Apache 2.0

Fuente: Autor

4.1.2.6 Conexión cuenta de Twitter a otras redes sociales y correos electrónicos

La consulta y búsqueda de usuarios en otras plataformas de redes sociales se realizará a través de APIs *opensource* como OSRFramework que ofrece las dos opciones necesarias. Su implementación también se realiza en Python.

De la herramienta OSRFramework se utilizarán dos funcionalidades para la búsqueda de usuarios en otras redes sociales; haciendo uso de la aplicación usufy se realizará la búsqueda en distintas plataformas, a la fecha la conforman 306 plataformas como foursquare, github, pornhub, mercadolibre, facebook, twitch, youtube, instagram entre las más destacables. Comprueba con los usuarios existentes de las páginas mediante una respuesta de la web obtenida al acceder a un perfil de un usuario. Maneja una librería de adaptadores para las diferentes plataformas.

Como parte de la indagación de correo electrónico o direcciones de correo se utilizará la plataforma mailfy que explora 22 plataformas de correo públicas entre las más importantes se encuentra icloud.com, gmail.com. la respuesta RCPT TO o respuesta del protocolo de correo SMTP informa la existencia de la cuenta en el servidor de correo. Sin embargo, existen servidores de correo que admiten estos mensajes, a pesar de la inexistencia de la cuenta, evitando de esta forma la obtención automática de direcciones válidas evitando el envío masivo de correos (spam).

Tabla 25 Resumen OSRFramework

Source	https://github.com/i3visio/osrframework_console
Autor	i3visio Team
Licencia	GPLv3

Fuente: Autor

4.1.2.7 Obtención de datos de dispositivo móvil

Santoku es una distribución desarrollada como una bifurcación del OWASP (Proyecto de seguridad de aplicaciones web abiertas). Santoku puede ser instalado como una máquina virtual o como un sistema operativo (sistema operativo). Con Santoku, un examinador forense o principiante puede descargar, instalar y comenzar a utilizar un conjunto de herramientas forenses móviles gratuitas. La entrega de resultados es en cuestión de minutos.

Además, Santoku contiene herramientas que permiten al examinador para realizar adquisiciones e investigaciones tanto en iOS como en Android Mobile OS. En los Anexos se detalla el funcionamiento de esta herramienta para la extracción de una base de datos con los números celulares almacenados en un dispositivo móvil

Tabla 26 Resumen Santoku

Source	https://santoku-linux.com/
Autor	Now Secure
Licencia	GPLv3

Fuente: Autor

4.1.2.8 Obtención de hash en archivos .csv

Con el uso del módulo hashlib que incluye los algoritmos de hash seguros SHA256, SHA512, MD5, entre otros y mediante el método constructor se obtendrá un objeto hash alimentado por bytes a través del método update(), resumido con los métodos digest() o hexdigest().

Tabla 27 Resumen Hashlib

Source	https://github.com/python/cpython/blob/3.9/Lib/hashlib.py
Autor	Alexandr Sokolovskiy
Licencia	GPLv3

Fuente: Autor

4.1.2.9 Creación de PDFs

ReportLab herramienta de código abierto que funciona como motor para la creación de documentos PDF basados en datos y gráficos vectoriales personalizados. Herramienta de código abierto desarrollada en Python. Su biblioteca comprende tres capas:

- API para lienzo de gráficos que esquematiza las páginas PDF
- Biblioteca de gráficos y widgets que permite crear gráficos de datos reutilizables.
- Motor de diseño de página - PLATYPUS ("Diseño de página y tipografía usando scripts") - crea documentos partiendo de elementos como titulares, párrafos, fuentes, tablas y gráficos vectoriales.

Tabla 28 Resumen Reportlab

Source	https://www.reportlab.com/dev/downloads/
Autor	ReportLab
Licencia	GPLv3

Fuente: Autor

4.1.2.10 Firmado y sellado de documentos

Endesive es una biblioteca de Python para firma digital y verificación de firmas digitales en documentos de correo, PDF y XML.

Tabla 29 Resumen Endesive

Source	https://pypi.org/project/endesive/
Autor	Grzegorz Makarewicz
Licencia	GPLv3

Fuente: Autor

4.1.3 Herramientas integradas

El entorno virtualizado utilizado está montado en VirtualBox con sistema operativo KALI Linux de 64 bits. Partiendo de configuraciones necesarias que permitirán ejecutar la aplicación bajo la ejecución de dependencias y complementos a continuación detallados.

El prototipo está diseñado asegurando compatibilidad con otros sistemas GNU/Linux, bajo la premisa de que los mismos dispongan el intérprete de Python (versión 3.8).

Tabla 30 Resumen de herramientas integradas

Parte	Etapa	Modulo	Programa		
			Aplicación	***Versión***	***Call***
1	I	Búsqueda Tweet	Tweepy	3.9.0	Shell
2	I	Almacenamiento Tweets	MariaDB	15.1	Shell
3	I	Búsqueda de perfil de usuario	Tweepy	3.9.0	Shell
4	I	Descarga Imágenes o Video	Youtube-dl / Request	2020.07.28	Shell
5	I	Acceso a URL contiene Tweet y captura de pantalla	Selenium	3.141.0	Shell
6	II	Búsqueda de usuario en otras plataformas	usufy.py	0.18.0	Shell
7	III	Búsqueda de correo electrónico asociado a Twitter	mailfy.py	0.18.0	Shell
8	IV	Búsqueda de Número Telefónico	Tweepy	3.9.0	Shell
9	IV	Búsqueda de Número Telefónico	Santoku	0.5	NA
10	V	Generación Hash archivos .csv	Hashlib	2.5	Shell
11	V	Generación reporte	Reportlab	3.5.50	Shell
12	V	Firmado Reporte	Endesive	1.15.12	Shell

Fuente: Autor

4.1.4 Diseño del prototipo de aplicación

En esta sección discutiremos sobre el diseño del prototipo de aplicación que será una herramienta para representar los procesos en el entorno digital como se describe en nuestro modelo de la Figura 15. Básicamente dividiremos nuestro prototipo de forensia digital en dos módulos que son: investigación y análisis. Cada módulo seguirá los procesos del modelo, se ha considerado que la fase de obtención de números celulares es una segunda etapa de investigación debido a que deriva de la primera ronda de obtención de datos. Esta aplicación toma el nombre TFT Técnicas Forenses en Twitter.

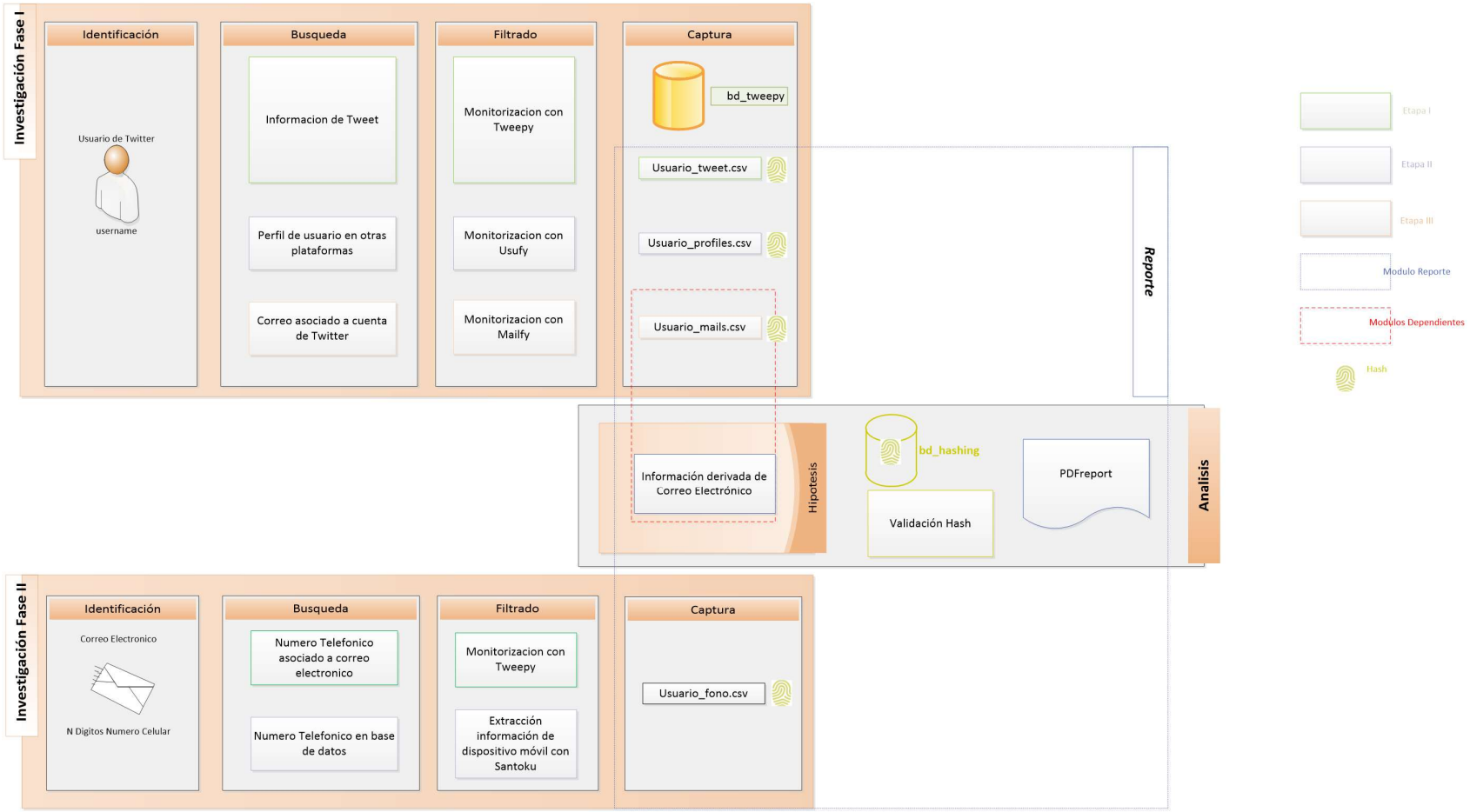


Figura 17 Interacción entre componentes aplicación TFT Técnicas Forenses en Twitter

Fuente: Autor

A. Módulo de investigación

Este módulo se centrará en la investigación. La sección de Modelo Propuesto ha descrito los procesos involucrados en este módulo que son identificación, búsqueda, filtrado y captura. La figura 18 ilustra el diagrama de flujo que aclara todo el proceso en este módulo.

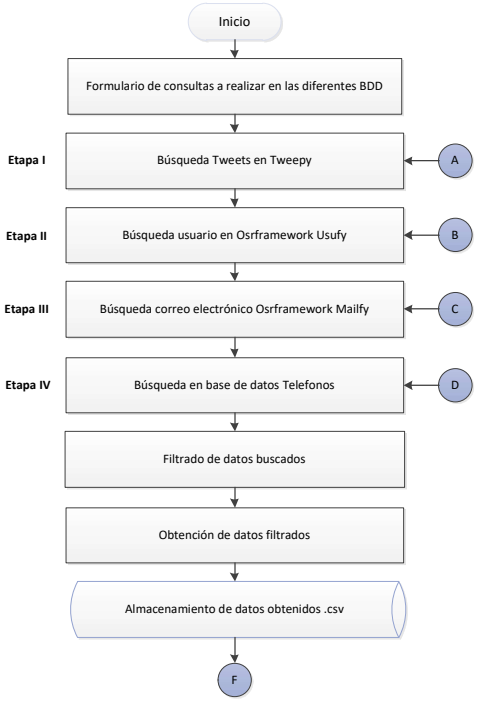


Figura 18 Diagrama de Flujo de Datos en el módulo Investigación

Fuente: Autor

Como podemos ver, el diagrama de flujo corresponde a la actividad de investigación en nuestro modelo propuesto y cumple con los requisitos de implementación de modelo. El usuario debe responder una lista de consultas, que pueden responderse en función de la información proporcionada por el equipo de aplicación que solicitó esta investigación o la investigación física que se realizó en la actividad anterior.

Etapa I - Búsqueda de un Tweet

El proceso de consulta depende de la etapa de búsqueda que se haya iniciado, para la Figura 20 se detalla la Etapa I y requiere como variables de entrada el nombre de usuario que se investigará, una palabra exacta para coincidencia que podría ser algún indicio al que se quiere apuntar en la investigación o la mención que se ha realizado a un nombre de usuario especifico de la red social @usuariodenunciante y finalmente la variable asociada a la fecha de búsqueda.

La información resultante de la búsqueda por nombre de usuario y fecha de inicio de búsqueda será almacenada en una base de datos con la finalidad de mantener un registro en caso de auditoria o eliminación de la publicación considerando que el tweet puede volverse inaccesible después de iniciado el proceso de investigación. En la figura 19, se detalla el proceso de creación de la base de datos denominada bd_tweepy.

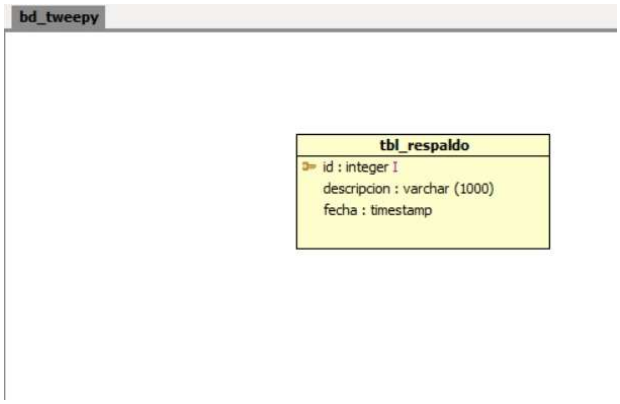


Figura 19 Diagrama de Base de Datos bd_tweepy

Fuente: Autor

Al ejecutarse el proceso de filtrado por palabra clave, la Parte 1 descargara la información que contenga las coincidencias los criterios de búsqueda, realizara una captura de pantalla de la URL asociada al Tweet y descargara los archivos contenidos en el Tweet como imágenes o videos, a continuación, se ejecutara la Parte 2 que generara la identificación de la información del perfil de usuario.

