UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROYECTO DE INVESTIGACIÓN

TEMA:

Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia".

Proyecto de investigación presentado previo a la obtención del Título de Ingeniero en Sistemas de Información.

AUTOR:

Tipanta Díaz Kevin Mauricio

DIRECTOR DE TESIS:

Ing. Rubio Peñaherrera Jorge Bladimir

LATACUNGA – ECUADOR

2023

DECLARACIÓN DE AUTORÍA

Yo, **TIPANTA DIAZ KEVIN MAURICIO con C.I.: 172421461-2** declaro ser el autor del presente proyecto de Investigación: **"Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la oficina técnica de violencia Carcelén" Casa de Justicia"**, siendo el **Ing. Rubio Peñaherrera Jorge Bladimir**, tutor del presente trabajo, eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certificamos que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.

Atentamente,

.....

Tipanta Diaz Kevin Mauricio

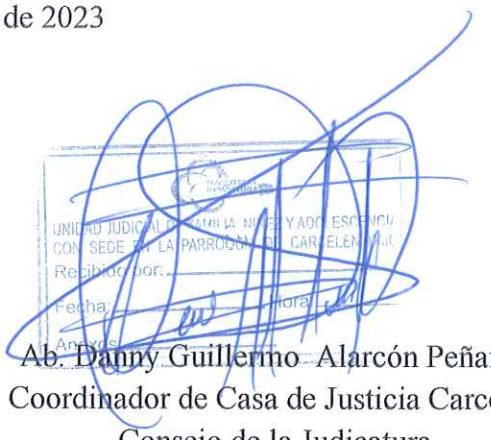
CI: 1724214612

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Cotopaxi, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

CEDO los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Latacunga, 13 de febrero de 2023



Ab. Danny Guillermo Alarcón Peñafiel
Coordinador de Casa de Justicia Carcelén
Consejo de la Judicatura
CC.0201766524

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación con el título: **Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia"** del estudiante: **TIPANTA DIAZ KEVIN MAURICIO** de la Carrera de Ingeniería en Sistemas de Información, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Honorable Consejo Académico de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, 13 de febrero del 2023

.....

TUTOR DE INVESTIGACION

Ing. Rubio Peñaherrera Jorge Bladimir

C.C.: 050222229-2

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la Facultad de **CIENCIAS DE LA INGENIERÍA Y APLICADAS**; por cuanto, el postulante: **TIPANTA DIAZ KEVIN MAURICIO**, con el título del proyecto de investigación: **Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia".** Ha considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación del Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional

Latacunga, 13 de febrero del 2023

Para constancia firman:

Lector 1 (Presidente)
Nombre: MG. CANTUÑA KARLA
CC: 0502305113

Lector 2
Nombre: MG. VILLA MANUEL
CC: 1803386950

Lector 3
Nombre: ING. DIEGO FALCONÍ
CC: 0550080774

AGRADECIMIENTO

En el presente trabajo quiero agradecer primero a mis padres ya que, sin su apoyo emocional, económico no podría haber conseguido todo lo que he logrado, siempre estuvieron conmigo motivándome para culminar mi carrera.

A mi querida Universidad quien me acogió por años y en donde me forme como profesional y como persona, estoy agradecido por tantas alegrías que me ha brindado y siempre tendré los mejores recuerdos de esta mi querida Institución.

A mis profesores ya que cada uno de ellos impartieron sus conocimientos favoreciendo a desempeñar mi profesión con amor, valores éticos morales finalizando asi esta etapa académica.

Kevin Tipanta Díaz

DEDICATORIA

Quiero empezar dedicando este trabajo a dos personas muy importantes en mi vida universitaria que por circunstancias de la vida ya no me pueden acompañar en este gran momento de mi vida, me enseñaron el verdadero valor de la vida y las ganas de salir adelante papi Paco y papito Beto.

Por siguiente Quiero dedicar este trabajo con mucho amor a mis padres, que siempre han hecho hasta lo imposible por que culmine mi vida universitaria, estando conmigo dándome ánimos y fortalezas en todos los ámbitos de mi vida, es por esto que este logro es de ellos.