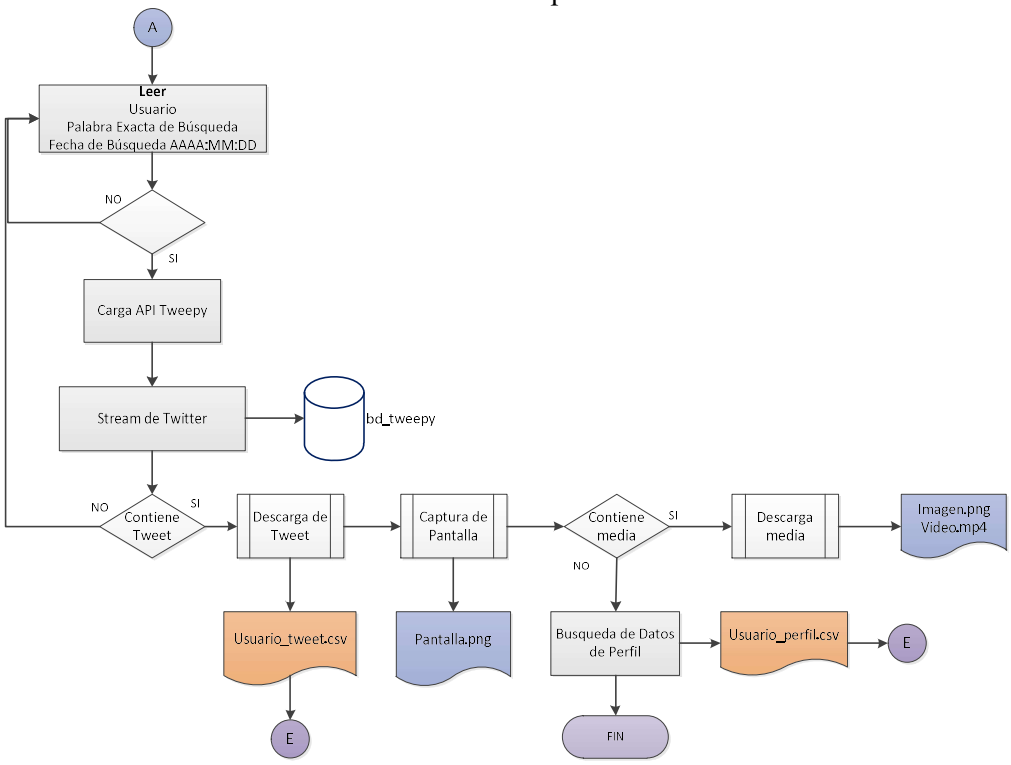


Figura 20 Diagrama de Flujo de los Procesos de búsqueda en módulo de Investigación de un Tweet

Fuente: Autor

Etapa II - Búsqueda de usuario en otras plataformas

Para la etapa de búsqueda del mismo nombre de usuario que está siendo usado en otras redes sociales se realiza el proceso detallado en la Figura 21. Requerirá como variable de entrada el *username* o nombre de usuario que está siendo investigado.

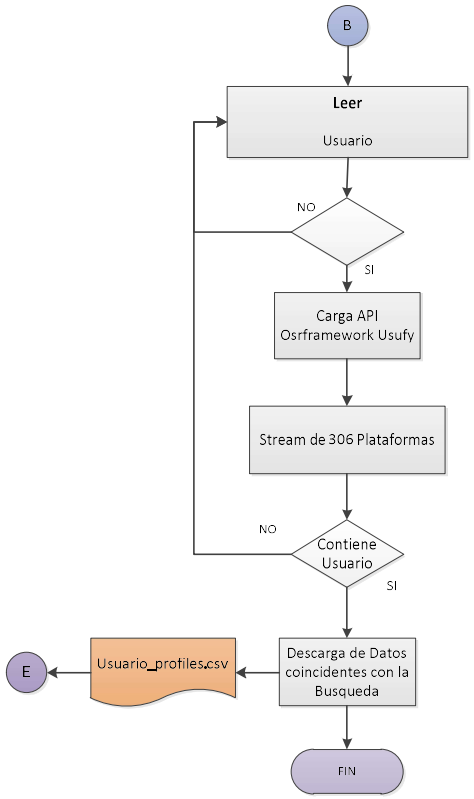


Figura 21 Diagrama de flujo de los procesos de búsqueda en el Módulo de Investigación de un nombre de Usuario en diferentes plataformas

Fuente: Autor

Etapa III - Búsqueda de correo electrónico asociado a Twitter

Para la etapa de Búsqueda del correo electrónico asociado a procesos de autenticación en Twitter se realiza el proceso detallado en la Figura 22. Requerirá como variable de entrada el *username* o nombre de usuario que está siendo investigado.

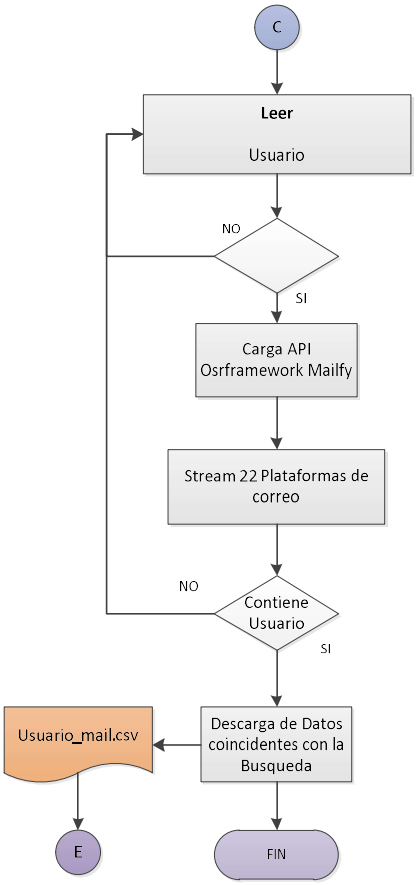


Figura 22 Diagrama de flujo de los procesos de búsqueda en el Módulo de Investigación de correo electrónico usado para autenticación en Twitter

Fuente: Autor

Una vez ejecutadas las 3 etapas previamente mencionadas se puede obtener información más clara del usuario a quien se está investigando y se podría generar una nueva hipótesis para definir a que persona pertenecen todos los datos antes recopilados.

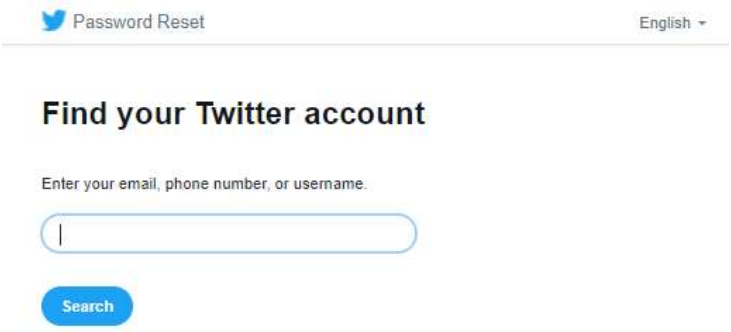


Figura 23 Proceso de recuperación de contraseña de una cuenta en Twitter

Fuente: (Twitter, 2020)

En base al proceso de recuperación de contraseña en la red social Twitter podemos corroborar lo hasta ahora obtenido, Figura 23, al buscar por usuario de la red social, se

va a desplegar la información asociada a la cuenta de donde se puede cotejar el correo electrónico y se obtiene un nuevo dato los dos últimos dígitos correspondientes al número telefónico del usuario de dicha cuenta, acorde a la información contenida en la Figura 24.

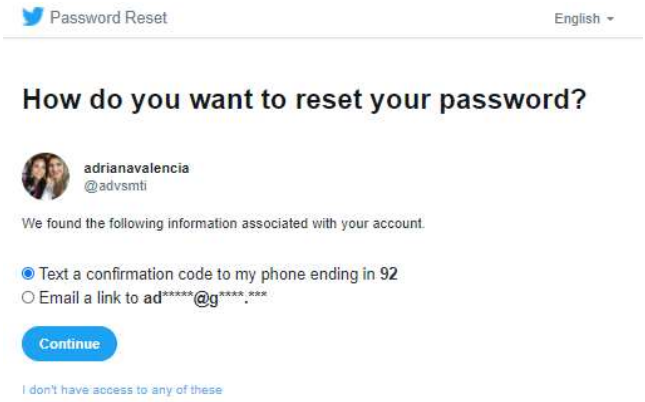


Figura 24 Información asociada a la cuenta de Twitter para recuperación de contraseña

Fuente: (Twitter, 2020)

En base a la verificación del usuario en los links de plataformas obtenidos en la etapa II de investigación se podrá corroborar el país de procedencia del número celular asociado y se obtendrán los 3 últimos dígitos del mismo.

A partir de esta condición se han planteado 3 hipótesis para obtener el número celular completo del investigado

Hipótesis 1, estos 3 dígitos pueden obtenerse y ser concordantes con la información publicada en su historial de Twitter

Hipótesis 2, aplica para casos de acoso, el denunciante puede haber establecido previamente contacto y el dato de número celular puede encontrarse dentro de los datos de contactos, llamadas o mensajes

Hipótesis 3, en la etapa II al ejecutarse Usufy de OSRFramework también realiza una búsqueda de concordancias dentro de la plataforma Telegram, en base a una vulnerabilidad encontrada en la plataforma de mensajería Telegram, al realizar una búsqueda de usuario, ver Figura 25, por defecto podemos realizar llamadas para establecer una comunicación a través de dicha plataforma de mensajería como se puede validar en la Figura 26.

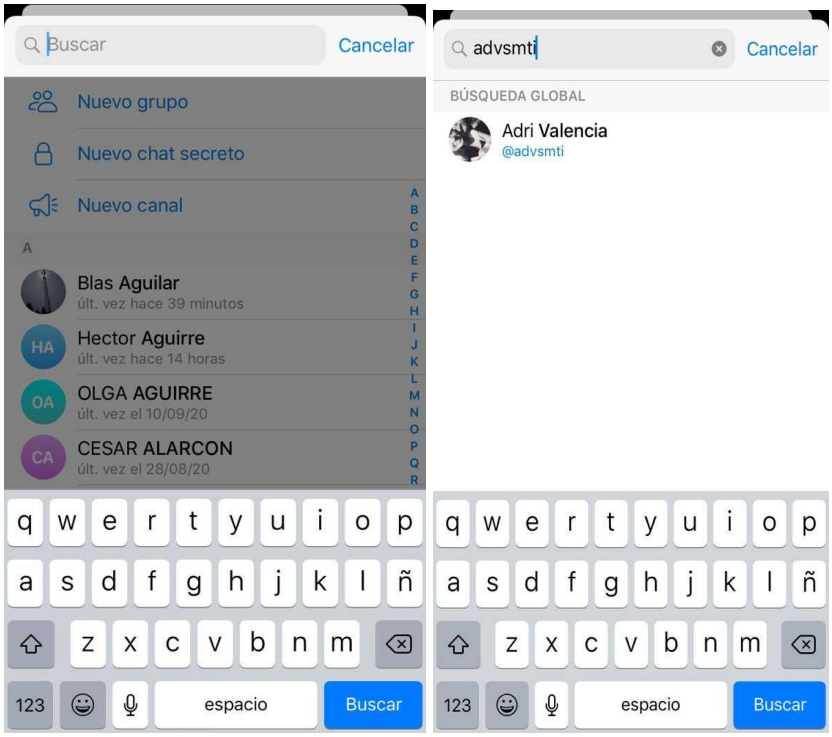


Figura 25 Búsqueda de usuarios en Plataforma de Mensajería Telegram

Fuente: (Telegram, 2020)

Figura 26 Opciones que pueden ejecutarse en la Plataforma de Mensajería Telegram

Fuente: (Telegram, 2020)

La hipótesis 1 y 2 serán aplicadas dentro de este desarrollo, debido a que el establecimiento de comunicación mediante la plataforma de mensajería Telegram es considerado un método intrusivo que atenta contra los derechos del investigado no se puede ejecutar sin orden judicial y no aplicaría dentro de un proceso de denuncia sino en el proceso mismo del juicio si es que un juez da la orden para ejecutar dicho proceso.

Etapa IV - Búsqueda de Número Telefónico

Para la etapa de Búsqueda del número telefónico del usuario y que se encuentra asociado a procesos de autenticación en Twitter se realiza el proceso detallado en la

Figura 27. Requerirá como variable de entrada el *username* o nombre de usuario que está siendo investigado y los dígitos asociados al celular que han sido encontrados resultado de los procesos de recuperación de contraseña en las diversas plataformas.

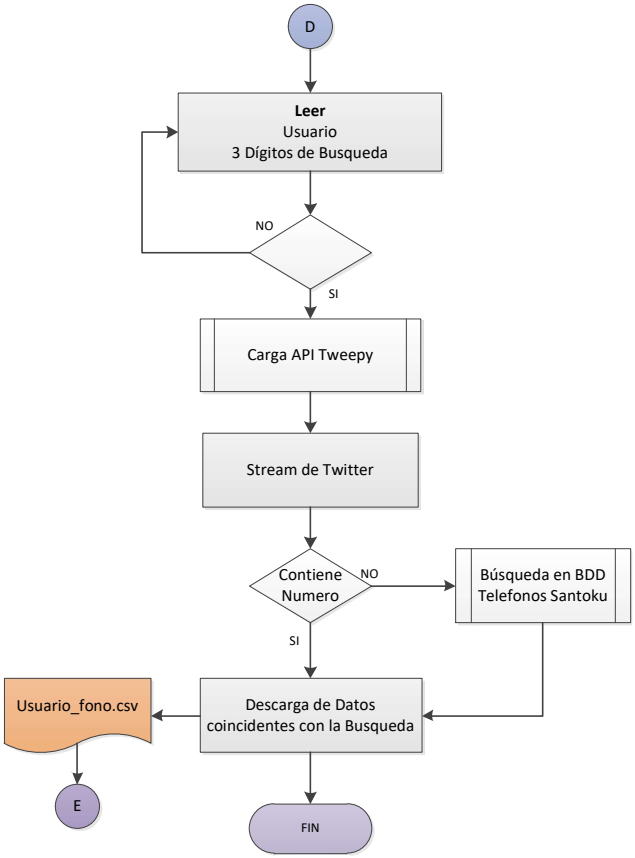


Figura 27 Diagrama de flujo de los procesos de búsqueda de número telefónico de usuario

Fuente: Autor

Las aplicaciones filtraran toda la información relevante en función de los datos ingresados previamente y esta información se capturará y almacenará en los diferentes archivos de captura de datos.

Proceso de generación de hash en archivos .csv

Para cada archivo .csv generado se debe garantizar que su inalterabilidad hasta el proceso de lectura para armado del PDF, se ha propuesto como parte de la solución la generación de un hash por cada archivo y su posterior almacenamiento en la base de datos bd_tweepy tabla tbl_respaldo_hash.

Al generar un hash se debe considerar que el mismo será inalterable siempre que se mantenga el contenido, para la generación del hash no tiene intromisión el nombre del archivo o la modificación de permisos sobre el mismo.

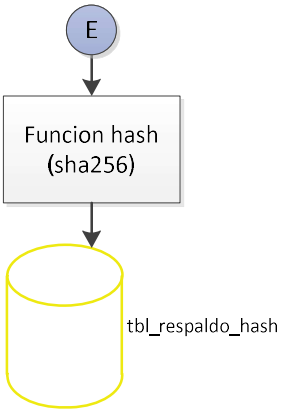


Figura 28 Diagrama de flujo función hash

Fuente: Autor

Proceso validación hash archivos previo generación de informe PDF

Antes de iniciar el proceso de generación de PDF se realizará una validación de los archivos existentes desde donde se planea realizar la extracción de información, para cada archivo existente se ejecutará la función hash y se cotejara con la información contenida en la base de datos, si los hash de los 5 archivos necesarios para la generación del PDF son iguales a los contenidos en la base de datos tabla tbl_respaldo_hash el proceso continuará caso contrario se emitirá un mensaje de error indicando que uno de los archivos se encuentra corrupto.

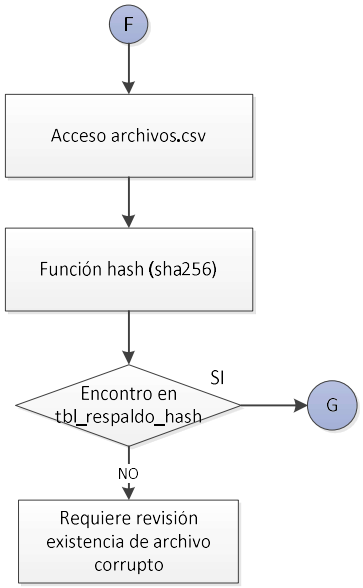


Figura 29 Diagrama de flujo proceso validación hash

Fuente: Autor

B. Módulo de análisis

Este módulo se centrará en analizar y generar un informe completo de nuestro prototipo. La Figura 30 muestra el diagrama de flujo del módulo. Aunque el diagrama de flujo parece simple, el proceso detrás de este módulo es desafiante porque primero necesitamos visualizar y mapear la información recopilada que podrá aclarar las conexiones de la persona que está siendo investigada. Y luego se producirá una hipótesis basada en la información que hemos encontrado. Finalmente, la aplicación producirá un informe completo basado en toda la información que se ha recopilado y se puede usar como evidencia de respaldo en esa investigación en particular.

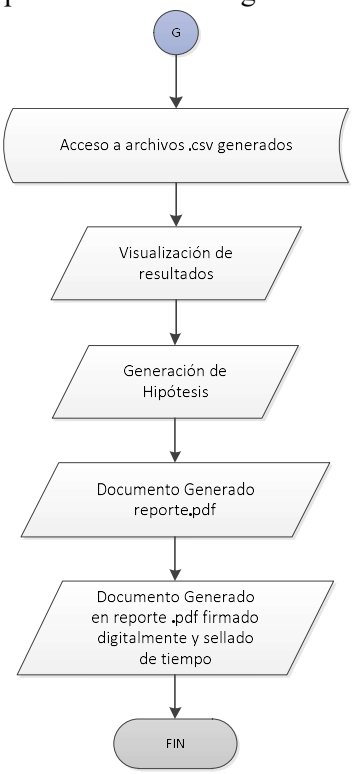


Figura 30 Diagrama de Flujo del módulo análisis

Fuente: Autor

4.1.5 Composición del script

El script será implementado en el lenguaje de programación Python por ser de gran manejo en el ámbito de la seguridad y de la informática forense.

En la siguiente sección se describirá brevemente la implementación en python de los módulos de investigación y análisis, con sus etapas; y, se detallará como se realiza la ejecución de las distintas herramientas tweepy, mailfy, usufy, donde se realiza la extracción de la información con su interfaz correspondiente, también se incluirá el proceso de búsqueda de teléfono celular asociado, el almacenamiento de estos datos y la generación del reporte.

Interfaz Inicial

El usuario de la aplicación tendrá como pantalla de inicio un menú que desplegara aquellas opciones asociadas con las etapas tratadas en los puntos anteriores y que pueden ser ejecutadas, como se describe en el código.

```
print("\n\t")
print("     | |_  |  __| | |_")
print("     |  _| |  |_  |  _|")
print("     | |_  |  __| | |_")
print("     \___| |_|    \___|")
print("\n\tTECNICAS FORENSES APLICADAS A LA RED SOCIAL
TWITTER")
print("\n\tEscoja la opción que se ajuste a su Búsqueda y
digite el numero")
print("[1] Búsqueda y Descarga de Información de Usuario de
Twitter")
print("[2] Búsqueda y Descarga de Nombre de Usuario en otras
plataformas, redes sociales")
print("[3] Búsqueda y Descarga de Información de Usuario y
correos electrónicos asociados")
print("[4] Búsqueda y Descarga de Información relacionada al
Numero Telefónico")
print("[5] Descarga de Información obtenida en formato PDF")
print("\n\nEscoja una opción [1,2,3,4,5] use 'q' para
finalizar")

menuOption = str(input("\n\tLuego de seleccionar una opcion
presione Enter "))
```

Búsqueda y Filtrado de Tweets

El uso de la librería Tweepy nos permite usar la paginación, iterando a través de líneas de tiempo, listas de usuarios, mensajes directos, etc. Para realizar la paginación, en la búsqueda y filtrado de tweets proporcionamos un parámetro al cursor que en este caso es ***user_timeline (screen_name, date_since)*** y a continuación a través de un lazo ***for*** realizamos la búsqueda en cada tweet de una palabra o mención específica. Solo devolverá las coincidencias de username + fecha + palabra exacta.

```
tweets_for_csv = []
cursor = tweepy.Cursor(api.user_timeline, screen_name =
username, since=date_since).items(100) ##Busqueda en
usertimeline de tweets por usuario y fecha
for tweet in cursor:
linea = (tweet.text)
if mencion in linea:
#crea el array obtenido con la informacion de twitter:
username, tweet id, date/time, text
tweets_for_csv.append([username,tweet.id,
tweet.created_at,tweet.text])
```

Almacenamiento de tweets sin filtro de palabra clave en base de datos

Conexión a la base de datos bd_tweepy **pymysql.connect** y creación de un registro en la tabla tbl_respaldo **sql = """INSERT INTO** con la información contenida en la API Tweepy de un tweet con la información sin filtrar de usuario, fecha de publicación, fecha de creación y URL del tweet.

```
 #insercion en la base
            db =
pymysql.connect("localhost","utweepy","1234","bd_tweepy" )
            bdi = db.cursor()
            text='usuario: '+str(username)+' Fecha Publicacion:
'+str(created_at)+' Texto: '+str(linea)+' URL Tweet:
'+str(status_url)
            #metodo para insertar en la base
            sql = """INSERT INTO tbl_respaldo(descripcion)
            VALUES(' """+text+""" ')"""
            bdi.execute(sql)
            db.commit()
            db.close()
```

Captura de Pantalla de Twitter con contenido del Tweet
Con la finalidad de tener una imagen de twitter que respalde la información que ha sido extraída se realiza una captura de pantalla del Tweet en la red social, para ello a través de los webdriver del navegador Chrome se ejecuta un script que imprima el contenido de la ventana y lo almacene en una imagen de extensión .png

```
driver=webdriver.Chrome()
driver.get(status_url)
time.sleep(5)
S = lambda X: driver.execute_script('return
document.body.parentNode.scroll'+X)
driver.set_window_size(S('Width'), S('Height'))
driver.find_element_by_tag_name('body').screenshot(username+".pn
g");
```

Descarga de imágenes y videos contenidos en el Tweet
Como parte del proceso de forensia se necesita almacenar el contenido del Tweet que corresponde a media para ello a través del comando ***ydl.download*** o ***requests.get*** aplicable a imágenes se descargara la URL contenida en el metadato entities del Tweet.

```
if 'video' in medialinea:
print ("contiene video a descargarse de " + medialinea)
try:
download_path = str(Path(download_location, "%(id)s.%(ext)s"))
ydl_opts = {
```

```
"outtmpl": download_path,
"quiet": True,
}
with youtube_dl.YoutubeDL(ydl_opts) as ydl:
ydl.download([videos, ])
except Exception as e:
continue
else:
print ("contiene imagenes a descargarse de " + medialinea)
try:
result = requests.get(medialinea)
file = open(tweet.id+".png", "wb")
```

Generación y almacenamiento de hash de archivos .csv

Mediante la librería ***hashlib.sha256*** obtenemos el hash del archivo .csv, ***hexdigest*** devuelve como una cadena de doble longitud conteniendo solo dígitos hexadecimales, se almacena el hash en la tabla tbl_respaldo_hash ***bdi.execute(sqlhashp)***

```
BLOCKSIZE = 65536
        hasher = hashlib.sha256()
        with open(outfile, 'rb') as afile:
            buf = afile.read(BLOCKSIZE)
            while len(buf) > 0:
                hasher.update(buf)
                buf = afile.read(BLOCKSIZE)
        ##print(hasher.hexdigest())##para ver que codigo
del hash
        #guardar campos en la base
        h1=str('\''+ hasher.hexdigest()+ '\'')
        narchivo=','+str('\''+outfile+ '\'')
        estadoar=','+str('\''+'i'+ '\'')
        #i=insertado
        #e=encontrado
        #c=caducado
        print(hasher.hexdigest())
        ##conexion a base de datos
        #db =
pymysql.connect("192.168.100.27","root","root","bd_tweepy"
)
        #cursor = db.cursor()
        ###metodo para insertar en la base
        sqlhashp = """INSERT INTO
tbl_respaldo_hash(descripcion_hash,nombre_archivo,estado_ar
chivo)    VALUES("""+h1+narchivo+estadoar+""")"""
        bdi.execute(sqlhashp)
        db.commit()
```

Búsqueda de Información del perfil de usuario

Para ejecutar la búsqueda requerida de información de perfil basaremos la extracción de datos a través del Twitter API wrapper ***API.get_user*** en este caso se extraerá la metadata del perfil concerniente a nombre de pantalla, descripción, ubicación, fecha de creación de cuenta, seguidores y amigos o usuarios seguidos.

```
item=api.get_user(username)
        #creo el array de la informacion del perfil
        nombre=item.name
        nombrepantalla=item.screen_name
        descripcion=item.description
        ubicacion=item.location
        imprimir=[nombre,nombrepantalla,descripcion,ubicacion]
```

Búsqueda Usuario en otras plataformas

A través el módulo usufy de la aplicación OSRFramework identificaremos los perfiles de redes sociales o plataformas que usa el investigado, usando el *username* como argumento de Entrada, en usufyArgs, tendremos como Salidas: Perfiles conocidos en redes sociales que utilizan e mismo *username*.

```
usufyArgs=["-n"] + [str(usuario1)] + ["-o"] + ["./profiles"] +
["-F"] + [str(usuario1)+"_profiles"]
        parser= usufy.get_parser()
        args= parser.parse_args(usufyArgs)
```

Búsqueda Correo electrónico asociado a procesos de autenticación

A través el módulo mailfy de la aplicación OSRFramework identificaremos el correo electrónico usado para autenticación en Twitter, usando el *username* como argumento de Entrada, en mailfyArgs, tendremos como Salidas: Perfiles conocidos en redes sociales que utilizan e mismo *username*.

```
mailfyArgs=["-n"] + [str(usuario2)] + ["-o"] + ["./profiles"] +
["-F"] + [str(usuario2)+"_mails"]
        parser = mailfy.get_parser()
        args = parser.parse_args(mailfyArgs)
```

Búsqueda número telefónico en el historial de Twitter

Tweepy da acceso a realizar la paginación, en la búsqueda y filtrado de tweets proporcionado solo un parámetro al cursor que en este caso es *user_timeline (screen_name)* para extraer todo el historial del usuario y a continuación a través de un lazo *for* realizamos la búsqueda en cada tweet en el contenido del texto, tweet.text de la información relacionada al número celular.

```
tweets_for_csv = []
        cursor = tweepy.Cursor(api.user_timeline, screen_name =
usuario3).items(1000)
        for tweet in cursor:
            linea = (tweet.text)
            if telefono in linea:
vardescripcion=tweets_for_csv.append([usuario3, tweet.id,
tweet.created_at, tweet.text])
```

Búsqueda número telefónico asociado en base de números telefónicos obtenidos con Santoku

De la información recabada por la herramienta forense Santoku de un dispositivo móvil y contenida en un archivo de texto plano, se leerá la información de dicho archivo *open (archivo)* y se realizará la búsqueda de la coincidencia por numero celular a través de un lazo *for*

```
open('/home/adrival/Desktop/telfwhats.txt','r') as f:
                    for linea in f:
                        NumeroLinea1=NumeroLinea1+1
                        PosicionTexto1=linea.find(telefono)
                        if PosicionTexto1>=0:
                            print ("El numero telefonico se
encuentra en su base en la linea %i" % NumeroLinea1)
                            uvarnumero=linea
                            vardescripcion="base datos"
                            print ("y es:" + linea)
                            break
```

Validación hash archivos .csv

Desde la tabla tbl_respaldo_hash se toma el valor del hash y se compara con el hash del archivo desde el que se va a leer la información para generar el PDF, si los hash son concordantes avanzara a la siguiente etapa

```
        cont=0
        #print(hashidtw)
        sql1 = "SELECT id_hash FROM tbl_respaldo_hash where
descripcion_hash="+hashidtw+" and estado_archivo='i'" +";"
        bdi.execute(sql1)
        results = bdi.fetchall()
        #print(sql1)

        for row in results:
            id = row[0]
            idu=int(row[0])
            print(idu)
            if idu>0:
                cont=cont+1
```

Reporte PDF con los datos previamente obtenidos

Los documentos generados en las etapas anteriores y que fueron descargados como archivos .csv serán compilado y presentados en un informe, a través de un template simple contenido en ReportLab ,*doc = SimpleDocTemplate,* se generara un documento pdf que tendrá por nombre la cedula del afectado o solicitante del reporte.

```
        textof='%s' %formatoFecha
        pdfn=ruta+cedula+".pdf"
        doc = SimpleDocTemplate(pdfn, pagesize=letter,
                rightMargin=72, leftMargin=72,
                topMargin=72, bottomMargin=18)
```

Firmado y sellado de reporte PDF

Para finalizar acorde al principio de integridad se debe sustentar la inalterabilidad y totalidad de la información a través de la firma electrónica y sellado de tiempo del documento previamente generado, *p12 = pkcs12.load_key_and_certificates*.

```
pfx=ruta+pfxo+".p12"#".pfx"
        date = datetime.datetime.utcnow() -
datetime.timedelta(hours=12)
        date = date.strftime("D:%Y%m%d%H%M%S+00'00'")
        dct = {
                "aligned": 0,
                "sigflags": 3,
                "sigflagsft": 132,
                "sigpage": 0,
                "sigbutton": True,
                "sigfield": "Signature1",
                "sigandcertify": True,
                "signaturebox": (470, 840, 570, 640),
                "signature": "Digitally Signed by Adriana
Valencia",
                #        "signature_img": "signature_test.png",
                "contact": "avalencia.mti@uisek.edu.ec",
                "location": "Quito-Ecuador",
                "signingdate": date,
                "reason": "Este documento ha sido firmado",
                "password": clave,
                }
        with open(pfx, "rb") as fp:
            p12 = pkcs12.load_key_and_certificates(fp.read(),
b"1234", backends.default_backend())
            fname = str(cedula)+".pdf"
```

4.1.6 Detalle de las Interfaces de Usuario

En detalle se presentan las pantallas que conforman el prototipo, con su respectiva descripción

Al acceder el usuario podrá observar una pantalla con un menú de opciones donde se desglosa la información que puede ser obtenida por el programa de TECNICAS FORENSES APLICADAS A LA RED SOCIAL TWITTER en sus siglas TFT, ver Figura 31.