A mi Ñaña Mayte quien ha sido un pilar fundamental en toda mi vida y a quien le agradezco todo su cariño y enseñanzas que me ha regalado hasta el día de hoy. A mi sobrina Helen quien con sus ocurrencias al recibirme cuando llegaba de la universidad siempre me sacaba una sonrisa aun en los peores momentos a ellas quienes me han apoyado siempre en todos los caminos de mi vida y son parte de este triunfo profesional.

A mi enamora Jakeline que sin ella no podría haber conseguido este logro en mi vida siendo la persona que más me ha motivado en el estudio por el motivo que estaba lejos de mi casa con sus frases motivacionales y su amor infinito hacia mi persona y ella es mi pilar fundamental en mi triunfo profesional.

A mis abuelitos quienes me han guiado, enseñado el valor del trabajo y que me han llenado de amor en el tiempo que estuvieron conmigo, llegaron a ver el proceso de mi camino profesional, a mi Papito Pachito quien es un buen abuelito cariñoso y me siento bendecido porque está presente en otro paso de mi vida y me apoyado en todas las etapas de ella.

Por último, al Ing. Jorge Rubio quien ha sabido guiarme en este paso final de mi tesis y que, con su paciencia, enseñanzas, consejos ha logrado que culmine mi proyecto de una manera firme y ordenada.

Kevin Tipanta Diaz

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO: Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia".

Autor:

Tipanta Díaz Kevin Mauricio

RESUMEN

En los últimos años se ha comprobado que la gran mayoría de personas en el mundo tienen o usan un teléfono inteligente con los diferentes sistemas operativos ya sean estos Android o iOS, que actualmente podemos decir son los dos sistemas operativos para dispositivos móviles más utilizados debido a su fácil utilización y aprendizaje. El presente proyecto de investigación se enfoca en el análisis de las distintas herramientas forenses que contiene el Sistema Operativo Tsurugi lo que permitirá la obtención, recuperación y validación de información aplicando el modelo de proceso de Triage de Campo Forense Cibernético (CFFTPM) junto a las herramientas Android Triage y iOS Triage herramientas propias del Sistema Operativo Tsurugi proponen un enfoque "in situ" o de campo con la finalidad de la identificación, análisis e interpretación de la evidencia digital en un corto período de tiempo, con el beneficio de evitar los trámites burocráticos que retrasan los procesos de validación de evidencias.

Debido a que en la actualidad en la Oficina Técnica de Violencia las peritos no pueden dar una validez a la evidencias presentadas por los usuarios, toda vez que el mayor número de evidencias presentadas son mensajes instantáneos. Aplicando la metodología tradicional forense, el sistema será de utilidad para la obtención de información y con ello asegurar que los usuarios presenten sus evidencias a las peritos, es decir conllevara a identificar evidencias, adquirir datos y analizarlos para generar los respectivos informes. Aplicando las herramientas junto al modelo se comprueba mediante la documentación en cada una de las fases facilitando la realización de los informes finales, por ende, se verifica los aspectos más importantes que requiere un proceso de investigación como los es la rapidez y fiabilidad al momento de obtener una imagen forense, que permita validar la información recopilada, actividad que se realizó con la demostración del sistema a la oficina técnica evidenciando de todas las funciones del sistema Tsurugi son eficaces para las necesidades periciales con lo que se decreta la validez del presente trabajo.

Palabras Claves:

Dispositivos móviles, Sistema Operativo Tsurugi, Herramientas forense Digitales, Modelo de proceso de Triage de Campo Forense Cibernético.

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING SCIENCES AND APPLIED

THEME: "Analysis of mobile devices with the tools the Tsurugi Operating System from cases derived from "House of Justice" Technical Office of the Prison Violence Unit"

Author:

Tipanta Díaz Kevin Mauricio

ABSTRACT

In these years it has been verified that the large people around the world have or use a smartphone with different operating systems, whether Android or iOS, which can currently say are the two most widely used operating systems for mobile devices due to its easy use and learning. This research project focuses on the analysis of the different forensic tools contained in the Tsurugi Operating System, which will allow the obtaining, recovery and validation of information by applying the Cyber Forensic Field Triage process model (CFFTPM) together with the tools Android Triage and iOS Triage, Tsurugi Operating System tools, propose an "in situ" or field approach with the purpose of identifying, analyzing and interpreting digital evidence in a short period of time, with the avoiding bureaucratic benefit procedures, that delay the evidence validation processes.