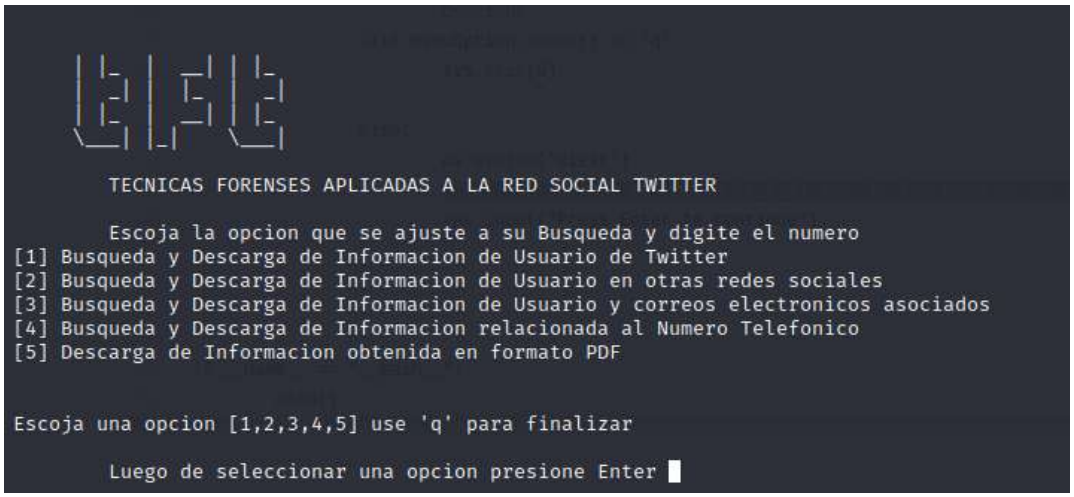


Figura 31 Pantalla Principal Programa Técnicas Forenses Aplicadas a la Red Social Twitter TFT

Fuente: Autor

Para acceder a la opción (1) que corresponde a la Etapa I Búsqueda y Descarga de Información de Usuario de Twitter se desplegaran las opciones detalladas de la figura 32.

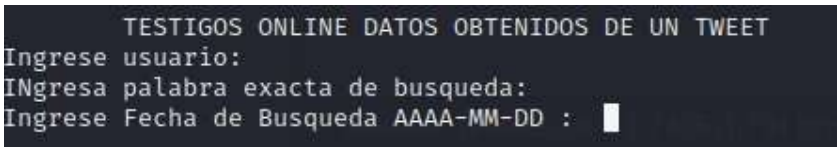


Figura 32 Pantalla Datos Obtenidos de un Tweet

Fuente: Autor

Dentro de la opción (2) que corresponde a la Búsqueda y descarga de información del nombre de usuario en otras redes sociales, se desplegaran las opciones detalladas en la figura 33.

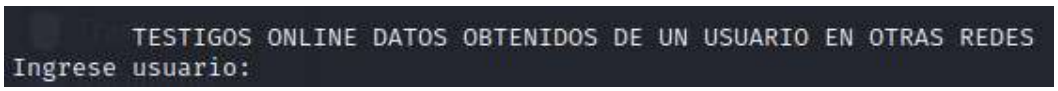


Figura 33 Pantalla Datos Obtenidos de usuario en otras redes o plataformas

Fuente: Autor

Para la opción (3) que contiene a la etapa de Búsqueda y descarga de información de Usuario por correos electrónicos asociados a procesos de autenticación en Twitter se tiene el ingreso de la información detallada en la figura 34.

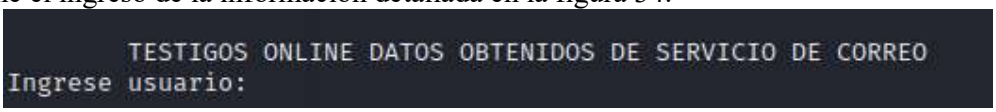


Figura 34 Pantalla de Servicios de Correo

Fuente: Autor

Al ejecutar la opción (4) que deriva de las anteriores etapas y permite realizar la Búsqueda de Número Telefónico se ingresaran los datos indicados en la figura 35, considerando que previamente se ha establecido que, de la revisión en las diferentes plataformas, se han encontrado al menos los últimos 3 dígitos del numero celular del investigado

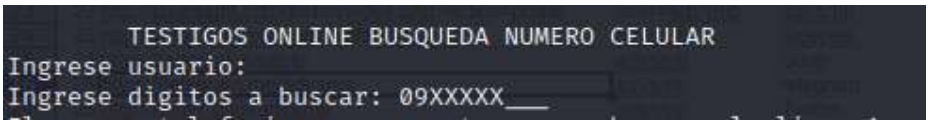


Figura 35 Pantalla Búsqueda Numero Celular

Fuente: Autor

Como un producto final dentro del módulo análisis se tiene la opción de conseguir un archivo PDF que contiene la información extraída en los .csv generados por cada etapa previa, dentro de la opción (5) Descarga de Información de Usuario y Número Telefónico obtenida a formato PDF se tendrá entonces el ingreso de las siguientes variables:

a) Ingreso del usuario de Twitter del que se va a realizar el informe

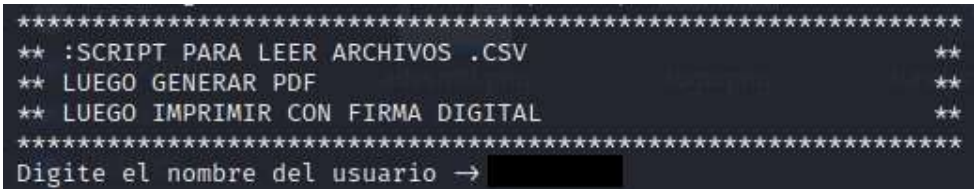


Figura 36 Pantalla Generación Archivo PDF

Fuente: Autor

Una vez se ha realizado la validación de hash entre documentos entrantes vs hash almacenado en la base se podrá realizar el informe caso contrario el proceso se detendrá

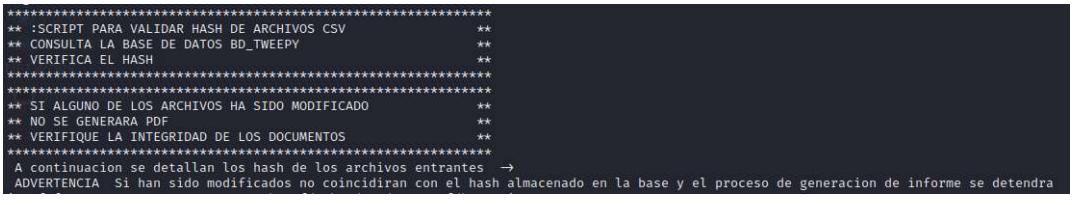


Figura 37 Pantalla Validación Hash archivos

Fuente: Autor

Si el proceso ha sido exitoso solicitara el ingreso de los datos correspondientes al solicitante del informe

a) Nombre del solicitante
b) Numero de Cedula de Identidad del Solicitante

```
Digite el nombre completo de la persona que realiza esta solicitud →
Digite la cedula del solicitante → [redacted]
*****INICIA PROCESO DE GENERACION DE PDF*****
PDF generado exitosamente!
*****INICIA PROCESO DE FIRMADO DIGITAL*****
```

Figura 38 Pantalla Generación Archivo Firmado Digitalmente

Fuente: Autor

Para obtener el archivo firmado digitalmente y sellado en el tiempo se debe tener el archivo de la firma digital en formato .p12 o .pfx, Figura 37, dentro del módulo que genera el reporte.

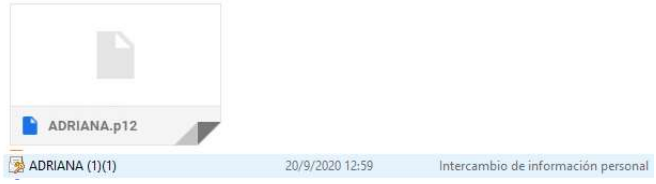


Figura 39 Ejemplo de Archivo con Firma Digital

Fuente: Autor

A continuación, para el firmado y sellado se solicitarán los datos concernientes al nombre del archivo que contiene la firma electrónica y la clave que habilita dicha firma. Figura 38.

```
*****INICIA PROCESO DE FIRMADO DIGITAL*****
Digite el nombre del archivo .pfx (firma digital)      → [redacted]
Digite la clave para la firma digital      → [redacted]
```

Figura 40 Requisitos para generación de archivo con firma electrónica

Fuente: Autor

CAPITULO IV

VALIDACION EMPIRICA

5.1 Método

Debido a que la propuesta requiere el uso de datos reales personales obtenidos de la red social Twitter y considerando posibles conflictos legales y éticos por el uso y manejo de dichos datos, en la prueba de funcionamiento se utilizaran cuentas de Twitter establecidas con la finalidad de aplicar técnicas forenses a los mensajes obtenidos del timeline de Twitter. Esto quiere decir que a partir del post de un tweet de un usuario ficticio se van a ejecutar todas las pruebas posibles para obtención de información.

5.2 Estado Inicial

5.2.1 Reconocimiento

Proceso que consiste en el establecimiento de los detalles del evento.

Por solicitud de la afectada Adriana Valencia a quien en adelante se le conocerá como denunciante, y bajo recepción del formato de denuncia en línea proporcionado en el sitio web de la Fiscalía General del Estado, por violencia psicológica contra la mujer se conoce el relato de los hechos e involucrados, detallados a continuación en la figura 39.

Figura 41 Formato denuncia en línea página web fiscalía

Fuente: Denuncia en línea (Fiscalía, 2020)

El contenido del formulario de denuncia con toda la información solicitada, se puede evidenciar en la figura 40

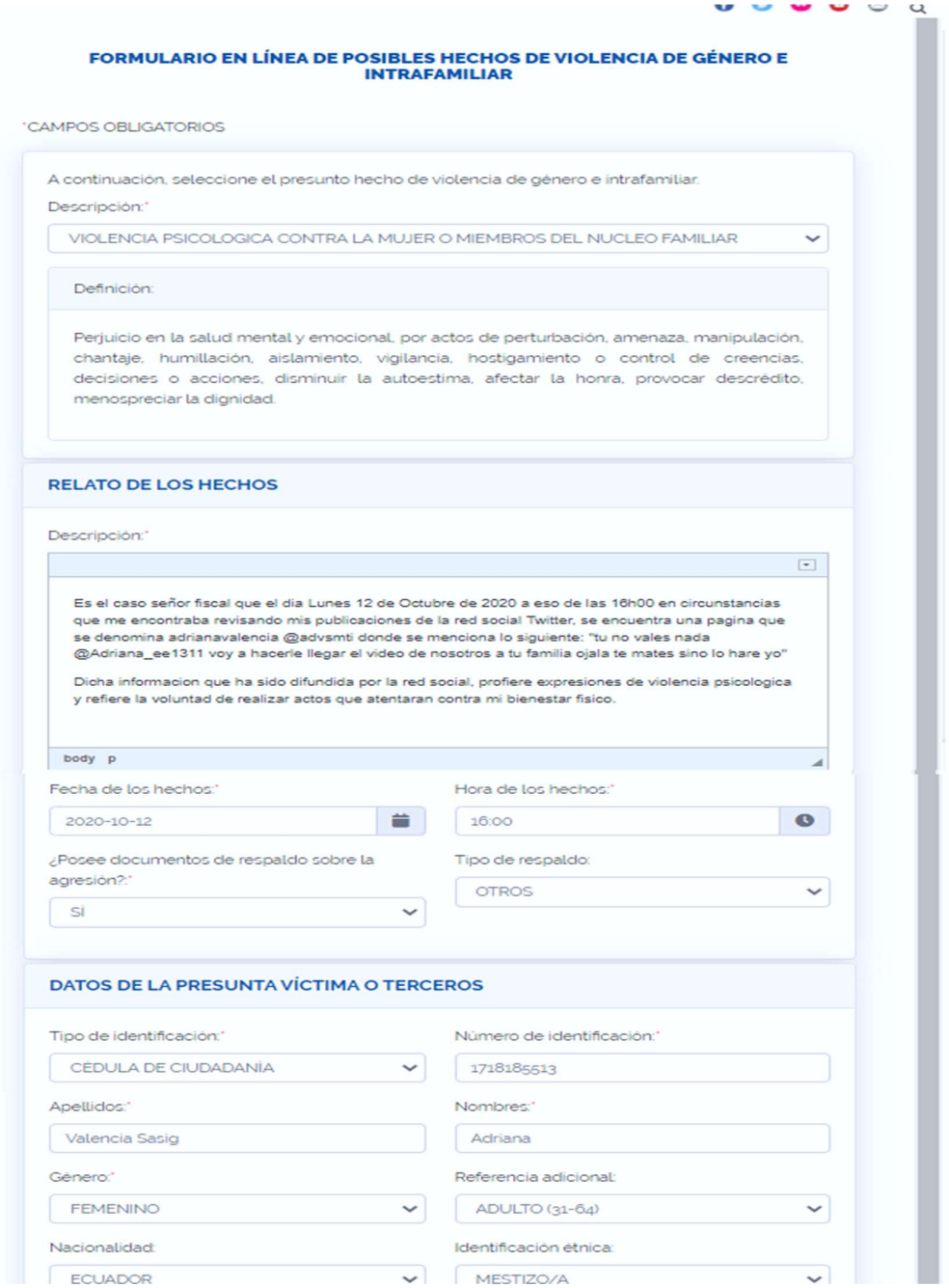


Figura 42 Formato denuncia en línea página web fiscalía

Fuente: Denuncia en línea (Fiscalía, 2020)

5.2.2 Construcción

De la verificación superficial en la red social Twitter bajo los criterios de la denunciante se puede considerar como datos de inicio:

a) Nombre usuario de la denunciante en la red social @Adriana_ee1311

b) Acorde a la denuncia el agresor se identifica con el nombre de usuario @advsmti
c) El hecho habría tenido lugar con fecha 12 de octubre de 2020.

Esta información se ha extraído del muro de notificaciones del denunciante como se puede evidenciar en la figura 41.

Figura 43 Publicación realizada en Twitter dirigida al usuario Adriana_ee1311

Fuente: Muro Notificaciones usuario (Twitter, 2020)

5.2.3 Investigación

Actividad que se llevara a cabo a través del prototipo diseñado.

5.2.3.1 Identificación

En base al nombre de usuario proporcionado en la denuncia considerado como agresor y corroborado a través de la notificación en el muro del afectado, se valida el muro de publicaciones del usuario @advsmti, en base a la información visualizada en la figura 42 se establece que existen datos suficientes para ser recabados de esta cuenta.

Figura 44 Muro de Publicaciones del presunto agresor

Fuente: Autor

5.2.3.2 Búsqueda, Filtrado y Captura

Se obtendrá los datos en el siguiente orden:

Etapa I: Ejecución de la API Tweepy en Twitter bajo los criterios de búsqueda por usuario, palabra clave y fecha.

Parte 1. Se monitoriza el stream de Twitter acorde a la figura 43 por:

a) Usuario @advsmti
b) Palabra de búsqueda @Adriana_ee1311
c) Fecha de búsqueda 2020-10-12

Figura 45 Pantalla resultante de la ejecución por búsqueda de contenido de un Tweet

Fuente: Autor

Al ejecutar la consulta, se obtiene como resultado la información contenida en Twitter del usuario advsmti filtrado por la mención @Adriana_ee1311 en la fecha 12 de octubre 2020; de esta consulta se desglosan cuatro productos, primero 1 archivo con el contenido del Tweet almacenado con el siguiente formato de nombre: advsmti_tweet.csv, resultados de la Figura 44, en este caso la publicación tiene contenido de video se realiza la descarga del mismo y lo almacena por su ID de Tweet en extensión .mp4, ver figura 45, se genera un acceso directo al tweet que se busca en la página de twitter y se toma una captura de pantalla con el contenido respaldando la información antes obtenida como se puede ver en la figura 46, adicional se genera un segundo archivo con el contenido del perfil de usuario denominado advsmti_perfil.csv ver Figura 47.

Parte 1

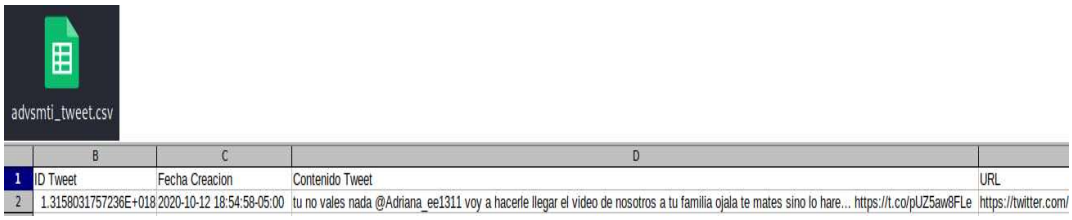


Figura 46 Datos obtenidos de la consulta información Tweet

Fuente: Autor

Parte 2

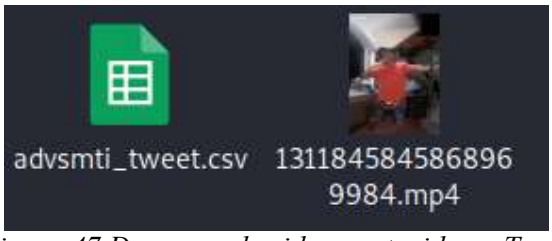


Figura 47 Descarga de video contenido en Tweet

Fuente: Autor

Parte 3

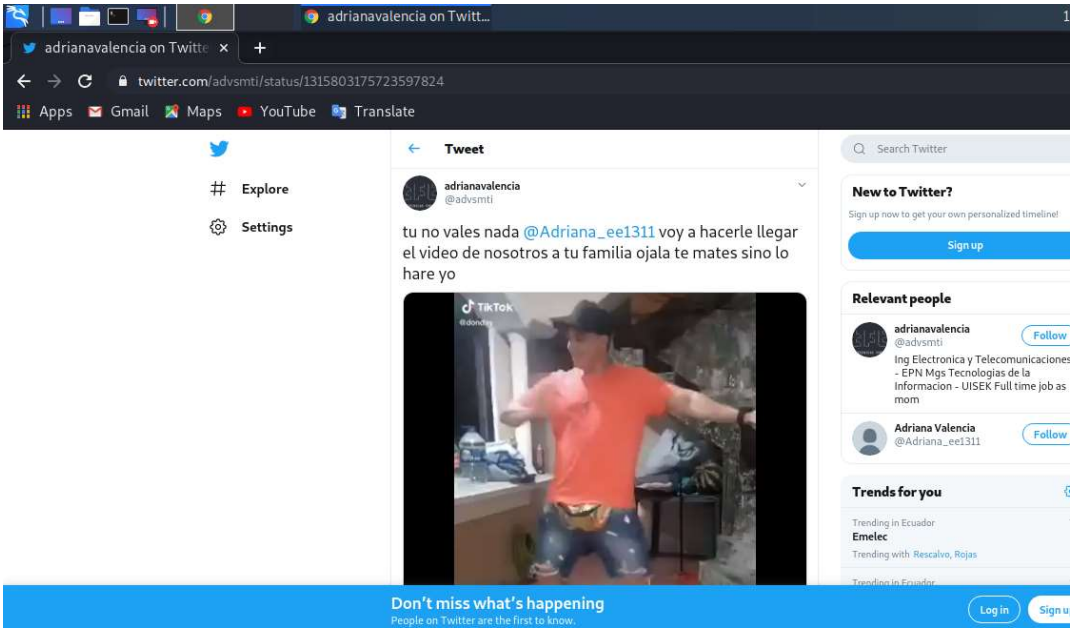


Figura 48 Redireccionamiento a buscador Chrome en URL de Tweet

Fuente: Autor

Parte 4

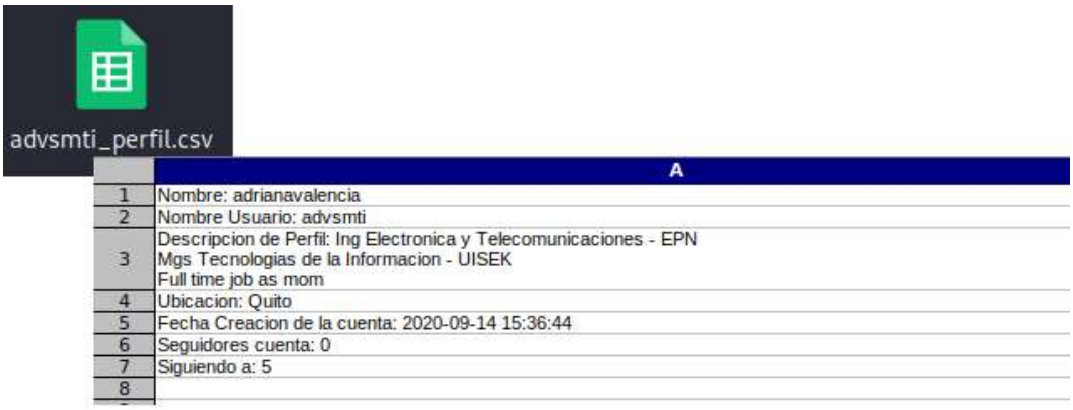


Figura 49 Informacion de perfil usuario

Fuente: Autor

El proceso de búsqueda por usuario y fecha generara contenido para la base de datos bd_tweepy con toda la información de los tweets sin filtro por ninguna palabra clave como se puede validar en la figura 48.

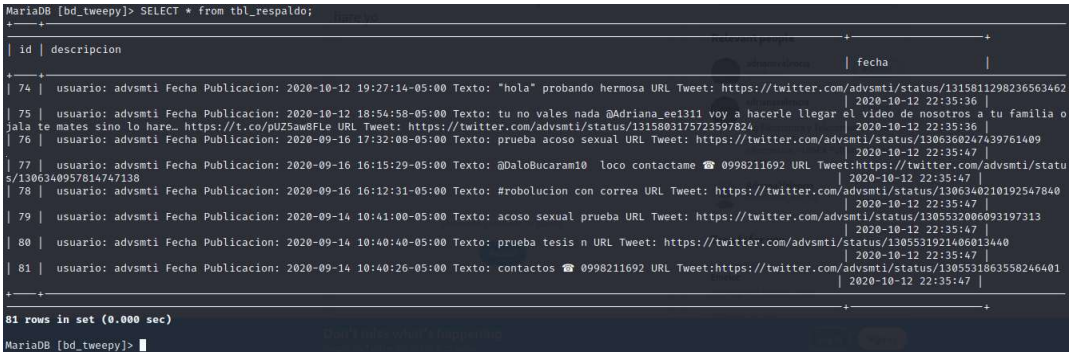


Figura 50 Contenido tabla tbl_respaldo con datos twitter

Fuente: Autor

Los archivos resultantes advsmti_tweet.csv y advsmti_perfil.csv generarán sus respectivos hash que serán almacenados en la base de datos bd_tweepy tabla tbl_respaldo_hash, como se muestra en la figura 49.

Figura 51 Contenido tabla tbl_respaldo_hash con datos hash

Fuente: Autor

Etapa II: Búsqueda del usuario en otras plataformas

Se ejecutará una búsqueda por usuario y nombre como se valida en la Figura 50:

- Usuario: advsmti
- Nombres: adriana valencia

Al ejecutar la consulta, se obtiene como resultado la información contenida en diferentes plataformas como redes sociales, repositorios digitales, sitios de compra donde se encuentre registrado el mismo nombre de usuario; de esta consulta se desglosa un producto, un archivo con el contenido resultado de la búsqueda en las plataformas relacionadas a osrframework; para el ejemplo antes mencionado se obtienen los resultados de la Figura 51.

Figura 52 Inputs para ejecutar búsqueda de usuario en varias plataformas con motor de búsqueda OSRFramework

Fuente: Autor

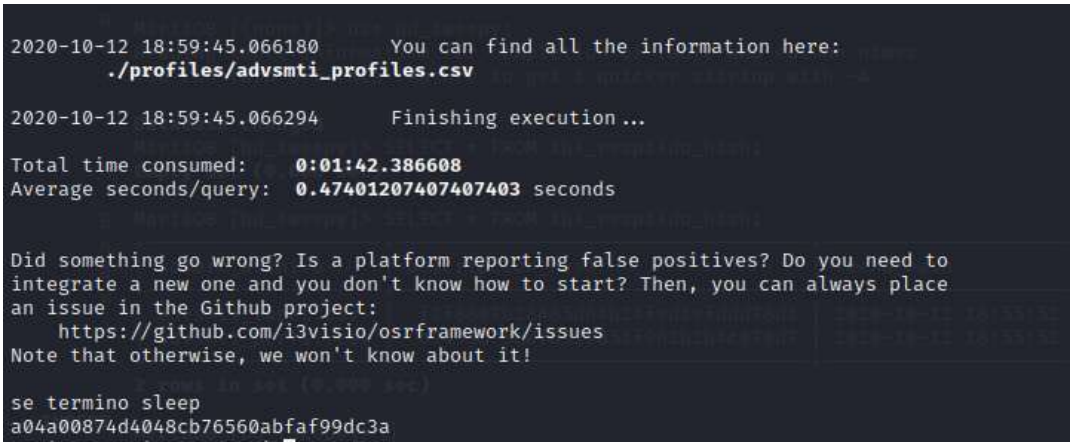
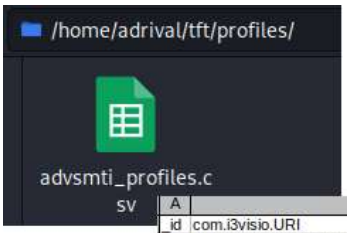


Figura 53 Resultados de la ejecución búsqueda de usuario en varias plataformas con motor de búsqueda OSRFramework

Fuente: Autor

El archivo obtenido se descarga como advsmti_profiles.csv con los resultados de la información relacionada a un usuario de Twitter en otras plataformas



_id	com.i3visio.URI	com.i3visio.Alias	com.i3visio.Platform	com.i3visio.Name
1	https://www.canva.com/advsmti	advsmti	Canva	N/A
2	http://advsmti.blogspot.com.es/	advsmti	Blogspot	N/A
3	http://www.bucketlistly.com/users/advsmti	advsmti	Bucketlistly	N/A
4	http://advsmti.carbonmade.com	advsmti	Carbonmade	N/A
5	https://www.causes.com/advsmti	advsmti	Causes	N/A
6	http://www.burbuja.info/inmobiliaria/member-advsmti.htm	advsmti	Burbuja.info	N/A
7	http://www.colourlovers.com/lover/advsmti	advsmti	Colourlovers	N/A
8	https://forums.digitalspy.com/profile/discussions/advsm	advsmti	Digitalspy	N/A
9	http://www.ebay.com/usr/advsmti	advsmti	Ebay	N/A
10	https://site.douban.com/advsmti	advsmti	Douban	N/A
11	https://www.freelancer.com/u/advsmti	advsmti	Freelancer	N/A
12	http://www.instagram.com/advsmti	advsmti	Instagram	N/A
13	https://mastodon.xyz/@advsmti	advsmti	MastodonXyz	N/A
14	https://www.minds.com/advsmti	advsmti	Minds	Android App
15	https://onename.com/advsmti	advsmti	Onename	N/A
16	http://www.meneame.net/user/advsmti	advsmti	Meneame	N/A
17	http://pastebin.com/u/advsmti	advsmti	Pastebin	N/A
18	https://www.okcupid.com/profile/advsmti	advsmti	Okcupid	N/A
19	https://www.patreon.com/advsmti	advsmti	Patreon	N/A
20	http://pixinsight.com/forum/index.php?action=profile	user=advsmti	advsmti	Pixinsight
21	http://www.researchgate.net/profile/advsmti	advsmti	Researchgate	N/A
22	http://500px.com/advsmti	advsmti	500px	N/A
23	http://www.sidereel.com/profile/advsmti	advsmti	Sidereel	N/A
24	https://telegram.me/advsmti	advsmti	telegram	N/A
25	http://twitter.com/advsmti	advsmti	Twitter	N/A
26	https://www.youtube.com/user/advsmti/about	advsmti	Youtube	N/A
27	https://www.xing.com/profile/advsmti	advsmti	Xing	N/A
28	https://advsmti.soup.io	advsmti	Soup	N/A

Figura 54 Datos obtenidos de la consulta usuario en otras plataformas

Fuente: Autor

El listado contiene el nombre del sitio y la URL donde se podría redirigir la consulta para obtener más datos del usuario ver Figura 53.