Due to the fact that currently, in the Technical Office of Violence, the experts cannot validate the evidence presented by the users, since the greatest number of evidences presented are instant messages. Applying the traditional forensic methodology, the system will be useful for obtaining information and thus ensuring that users present their evidence to the experts, that is, it will lead to identifying evidence, acquiring data and analyzing it to generate the respective reports. Applying the tools together with the model, it is verified through the documentation in each of the phases, facilitating the preparation of the final reports, therefore, the most important aspects required by an investigation process are verified, such as speed and reliability at the time of obtaining a forensic image, which allows validating the information collected, an activity that was carried out with the demonstration of the system to the technical office, evidencing all the functions of the Tsurugi system are effective for the expert needs, thus the validity of this work is decreed.

Keywords: Mobile Devices, Tsurugi Operating System, Digital Forensic Tools, Cyber Forensic Field Triage Process Model.

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del proyecto de investigación cuyo título versa: **"ANÁLISIS DE DISPOSITIVOS MÓVILES CON LAS HERRAMIENTAS DEL SISTEMA OPERATIVO TSURUGI DE CASOS DERIVADOS DE LA OFICINA TÉCNICA DE LA UNIDAD DE VIOLENCIA CARCELÉN" CASA DE JUSTICIA""** presentado por **Tipanta Diaz Kevin Mauricio**, egresado de la carrera de **Sistemas de información** perteneciente a la **facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad por lo que autorizo al peticionario hacer uso del presente aval para los fines académicos legales.

Latacunga, 8 de febrero del 2023

Atentamente,

CENTRO DE IDIOMAS

Mg. Lidia Rebeca Yugla Lema.
DOCENTE DEL CENTRO DE IDIOMAS-UTC
0502653340

1. INFORMACIÓN GENERAL

TÍTULO DEL PROYECTO:

Análisis de dispositivos móviles con las herramientas del Sistema Operativo Tsurugi de casos derivados de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia".

FECHA DE INICIO:

Octubre 2022

FECHA DE FINALIZACIÓN:

Marzo 2023

LUGAR DE EJECUCIÓN:

Provincia: Pichincha, Cantón: Quito Sector: Carcelén industrial Calles Joaquín Mancheno y Tadeo Benítez /Consejo de la judicatura "Oficina técnica de violencia Casa de Justicia".

UNIDAD ACADÉMICA QUE AUSPICIA:

Universidad Técnica de Cotopaxi

CARRERA QUE AUSPICIA:

Ingeniería en Sistemas de Información.

EQUIPO DE TRABAJO:

COORDINADOR:

Nombre:	Ing. Jorge Bladimir Rubio Peñaherrera.
Nacionalidad:	ecuatoriano
Fecha de Nacimiento:	Pujilí, 16 de mayo de 1976.
Estado Civil:	Casado
Residencia:	Pujilí, Calle Gabriel Álvarez 1-13 y Juan José Merizalde.
E-mail:	jorge.rubio@utc.edu.ec
	jbladimirrp@hotmail.com

Teléfono: 0995220308

Títulos Obtenidos:

PREGRADO: Ingeniero en Informática y Sistemas Computacionales

POSGRADO: Magister en Gerencia Informática, mención Desarrollo de Software y Redes – PUCE-SA.

Diplomado Superior en Gerencia Informática PUCE-SA.

ESTUDIANTE:

Nombre: Tipanta Diaz Kevin Mauricio
Nacionalidad: ecuatoriano
Fecha de Nacimiento: 04 de diciembre de 1999
Estado Civil: Soltero
Residencia: Pichincha "Sangolquí-Rumiñahui"
Correo: kevin.tipanta4612@utc.edu.ec
Teléfono: 0983382250

ÁREA DEL CONOCIMIENTO:

06 Información y comunicación (TIC)/ 061 Información y Comunicación (TIC)/

0612 Base de datos, diseño y administración de redes.

LÍNEA DE INVESTIGACIÓN:

Tecnología de la Información y comunicación

SUB LÍNEA DE INVESTIGACIÓN DE LA CARRERA:

Diseño implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2. INTRODUCCIÓN

Los dispositivos móviles se han convertido en plataformas de información de alta capacidad, cada vez más utilizados por la fuerza de trabajo. Cada generación de dispositivos móviles trae consigo nuevas innovaciones y tecnologías que día con día continúan en crecimiento. Las capacidades de estos dispositivos están en constante evolución, proporcionando a los usuarios una mayor capacidad de almacenamiento, la realización de tareas adicionales como mensajes de texto, mensajes multimedia, mensajería instantánea, correo electrónico y navegación por Internet. Con el tiempo, estos dispositivos también acumulan información considerable sobre el propietario y las actividades realizadas por éste. Pero, algo que debemos tomar en cuenta es que mientras existan más servicios que nos facilita las cosas de igual forma va incrementado el peligro, es decir, al proporcionar tantas facilidades también proporciona más facilidades para cometer algún delito o crimen.

Cuando los dispositivos móviles están involucrados en un crimen u otro incidente estos pueden ser de gran utilidad como evidencia digital y así poder establecer la responsabilidad legal del propietario. Los datos de un dispositivo móvil deben ser recuperados de tal modo que se evite la modificación y se mantenga la integridad del contenido recuperado.

Cualquier mecanismo de seguridad que impida la recuperación de datos, debe ser evitado o eliminado. Con el auge en el uso de la telefonía celular como medio para la realización de actos ilícitos o que estén involucrados en uno, varias empresas y organizaciones se han dedicado al desarrollo de distintas herramientas y metodologías forenses para el análisis de dispositivos móviles. El análisis forense a dispositivos móviles (celulares), es cada vez mayor, en consecuencia, las herramientas forenses son un desarrollo relativamente reciente y en las primeras etapas de madurez. Por lo que especialistas forenses requieren de metodologías y herramientas que permitan la recuperación adecuada e integra de datos, y así poder presentar un informe detallado de los datos contenidos en el equipo involucrado.

La presente investigación demuestra como aplicando una metodología forense se puede obtener información segura que permita a los peritos informáticos analizar las evidencias presentadas por los usuarios y de esta manera obtener datos, analizar los mismos y generar informes aplicando las herramientas del Sistema Operativo Tsurugi, para la presente investigación se tomó como caso de estudio la Oficina Técnica de la Unidad de Violencia Carcelén o conocida también como “Casa de Justicia”. El Modelo de Proceso de Triage de Campo Forense

Cibernético (CFFTPM) junto al Sistema operativo Tsurugi propone un enfoque in situ o de campo con la finalidad de la identificación, análisis e interpretación de la evidencia digital en un corto período de tiempo, con el beneficio de evitar los trámites burocráticos que retrasan los procesos de validación de evidencias. El modelo propuesto se adhiere a los principios forenses comúnmente mantenidos, y no niega la capacidad que una vez concluido el campo de triage inicial, los sistemas o medios de almacenamiento sean transportados de vuelta a un entorno de laboratorio para un examen más exhaustivo y análisis. El CFFTPM se ha utilizado con éxito en varios casos del mundo real, y su importancia investigadora y enfoque pragmático ha sido ampliamente demostrado. Además, las pruebas derivadas de estos casos no han sido impugnado en los procedimientos judiciales donde se ha introducido.

2.1. EL PROBLEMA

En la actualidad la Unidad Judicial de Violencia Intrafamiliar Carcelén "Casa de Justicia" tiene como dificultad la validación de la información que es entregada por los usuarios de los dispositivos móviles de manera inmediata, ágil y oportuna con la finalidad de conocer si estos o no han sido adulterados. Por consiguiente, si se requiere una pericia informática esta llevaría mucho tiempo y costaría mucho dinero ya que estas llevan un extenso periodo de tiempo en donde se necesita seguir un proceso que inicia con la cadena de custodia, desmaterialización de las evidencias y designación de un perito informático. Esto complica a la unidad de violencia debido a que es una unidad de contravenciones por tal motivo los delitos poseen otro tratamiento basado en la Ley orgánica para la prevención y erradicación de genero contra las mujeres, expedita que tiene que ser atendida inmediatamente.