A	B
24	https://telegram.me/advsmti
25	http://twitter.com/advsmti
26	https://www.youtube.com/user/advsmti/about

Figura 55 Resultados obtenidos de URLs para realizar búsqueda de información adicional

Fuente: Autor

Etapa III: Búsqueda del correo electrónico asociado al usuario

Se ejecutará una búsqueda por usuario como se valida en la Figura 54:

- Usuario: advsmti

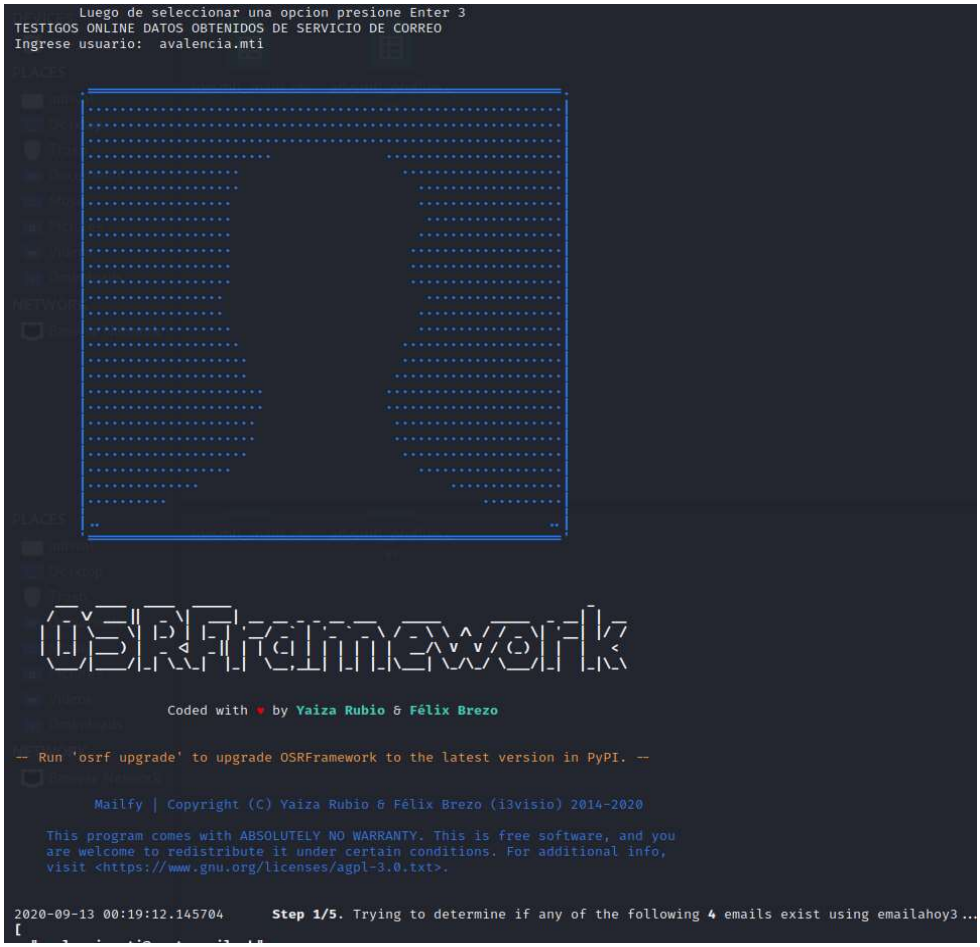


Figura 56 Inputs para ejecutar búsqueda de usuario en servicios de correo con motor de búsqueda OSRFramework

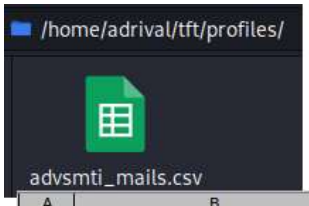
Fuente: Autor

Al ejecutar la consulta, se obtiene como resultado la información contenida en diferentes servicios de correo, donde se encuentre registrado el mismo nombre de usuario; de esta consulta se desglosa un producto, un archivo con el contenido resultado de la búsqueda en servicios de correo relacionados a osrframework; para el ejemplo antes mencionado se obtienen los resultados de la Figura 55.

Figura 57 Datos arrojados por la plataforma correspondientes a la cuenta de correo electrónico

Fuente: Autor

El archivo de esta etapa se descarga como advsmti_mails.csv con los resultados de la información relacionada al correo electrónico usado para procesos de autenticación en otras plataformas en este caso específico encontró una coincidencia con la Plataforma Twitter



	A	B	C	D	E
1	_id	com.i3visio.Email	com.i3visio.Alias	com.i3visio.Domain	com.i3visio.Platform
2	1	advsmti@gmail.com	advsmti	gmail.com	Twitter

Figura 58 Datos obtenidos de la consulta de correos electrónicos usados para autenticación en plataformas

Fuente: Autor

5.2.4 Análisis

De las consultas realizadas previamente se puede tener la presunción del contacto telefónico asociado a determinado correo electrónico, mediante la opción que se habilita por defecto al realizar la recuperación de la contraseña, desde donde se puede obtener indicios correspondientes al correo o número telefónico vinculados como parte de la configuración inicial de una cuenta.

5.2.4.1 Hipótesis

Con el conocimiento de la cuenta de correo asociada a la cuenta de Twitter se procede a realizar procesos de reseteo de contraseña como se visualiza en la Figura 57, desde donde se obtienen los datos que corroboran que el correo encontrado en la etapa III está vinculado a dicha cuenta, adicional se puede validar los dígitos finales del numero celular asociado.

Figura 59 Recuperación de contraseña Twitter

Fuente: Menú recuperación de contraseña usuario advsmti (Twitter, 2020)

El mismo proceso se puede repetir para las redes sociales obtenidas en la etapa II, con lo que se podrá seguir aportando información para determinar el número telefónico asociado a un usuario. En detalle se muestran los resultados obtenidos para el proceso de recuperación de contraseña en Plataformas como Instagram y Paypal

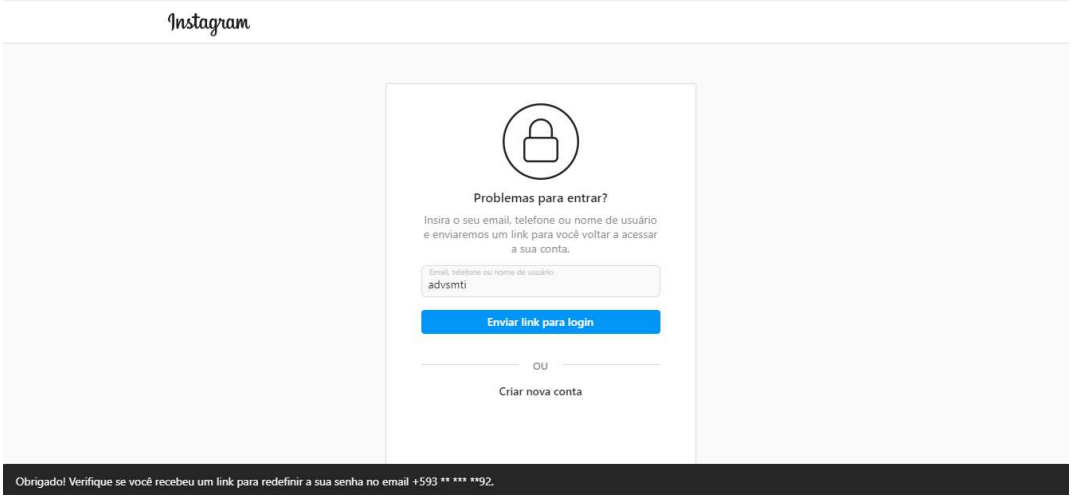


Figura 60 Recuperación de contraseña Instagram

Fuente: Menú recuperación de contraseña usuario advsmti (Instagram, 2020)

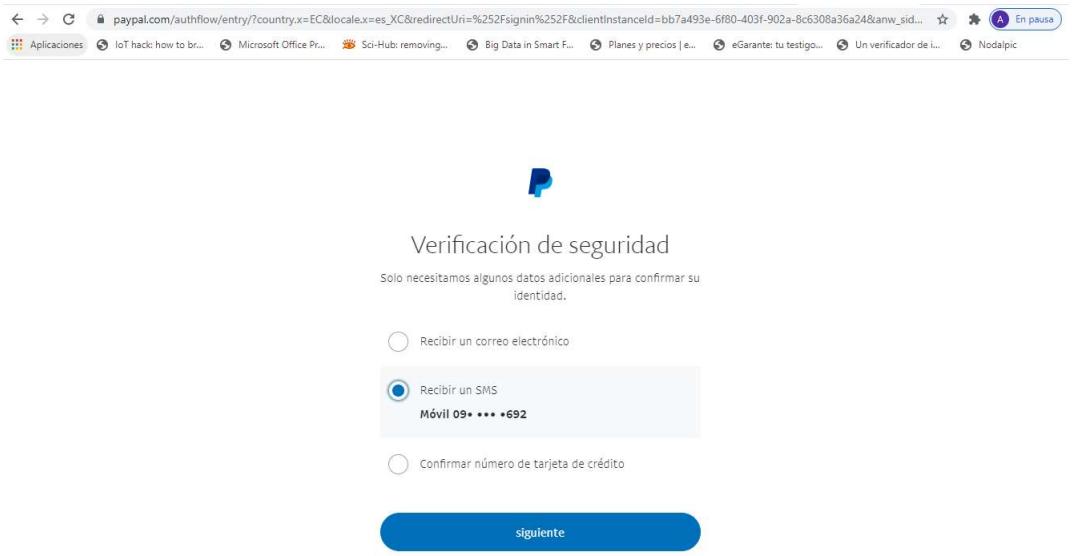


Figura 61 Recuperación de contraseña Paypal

Fuente: Menú recuperación de contraseña usuario advsmti (Paypal, 2020)

En base a la información anteriormente indicada y que fue obtenida de data de las etapas II y III podemos generar una nueva hipótesis para determinar el número celular del usuario, esto en base a que se tienen al menos los 3 últimos dígitos relacionados a las cuentas que maneja dicho usuario.

Caso 1, estos 3 dígitos son concordantes con la información publicada en su historial de Twitter

```
Digitos a buscar en contenido/historial Twitter XXX692
El numero se encuentra en tweet contenido en la linea  1 del historial, y es:
1305142119124926465 2020-09-13 08:51:44 CDT <advsmti> contacto ☎ 0998211692
```

Figura 62 Datos arrojados de la búsqueda del número en el historial de Twitter

Fuente: Autor

Caso 2, aplica para casos de acoso, el denunciante puede haber establecido previamente contacto y el dato de número celular puede encontrarse dentro de los datos de contactos, llamadas o mensajes

```
Digitos a buscar en base de numeros telefonicos obtenidos del denunciante
692
El numero se encuentra en la linea 6 de la base de numeros telefonicos, y es:
998211692
```

Figura 63 Datos arrojados de la búsqueda del número en base de datos telefónicos

Fuente: Autor

Los hash de cada archivo generado en cada etapa de búsqueda quedaran almacenados con su respectiva descripción en la tabla tbl_respaldo_hash acorde a la información detallada en la figura 62.

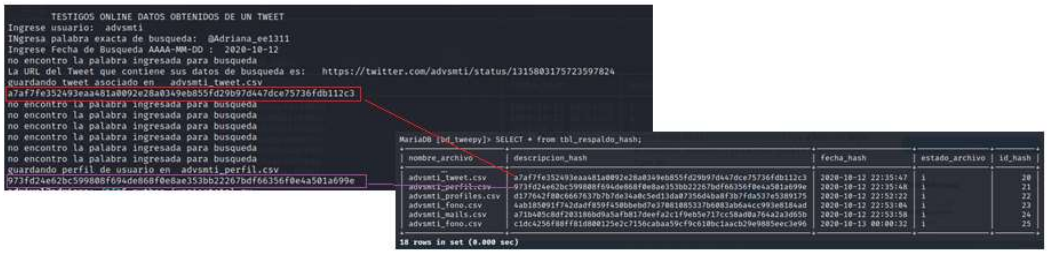


Figura 64 Hash almacenados en la Base de datos

Fuente: Autor

5.2.4.2 Informes

El archivo de esta etapa corresponde a un unificado de todas las etapas anteriores, por lo tanto, solicitara los datos concernientes a nombre de usuario, nombre del afectado que está solicitando el informe y su correspondiente número de cedula, datos que serán usados en el texto de Conformidad y Autorización. Para el proceso de firmado digital se debe poseer una firma electrónica con su respectivo archivo de extensión .p12 o .pfx e ingresar la clave de autenticación.

Previo al proceso de generación de PDF se desarrollará una validación de los hash de cada archivo que se usará para el informe contrastados con la información almacenada en la base de datos, ver figura 63, si ninguno de los archivos ha sido modificado manualmente seguirá con el proceso normal caso contrario arrojará un error por problemas de validación de la integridad de los archivos.

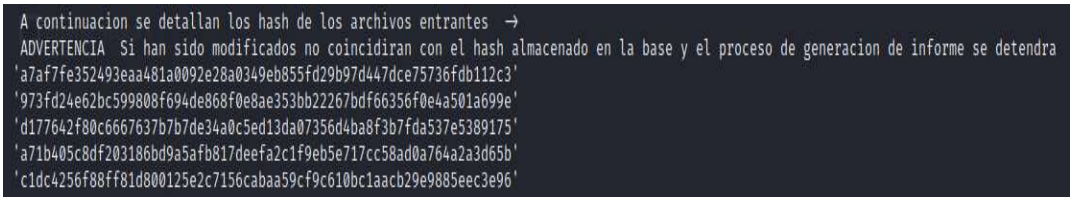


Figura 65 Validación hash archivos .csv

Fuente: Autor

Si ha pasado el proceso de validación de hash continuara con la creación del PDF para ello se requiere el ingreso de los datos del solicitante como se evidencia en la figura 64.

```
Digite el nombre del usuario → advsmti
****************************************************************
** :SCRIPT PARA VALIDAR HASH DE ARCHIVOS CSV                   **
** CONSULTA LA BASE DE DATOS BD_TWEEPY                         **
** VERIFICA EL HASH                                            **
****************************************************************
****************************************************************
** SI ALGUNO DE LOS ARCHIVOS HA SIDO MODIFICADO                **
** NO SE GENERARA PDF                                          **
** VERIFIQUE LA INTEGRIDAD DE LOS DOCUMENTOS                   **
****************************************************************
Digite el nombre completo de la persona que realiza esta solicitud → Adriana Valencia
Digite la cedula del solicitante → 1718185513
*****INICIA PROCESO DE GENERACION DE PDF*****
PDF generado exitosamente!
*****INICIA PROCESO DE FIRMADO DIGITAL*****
Digite el nombre del archivo .pfx (firma digital)      → ADRIANA
Digite la clave para la firma digital      → 1234
```

Figura 66 Inputs para realizar el informe PDF

Fuente: Autor

Los archivos generados tendrán el número de cedula del solicitante acorde a la información que se visualiza en la Figura 65.

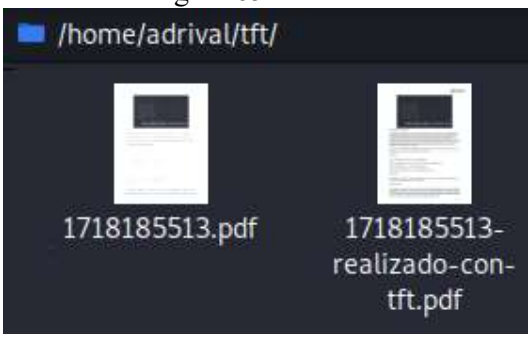


Figura 67 Documentos generados del proceso generación de PDFs

Fuente: Autor

Prueba Documental generada

A continuación, se detalla el contenido del informe resultante:

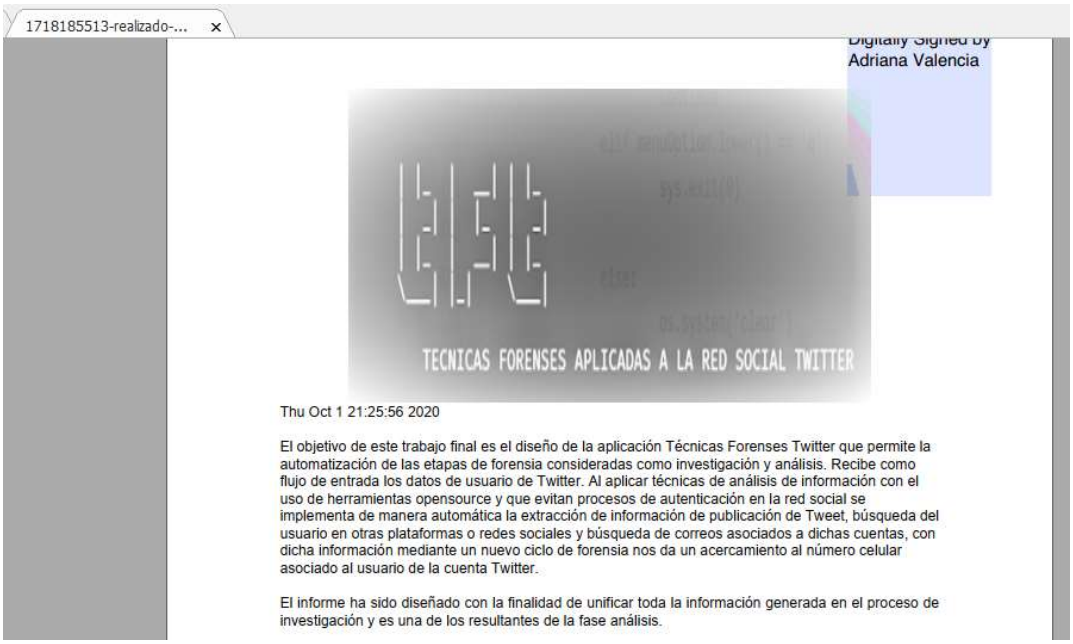


Figura 68 Portada

Fuente: Autor

Figura 69 Referencias

Fuente: Autor

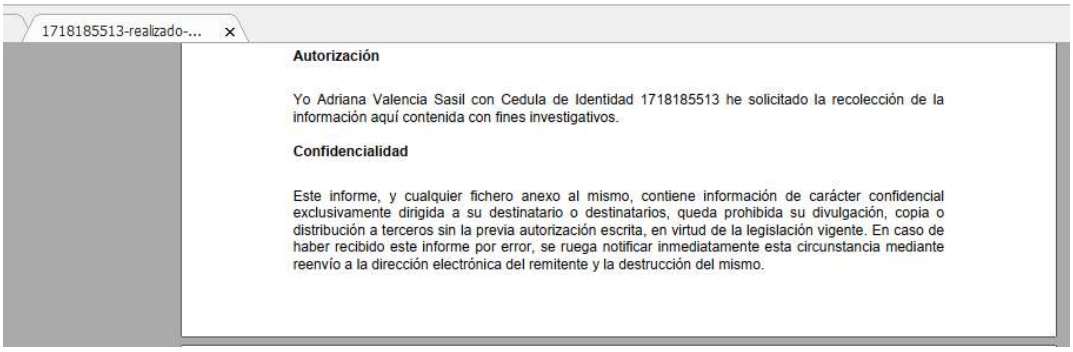


Figura 70 Manifiesto de Autorización

Fuente: Autor

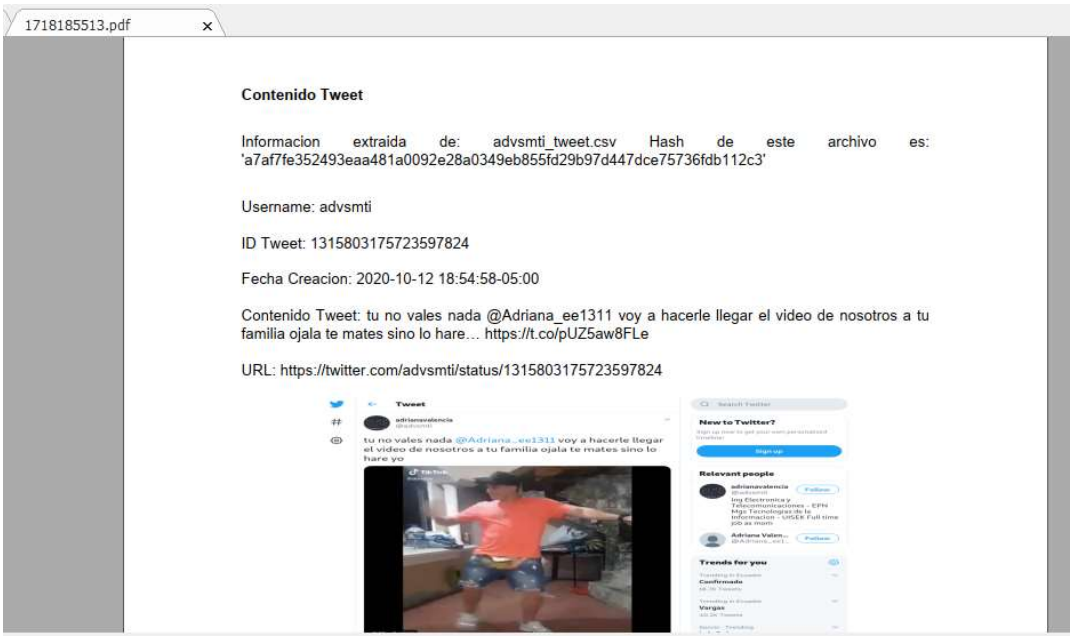


Figura 71 Etapa I –Mensaje Tweet

Fuente: Autor

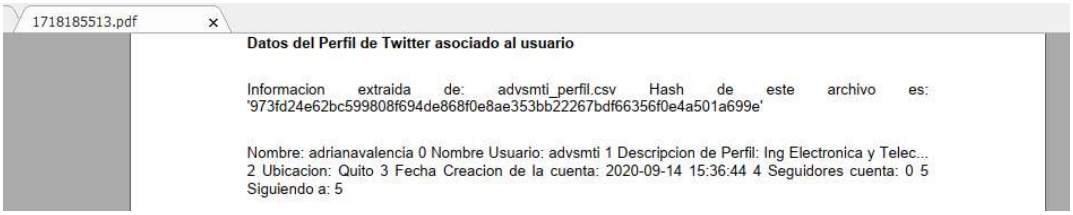


Figura 72 Etapa I –Datos Perfil

Fuente: Autor

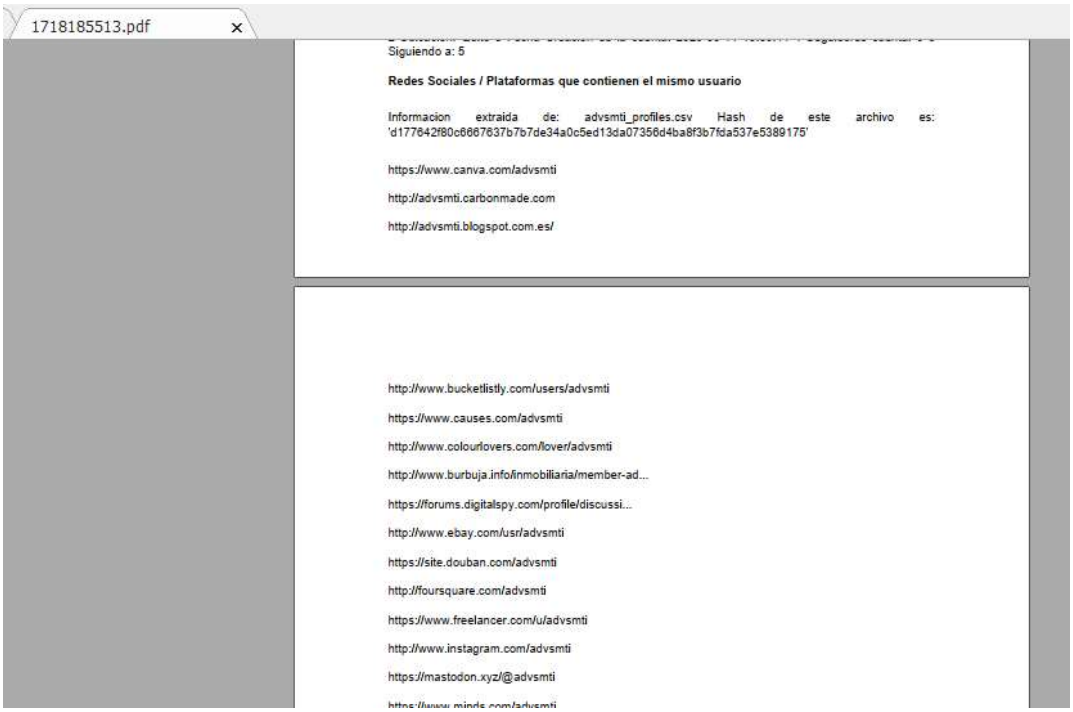


Figura 73 Etapa II – Redes Sociales / Plataformas con el mismo usuario

Fuente: Autor

Figura 74 Etapa III – Correos electrónicos asociados a diversos procesos de autenticación

Fuente: Autor

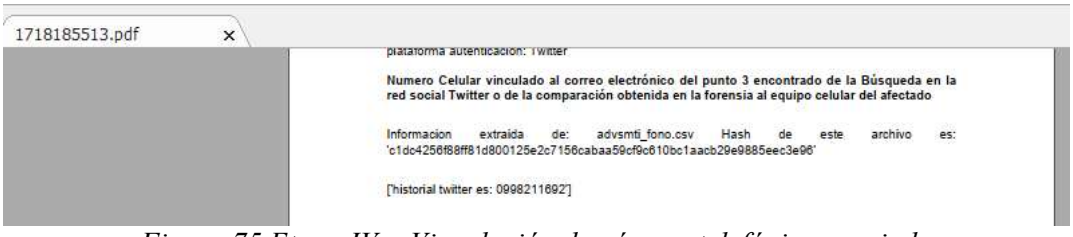


Figura 75 Etapa IV - Vinculación de número telefónico asociado

Fuente: Autor

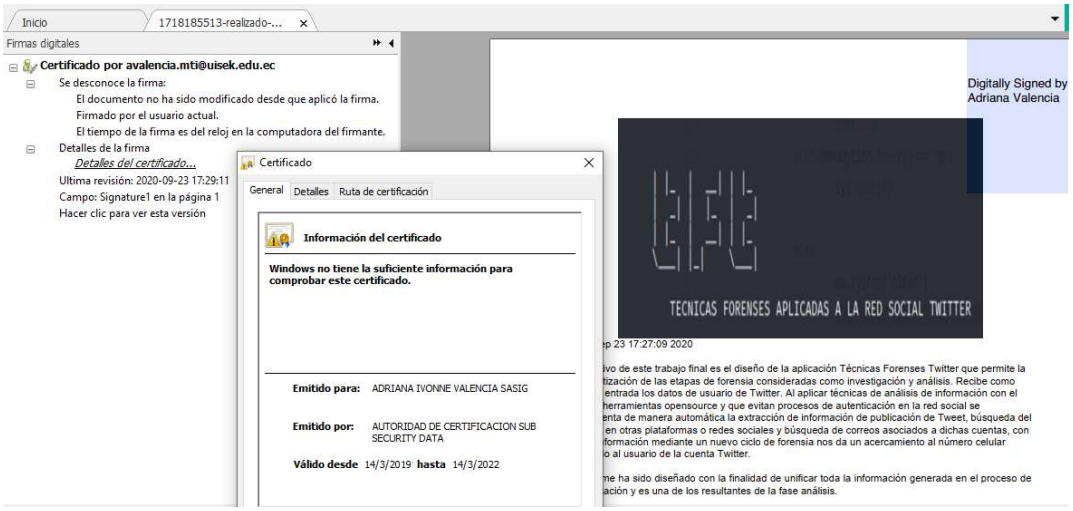


Figura 76 Verificación firma electrónica

Fuente: Autor

5.2.5 Evaluación

El informe será entregado al abogado del denunciante y Fiscalía y de ser necesario será defendido ante el jurado

CAPITULO VI

DISCUSION

6.1 CONCLUSIONES

Del análisis realizado en el estado del arte se puede evidenciar que actualmente la recolección, presentación y preservación de evidencia de redes sociales en línea carece de la introducción de una multiplicidad de datos a los que se puede acceder con la mejora en las herramientas de extracción y análisis. En esta investigación se ha propuesto varias herramientas y un modelo para que el investigador cumpla con los criterios técnicos, el marco legal y los debidos procesos para asegurar la admisibilidad de estas pruebas.

Los abogados litigantes utilizan igualmente información de redes sociales en procedimientos legales. Sin embargo, en la defensa los abogados enfrentan más obstáculos para buscar una citación para acceder a datos protegidos de redes sociales, a través del método vinculado a esta investigación se proponen varias fuentes para llegar a obtener evidencia sin que la misma sea intrusiva en el entorno del investigado.

Se ha desarrollado un modelo con estructura modular, con la finalidad de que trabaje de forma independiente ya que desde el punto de vista forense la información obtenida en redes sociales varia o aparece en cada etapa, lo que se plantea es que conforme a la conducción de la investigación una etapa pueda ser repetida sin que sea dependiente de la anterior, permitiendo realizar consultas y obteniendo resultados de cada una de ellas.

El tratamiento de los datos de Twitter a través de la API Tweepy garantiza la extracción de información verídica desde la red social, ya que a través de sus distintas librerías la obtención, procesamiento y categorización de Tweets se optimizan tiempos en el desarrollo del prototipo que tiene implicación directa en el desempeño de la aplicación

El manejo de la aplicación de búsqueda OSRframework fue satisfactorio considerando que es habitual que un usuario utilice el mismo nombre de usuario en distintas plataformas o redes sociales, lo que derivó en obtener resultados fiables del usuario registrado en otras plataformas o red social y automatización de la búsqueda de un correo electrónico asociado al proceso de autenticación de la red social Twitter.

El proceso de identificación de un usuario a partir del nombre de usuario de una red social es complejo y requiere del entendimiento de varios factores, para una investigación el paso más importante sería obtener una dirección IP, sin embargo, otros elementos también relacionados con el usuario permitirán llegar a conocer su identidad, en esta investigación se ha demostrado que se pueden llegar a recoger y almacenar datos necesarios explorando técnicas alternativas.

Durante el proceso judicial se expondrán los hechos o circunstancias que se presentaron para considerar el cometimiento de un ilícito, para exponer estos hechos se presentan las

pruebas, en este caso el documento electrónico generado contiene las pruebas y esta materializado conteniendo una transcripción del contenido original de la red social Twitter, adicional cumple las condiciones para ser admitido como tal ya que se encuentra firmado electrónicamente y contiene un sellado de tiempo.

Las técnicas descritas en la implementación de este trabajo pueden ser aplicables para otras redes sociales o plataformas pues mientras más datos se aporten a determinado perfil de usuario será más fácil reconstruir su identidad.

6.2 RECOMENDACIONES Y TRABAJOS FUTUROS

Se recomienda usar una fuente de datos que cumpla con políticas de acceso a datos y sea aceptada por la plataforma o red social que se va a investigar, en este trabajo puntualmente se usó inicialmente la plataforma Twint que realizaba un scrapping de la plataforma Twitter sin necesidad de autenticación o uso de contraseñas del usuario en modo developer, sin embargo Twitter realizo cambios a su modo de acceso y la bloqueo por lo que se tuvo que reenfocar el diseño a otra API para la obtención de datos.

Se puede implementar el mismo prototipo con una interfaz gráfica para que pueda ser usada con un complemento visual enfocada a los usuarios que no tienen habilidad con el uso de plataformas con comandos sin embargo el enfoque de ejecución y obtención de datos se mantendría.

Dentro del mismo modulo se podría implementar una función adicional que permita catalogar el Tweet mediante el entrenamiento de un algoritmo y lo asocie por palabras o contexto a la tabla de delitos del COIP, de esta forma se podría en un mismo escenario inclusive catalogar que tipo de delito está cometiendo el usuario de Twitter.