2.1.1. Situación Problémica

En países como México, regulado por la Auditoría Superior de la Federación (ASF), la modalidad de auditoría forense existe y "consiste en la aplicación de una metodología de fiscalización que conlleva la revisión rigurosa y pormenorizada de procesos, hechos y evidencias, con el propósito de documentar la existencia de un presunto acto irregular[1]", Mientras que en Perú esta modalidad procura "obtener y analizar la información para evidenciar la ocurrencia de hechos contrarios a las normas legales y de corresponder la cuantificación del perjuicio económico, aplicando procedimientos y técnicas forenses que aseguren la preservación de la cadena de custodia[1]"

En el Ecuador el manejo y la entrega de evidencias digitales son validadas por los peritos forenses de las oficinas forenses de la Policía Nacional lo cual conlleva una cadena de custodia de los dispositivos entregados lo que causa que las pruebas (evidencias) no tengan algunas veces la validez inmediata por lo que en las Oficinas Técnicas de Violencia presentan esos pequeños inconvenientes al momento que se presenta un caso de flagrancia no contar con las valides de pruebas presentadas en ese momento.

En la Oficina Técnica de Violencia se presenta un gran problema al momento de validar las evidencias (mensajes, audios, imágenes) de las partes procesales ya que las peritos no cuentan con un sistema ni un perito en su oficina para dar validez a las mismas evidencias, información que debe ser procesada en el menor tiempo posible el cual por falta de tiempo se deben acoger que son pruebas legitimas. Una de las pruebas entregadas son mensajes de texto de dispositivos móviles los cuales como evidencia pericial llevaría mucho tiempo al solicitar una pericia judicial de estos peritos dispositivos. Con el Sistema Operativo Tsurugi y sus herramientas se puede obtener la información requerida en menor tiempo requerido.

2.1.2. Formulación del problema

¿Cómo la implementación de modelos de análisis permitirá que se evite las pérdidas y edición de evidencias digitales en un proceso judicial?

2.2. OBJETO Y CAMPO DE ACCIÓN

2.2.1 Objeto de estudio:

Proponer un Marco de trabajo para el análisis forense a dispositivos móviles en la oficina técnica de la Unidad de Violencia Carcelén "Casa de Justicia".

2.2.2 Campo de Acción:

Aplicación de las metodologías de análisis forense para el desarrollo de un marco de trabajo utilizando las herramientas específicas del Sistema Operativo Tsurugi.

2.3.BENEFICIARIOS

Tabla 1. Beneficiarios

BENEFICIARIOS	***CARGO***	***DESCRIPCIÓN***	***N DE PERSONAS***
Directos	*Trabajadora social*	*Instigaciones periciales, seguimientos, acompañamientos sociales, coordinación con las redes comunitarias.*	*1*
	Psicóloga	*Evaluaciones psicológicas forenses, coordinación, atención, cámaras de Gesell, asistencia a audiencias penales.*	*1*
Sub Total Beneficiarios Directos			*2*
Indirectos	*Procesada*	*Usuario denunciado por el cometimiento de presuntos hechos violentos (físicos, psicológicos, tecnológicos).*	*15*
	Presunta victima	*Persona que denuncia un hecho que se siente afectada su integridad física, psicológica y sexual.*	*15*
Sub Total Beneficiarios Indirectos			*30*
Total de beneficiarios			*32*

Fuente: Investigador

2.4. JUSTIFICACIÓN

La Oficina Técnica de la unidad judicial de violencia contra la mujer y miembros del grupo familiar en sus siglas "UJVCMYMGF" como promedio realiza de 30 a 35 investigaciones mensuales de casos dispuestas por la autoridad competente, una de las limitantes que posee esta dependencia es que no cuentan con un perito informático que permita identificar si las pruebas presentadas por las partes procesales han sido adulteradas en lo referente a mensajes de texto,

audio entre otras pruebas informáticas de dispositivos móviles a estudiar, toda vez que los procesos contravenciones son cortos y realizar un peritaje informático de este tipo, llevaría tiempo, dinero y costos que los usuarios se encuentran limitados a solventar, abandonando los procesos favoreciendo la impunidad.

Es por ello la importancia de establecer este tipo de proyectos investigativos que permitan viabilizar el trabajo de las oficinas técnicas y así contribuir al acceso a la justicia de manera rápida y eficaz. Por otro lado, contar con un equipo que hace referencia a Digital Forense & Incident Response Análisis Forense Digital y Respuesta ante Incidentes o conocido por sus siglas "DFIR" se convierte hoy en día en un pilar fundamental para las grandes organizaciones Judiciales ya que, con el aumento del cibercrimen y la presentación de evidencias digitales, se hace primordial contar con un equipo capaz de prevenir posibles ataques y hacerles frente con una respuesta de incidencia efectiva.

Los teléfonos celulares modernos poseen una gama impresionante de capacidades que eran insondables para un dispositivo tan pequeño y portátil hace apenas una década. Esto, combinado con su omnipresencia, puede convertirlos en una fuente invaluable de datos dentro de cualquier caso civil o penal.

El análisis forense en dispositivos móviles actualmente es unas ciencias importantes ya que con las diferentes herramientas que podemos establecer técnicas y metodologías para la obtención de evidencias y recuperar datos que por terceros hayan sido eliminados.

2.5. HIPÓTESIS

La aplicación de las herramientas forenses del Sistema Operativo Tsurugi permitirá agilizar los procesos de obtención, recuperación y validación de información en la Oficina Técnica de la Unidad Judicial de Violencia Intrafamiliar.

2.5.1. Variable Independiente

Sistema Operativo Tsurugi y sus herramientas forenses.

2.5.2 Variable Dependiente

Análisis y validación de evidencias presentadas por los usuarios de la Oficina Técnica de la Unidad Judicial de Violencia Intrafamiliar Carcelén.

2.6. OBJETIVOS

2.6.1. Objetivo General

Analizar las distintas herramientas forenses del Sistema Operativo Tsurugi para la obtención, recuperación y validación de información mediante las evidencias presentadas en la oficina Técnica de Violencia por parte de las presuntas víctimas.

2.6.2. Objetivos Específicos

- Definir las bases teóricas referentes al análisis y seguridad de dispositivos móviles, de las evidencias presentadas en la oficina técnica de violencia Carcelén para su respectiva investigación.
- Especificar los artículos del COIP relacionados a los Delitos Informáticos contemplados en la Ley Ecuatoriana.
- Establecer la metodología, técnicas y herramientas oportunas para el análisis de dispositivos móviles en la Oficina Técnica de violencia Carcelén.

2.7. SISTEMA DE TAREAS

Tabla 2. Sistemas de Tareas

OBJETIVOS ESPECÍFICOS	ACTIVIDADES	RESULTADO DE LAS ACTIVIDADES	DESCRIPCIÓN (TÉCNICAS E INSTRUMENTOS)
Definir las bases teóricas referentes al análisis y seguridad de dispositivos móviles, de las evidencias presentadas en la oficina técnica de violencia Carcelén para su respectiva investigación.	• Buscar información en Diferentes fuentes bibliográficas. • Clasificación de la Información más relevante acorde al tema a investigar. • Describir y generar citas bibliográficas.	Marco teórico	Recopilación Bibliográfica (Fichas Bibliográficas)
Especificar los artículos del COIP relacionados a los Delitos Informáticos contemplados en la Ley Ecuatoriana.	• Buscar información sobre las penalizaciones en el ecuador de acuerdo al (COIP). • Indagar información sobre los artículos de la ley de comercio electrónico, firmas y mensaje de datos.	Selección de los delitos informáticos acorde a nuestra investigación	Código Orgánico Integral Penal De La República Del Ecuador Asamblea Nacional.
Establecer la metodología, técnicas y herramientas oportunas para el análisis de dispositivos móviles en la Oficina Técnica de violencia Carcelén.	• Análisis y comparación de herramientas del sistema operativo forense a utilizar. • Selección de herramientas más favorables para el análisis de dispositivos móviles.	• Selección de las mejores herramientas para el análisis forense digital. • Tabla comparativa de sistemas operativos forenses para dispositivos móviles. • Tabla comparativa de modelos de análisis de dispositivos móviles	• Entrevistas y Encuestas (Formulario). • Reuniones Presenciales (Fotografías). • Pruebas del Software Tsurugi.

3. FUNDAMENTACIÓN TEÓRICA

3.1.¿QUÉ ES FORENSE?

DESDE LA PERSPECTIVA DE CARAGUAY RAMÍREZ STALIN EN LA REFERENCIA [1] SUSTENTA: Que en general constituyen el conjunto de ciencias naturales y del derecho, aplicadas a investigación del delito, en servicio de los entes que procuran justicia mediante el respeto de la normativa relacionada y de la rigurosidad científica necesaria en su producción.