Dentro de la validación del proceso de recuperación de contraseña actualmente se está realizando de forma manual en el entorno web fuera de la aplicación, este módulo también podría estar embebido y ser parte de la programación del sistema de forma que valide los datos de recuperación de contraseña en todas las URLs obtenidas de la etapa Búsqueda del usuario en otras plataformas y devuelva los resultados relacionados a formas de recuperación como correo o teléfono asociados.

LISTA DE REFERENCIAS

Ademu, Inikpi & Imafidon, Chris. (2012). The Need for a New Data Processing Interface for Digital Forensic Examination. International Journal of Advanced Research in Artificial Intelligence.

Adedayo, Oluwasola. (2016). Big data and digital forensics. 1-7.

Asamblea de Montecristi. (2008). Constitución De La República Del Ecuador. *Decreto Legislativo*, 1–222.

Asamblea Nacional de la República del Ecuador. (2015). Código Orgánico General de Procesos. Ecuador

Asociación por los Derechos Civiles [ADC]. (2018). *La investigación forense informática en América Latina*. 1–29.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. *Fourth Digital Forensic Research Workshop*

Brandt, M. (2017). 80% Of Twitter's Users Are Mobile, Statista. www.statista.com/chart/1520/number-of-monthly-active-twitterusers/

Bryson, C., & Stevens, S. (2002). Handbook of computer crime investigation: forensic tools and technology. London: Academic Press.

Cajamarca, G., Lima, G., & Sebastián, J. (2017). Marco de trabajo estandarizado para el análisis forense de la evidencia digital. *Revista Publicando*, (111), 42–78.

Comisión Legislativa y de Fiscalización. (2009). Ley de seguridad pública del estado. *Registro Oficial*, 1–16.

Congreso Nacional del Ecuador. (2002). Ley de Comercio Electrónico, Firmas y Mensaje de Datos. Registro Oficial Suplemento 557.

Consejo de Europa. (2001). Convenio de Budapest. *Serie de Tratados Europeos*, *1*(4), 53.

Consejo de la Judicatura. (2014). Reglamento del Sistema Pericial Integral de la Función Judicial. *Registro Oficial*, *125*(125), 1–16. www.funcionjudicial.gob.ec

Coronel, B. D. (2018). Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web. *Universidad de Cuenca*, 142.

Chemerkin, Y. (2012). 5 thoughts on "Key Twitter and Facebook Metadata Fields Forensic Investigators Need to be Aware of". www.forensicfocus.com/articles/key-twitter-and-facebook-metadata-fields-forensic-investigators-need-to-be-aware-of/

Del Valle, D. (2018). Evidencia Digital. *Universidad Empresarial Siglo 21*, 1–69.

Dunn Ortega, M. A. (2019). Valor probatorio de la prueba documental de contenidos digitales durante la etapa de juicio en el Derecho Procesal Penal Ecuatoriano. *Universidad Católica de Santiago de Guayaquil*, 29.

Freiling, F., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. IMF.

Garfinkel, Harold. (2012). "The 'Red' as an ideal object", Etnografia e ricerca qualitativa, no. 1, pp. 19–31

Gogolin, Greg. (2010). The Digital Crime Tsunami. Digital Investigation. 7. 3-8. 10.1016/j.diin.2010.07.001.

Haghani, S., & Keyvanpour, M.R. (2017). A systemic analysis of link prediction in social network. *Artificial Intelligence Review*, 1-35.

Harrell, C. (2010). Overall DF Investigation Process.

Hubert, K. (2014). Information Security Reading Room Evidence Collection From Social Media Sites. *SANS Institute*, 24.

Hughes, A. Wojcik, S. (2019) “Sizing Up Twitter Users”, https://www.pewresearch.org/internet/2019/04/24/sizing-up-twitter-users/

Ieong, Ricci. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation. 3. 29-36. 10.1016/j.diin.2006.06.004.

ISO/IEC 27037:2012 Information technology— Security techniques— Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Jang, Yu-Jong & Kwak, Jin. (2014). Digital forensics investigation methodology applicable for social network services. Multimedia Tools and Applications. 74. 10.1007/s11042-014-2061-8.

Jara- Obregón, L. S., Ferruzola-Gomez, E., & Rodríguez-López, G. (2017). Delitos a través redes sociales en el Ecuador: una aproximación a su estudio. *RIDTEC | Vol. 13, n.° 2*, *13*(2).

Jara, M. (2010). La prueba electrónica documental en el código de procedimiento penal ecuatoriano. Universidad de Cuenca

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Computer Security: Guide to integrating forensic techniques into incident response: Recommendations of the National Institute of Standards and Technology (Special Publication 800-86). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Kohn, M.; Eloff, J.H.P.; Olivier, M.S. (2006). Information and Computer Security Architectures Research Group (ICSA), Department of Computer Science, University of Pretoria, "Framework for a Digital Forensic Investigation", Proceedings of the ISSA 2006 from Insight to Foresight Conference

Loarte Cajamarca, Byron Gustavo. Grijalva Lima, J. S. (2018). Desarrollo de una Guía Metodológica para el Análisis Forense en Equipos de Cómputo con Sistema Operativo Mac OS X. *Revista Publicando*, *5*(14), 44.

Lorca Ruiz, O. F. (2017). Violación a la intimidad en redes sociales en Ecuador. *Universidad Católica de Santiago de Guayaquil*, 28.

Marulanda, Juan, and Luis Acosta. 2010. "El Reto de Los Investigadores Informáticos Para Contrarrestar Las Técnicas Anti - Forense," 1–4.

Ministerio de Defensa Nacional. (2019). Plan Nacional de Seguridad Integral 2019-2030. *Secretaria Nacional de Planificación y Desarrollo*.

Mulazzani, M., Huber, M., & Weippl, E. (2012). Data Visualization for Social Network Forensics. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics VIII* (pp. 115–126). Berlin, Heidelberg: Springer Berlin Heidelberg.

Mumba, E. & Venter, H. (2014). Mobile forensics using the harmonised digital forensic investigation process. 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference.

NowSecure (2017, 1 September), HOWTO: Use AFLogical OSE for Logical Forensics of an Android Device [Online] Available: https://santokulinux.com/howto/howto-use-aflogical-ose-logicalforensics-android/.

Obama, B. (2011). International Strategy for Cyberspace. *White House*, 26. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Overill, Richard & Silomon, Jantje. (2012). Digital Meta-Forensics: Quantifying the Investigation.

Perumal, Sundresan. (2010). Digital Forensic Model Based On Malaysian Investigation Process. International Journal of Computer Science and Network Security. 9.

Piccirilli. 2015. "Universidad Nacional de La Plata Facultad de Informática TESIS Doctoral En Ciencias Informáticas ' PROTOCOLOS A APLICAR EN LA FORENSIA DE LAS NUEVAS TECNOLOGÍAS (PERICIA – FORENSIA y CIBERCRIMEN)."

Policía Nacional del Ecuador. (2015). Delitos informáticos o ciberdelitos. http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

Pollitt, M. M. (2007). An ad hoc review of digital forensic models in Systematic Approaches to Digital Forensic Engineering. *SADFE IEEE. Second International Workshop*, 43-54.

Pollitt, M. (1995) "Computer Forensics an Approach to Evidence in Cyberspace", Proceedings, Vol. II, 487-491

Pourkazemi, M., & Keyvanpour, M. (2013). A survey on community detection methods based on the nature of social networks. *ICCKE 2013*, 114-120.

Rogers, Marcus & Goldman, James & Mislan, Rick & Wedge, Timothy & Debrota, Steve. (2006). Computer Forensics Field Triage Process Model. Conference on Digital Forensics, Security and Law. 1. 27-40. 10.15394/jdfsl.2006.1004.

Sanya-Isijola, A. (2009). Models of Digital Forensic Investigation, *University of East London.*

Statista, (2020), Most popular social networks worldwide as of July 2020, ranked by number of active users, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Semprini, G. (2016). El análisis integral de la evidencia digital. *SID, Simposio Argentino de Informática y Derecho*, 12.

Subsecretaria de Gobierno Electrónico Ecuador. (2019). Estrategia Nacional de Ciberseguridad. https://www.gobiernoelectronico.gob.ec/objetivo-de-la-encs/

Twitter. (2020). https://about.twitter.com/company

Tian, Wenhong & Zhao, Yong. (2015). Big Data Technologies and Cloud Computing.

Vargas, E. (2017). Los criterios de valoración de la cadena de custodia en el procedimiento penal Ecuatoriano. *Pontificia Universidad Católica Del Ecuador*, 138.

Vicente, J., & Alvarado, Y. (2015). Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano. *Sembrador*, *8*, 24.

Zainudin, M, Merabti & Llewellyn-Jones. D, "Online social networks as supporting evidence: A digital forensic investigation model and its application design," 2011 International Conference on Research and Innovation in Information Systems, Kuala Lumpur, 2011, pp. 1-6.

ANEXOS

INSTALACION

a) Los siguientes paquetes de Python deben instalarse antes de iniciar la aplicación:

-osrframework

-tweepy

-endesive

-reportlab

-selenium

-youtube_dl

-requests

-hashlib

La forma más sencilla de instalarlos todos es utilizando el administrador pip (PyPI) con el archivo de requisitos:

pip install -r requisitos.txt

b) Antes de iniciar la aplicación, debe completar el archivo tft.py con sus propios tokens y claves para la aplicación Twitter (consulte apps.twitter.com para obtener más información).

Luego ejecute "./tft.py" o "python tft.py"

[CONSUMER]

consumer_key: <Ponga su consumer key>

consumer_secret: <Ponga su consumer secret key>

[ACCESS]

access_key: <Ponga el token de su app>

access_secret: <Ponga su clave secret app>

c) La base de datos con los números telefónicos debe corresponderse a un texto plano y debe ubicarse en `/home/user/Desktop/telfwhats.txt`

d)El archivo .p12 o .pfx de la firma digital debe ubicarse en el directorio desde donde se ejecuta el programa

FORENSIA DE DISPOSITIVOS MÓVILES ANDROID

Santoku Linux proporciona herramientas para extraer datos de dispositivos Android, así como emulando un dispositivo Android. La herramienta que vamos a utilizar para realizar la extracción de datos de Android dispositivos es Android Forensics Logical Open Source Edición o AFLogical OSE. AFLogical OSE tira MMS, SMS, contactos y registros de llamadas desde dispositivos Android.

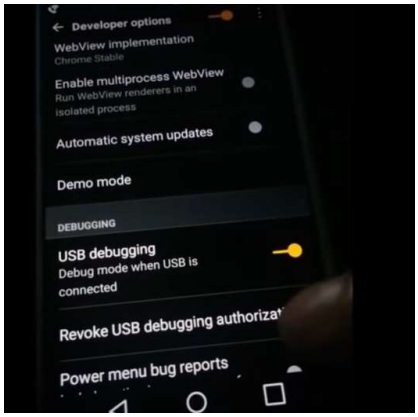
Usando un Motorola y siguiendo las instrucciones proporcionadas en el HOWTOS de AFLogicalOSE publicado en el sitio de Santoku:

1. Asegúrese de que el dispositivo Android esté conectado en la VM Santoku.

2. Habilite la depuración de USB en su dispositivo.

a) Aplicaciones> Configuración> Acerca del teléfono luego toque el número de compilación siete veces (hasta que aparezca un mensaje)

b) Vaya a Aplicaciones> Configuración> Opciones Desarrollador y asegúrese de que debugging USB este seleccionado

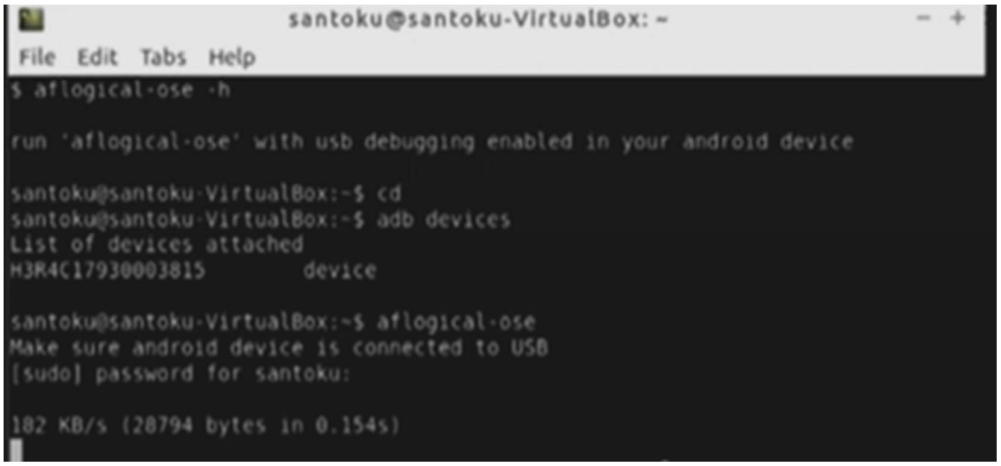


c. En el teléfono seleccione siempre confiar en este dispositivo VM Santoku

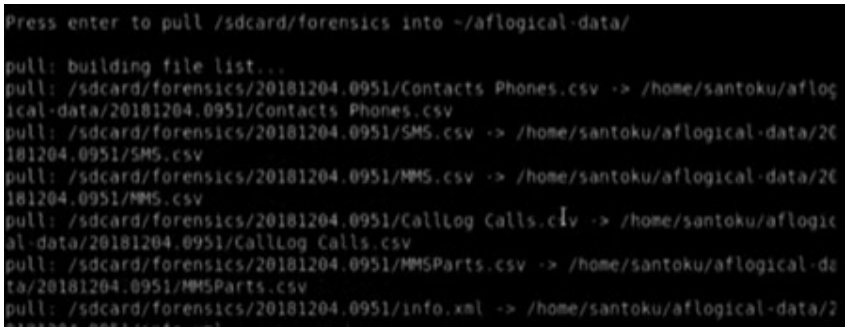
3. En la VM, seleccione: Santoku > Device Forensics > AF Logical OSE

4. En la ventana Terminal que se abre, ingrese como sigue:

$ aflogical-ose (OJO: esto empuja el AFLogicalOSE_1.5.2.apk a su dispositivo)



5. En la terminal cambia /sdcard/forensics into ~/aflogical-data/ con un Enter



6. $ sudo adb devices (Nota: esto mostrará una identificación para el dispositivo adjunto)

En su dispositivo Android, abra AFLogical Aplicación OSE, seleccione todas las marcas de verificación y extraer los datos. (Nota: una barra de progreso y un mensaje"Extracción de datos completada" aparecerá cuando termine)

7. Extraiga los datos de su tarjeta o teléfono a la VM Santoku

a. $mkdir ~/Desktop/AFLogical_Phone_Data

b. $ adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data

Sus datos extraídos ahora se almacenan en el siguiente directorio: ~ / Desktop / AFLogical_Phone_Data

Los archivos recuperados de nuestro dispositivo Android fueron recuperados y almacenados respectivamente en: CallLogCalls.csv, MMS.csv, MMSParts.csv, SMS.csv e info.xml que no arrojó datos utilizables (solo encabezados de campo) y ContactsPhones.csv pudo extraer contactos del teléfono que estaban vinculados desde el teléfono del propietario a su dispositivo.