Por ende, lo forense va de la mano de la ciencia lo cual conlleva a la investigación de algún tipo de delito ya sea este sexual, violento u otro calificado por la fiscalía y la judicatura.

3.2.¿QUÉ ES ANÁLISIS?

LA REAL ACADEMIA ESPAÑOLA (RAE) EN LA REFERENCIA [2] DECLARA QUE: El análisis es una Distinción y separación de las partes de algo para conocer su composición por otro lado es el Estudio detallado de algo, especialmente de una obra o de un escrito.

Gracias a la referencia dice que el análisis es el estudio detallado de un objeto, evento o situación para encontrar su base, motivos y causas a partir de su origen, creación o causas originales.

3.3.¿QUÉ ES DIGITAL?

LA REAL ACADEMIA ESPAÑOLA (RAE) EN LA REFERENCIA [3] DECLARA: Lo digital es un dispositivo o sistema: Que crea, presenta, transporta o almacena información mediante la combinación de bits.

Con la referencia expresa que lo digital es una facción de dispositivos utilizados para generar, transmitir, administrar, encausar y guardar señales digitales por medio de bits.

3.4.¿QUÉ ES UN DISPOSITIVO?

LA REAL ACADEMIA ESPAÑOLA (RAE) EN LA REFERENCIA [4] **DECLARA QUE:** Es un mecanismo o artificio para producir una acción prevista. Como resultado, puede ser comprendido como una mediación donde se establece el dialogo constante entre las relaciones de poder y saber.

3.5.DISPOSITIVO MÓVIL

FERNÁNDEZ-GONZÁLEZ, MANUEL; TORRES-GIL, ANTONIO JESÚS EN LA REFERENCIA [5] **MANIFIESTAN QUE :**Un dispositivo tecnológico o móvil puede entenderse un objeto o sistema que aúna ciencia y tecnología, y es utilizado por el hombre para mejorar su calidad de vida y el funcionamiento de la sociedad en que vive.

CLAROS, ÓLIVER ARIEL EN LA REFERENCIA [6] **CONSIDERA QUE:** Los dispositivo móviles son una pieza fundamental del mercado, que trae consigo una avalancha de nuevos modelos, colores, sabores, funciones, tecnologías , comunicación oral, radio y teléfono; mensajes de texto, explica básicamente que el teléfono móvil es el primer dispositivo portátil que permitió la comunicación entre dos personas de diferentes partes de un país, ciudad en tiempo real.

Se puede definir como un aparato de pequeño tamaño con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red con memoria limitada, que ha sido diseñado específicamente para una función pero que puede llevar a cabo otras funciones más generales.

3.6. ¿QUÉ ES UN MENSAJE?

EN LA REFERENCIA [7] EXPLICA QUE: La evidencia en la mensajería puede fortalecer un caso al proporcionar pruebas de maltrato y una imagen más clara de la dinámica de la relación, Aunque la evidencia en la mensajería puede ser extremadamente útil, no siempre se busca o se recopila de manera correcta, y puede eliminarse o adulterarse accidentalmente.

3.6.¿QUÉ ES UN WHATSAPP?

MARÍA GUADALUPE VEYTIA BUCHELI Y FELIPE ANTONIO BASTIDAS TERÁN EN LA REFERENCIA [8] **ARGUMENTAN:** que WhatsApp tiene grandes ventajas comunicativas, tecnológicas y económicas indudable que los distintos lenguajes digitales facilitan y diversifican la manera de comunicación de las personas, destacan que esta aplicación se ha consolidado como la principal herramienta de comunicación y la más influyente de las microrredes.

3.9. ANÁLISIS DIGITAL

MARÍN LÓPEZ, JUAN CAMILO; LÓPEZ TRUJILLO, MARCELO EN LA REFERENCIA [9] **EXPRESAN QUE:** El hoy en día hay una gran cantidad de desafíos, los cuales incluyen la captura, limpieza, almacenamiento, búsqueda, intercambio, transferencia, análisis, visualización y extracción de los datos.

Por ende, se descubrió que el análisis tiene muchas oportunidades sin explotar en el espacio de la seguridad informática y más aún en la computación forense así creando las distintas herramientas sofisticadas para la extracción y validación de la información encontrada.

3.9.1. Análisis forense digital

CARAGUAY RAMÍREZ STALIN EN LA REFERENCIA [1] **MANIFIESTA QUE :** El análisis forense digital como la rama de las ciencias forenses que se ocupa de recopilar, analizar y preservar los datos de los dispositivos digitales con la finalidad de utilizarlos para resolver casos criminales y que se puedan presentar como evidencia admisible en el ámbito legal en los tribunales de justicia. En una pequeña explicación podemos decir que es la aplicación de técnicas científicas y analíticas especializadas y orientadas a una infraestructura tecnológica que permitan:

- Buscar
- Analizar
- Perseverar
- Presentar

Datos que sean válidos dentro de un proceso penal.

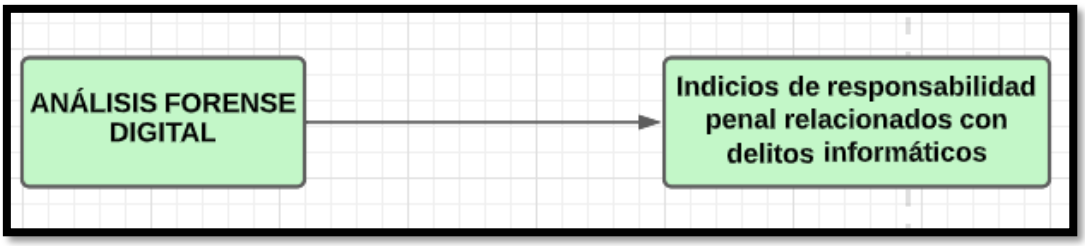


Figura 1. Relación entre el análisis forense digital y los delitos informáticos

3.10. INFORMÁTICA FORENSE

FLAVIO CEZAR AMATE, FELIPE RODRÍGUEZ MARTÍNEZ BASILE , NADJILA TEJO MACHADO EN LA REFERENCIA [10] **EXPRESAN:** Que la informática forense desarrolla hipótesis y responde preguntas sobre el ciber incidente o delito mediante la recolección de evidencia que ayude a esclarecerlo), con el fin de preservar la integridad de los datos, analizarlos y resolver el delito.

Con ello se establece que la informática forense es de gran ayudar para esclarecer y dar valides a las pruebas que sean encontradas y presentadas ante la justicia.

3.11. INFORMÁTICA FORENSE EN DISPOSITIVOS MÓVILES

YU LUNG LI EN LA REFERENCIA[11] **MANIFIESTA QUE:** El análisis de dispositivos móviles es el uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop DFRWS).

El análisis de dispositivos móviles es una de las técnicas digitales forenses que normalmente se aplican en los dispositivos móviles para obtener evidencia del dispositivo, creando así imágenes forenses para la desmaterialización y aprobación de evidencias presentadas.

3.12. INFORMÁTICA FORENSE EN DISPOSITIVOS MÓVILES ANDROID

BELTRAN, TAPIA EN LA REFERENCIA [12] **MANIFIESTAN QUE :**El sistema más utilizado en dispositivos móviles es Android. Las empresas desarrolladoras de sistemas operativos envían actualizaciones constantes con la finalidad de corregir vulnerabilidades existentes, el internet a dado paso a la conexión de una red global entre dispositivos móviles, por lo que, la seguridad en este se ha convertido en un desafío para los desarrolladores, cada día aparece millones de ataques por parte de ciberdelincuentes a entidades gubernamentales, empresas privadas y usuarios comunes, de esta manera la investigación forense pasa a formar parte fundamental para esclarecer estos hechos delictivos.

Es importante revisar bibliografía que permita la gestión de una causa pericial, con la finalidad de, proporcionar un informe detallado, los investigadores tienen a disposición; estándares, guías, y metodologías como:

- **ISO/IEC 27037**: Directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital. Es un documento que, publicó la Organización Internacional para la estandarización (ISO).
- **RFC 3227:** Guía para recolectar y archivar evidencia. Proporciona sistemas, directrices para la recopilación y archivo de las pruebas en un incidente de seguridad.
- **UNE 71505:** Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. Proporcionan la información sobre los sucesos en un sistema de información.
- **UNE 71506:** Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas. Define los procesos del análisis forense dentro del ciclo de gestión de evidencias electrónicas.

3.14. TIPOS DE ADQUISICIÓN

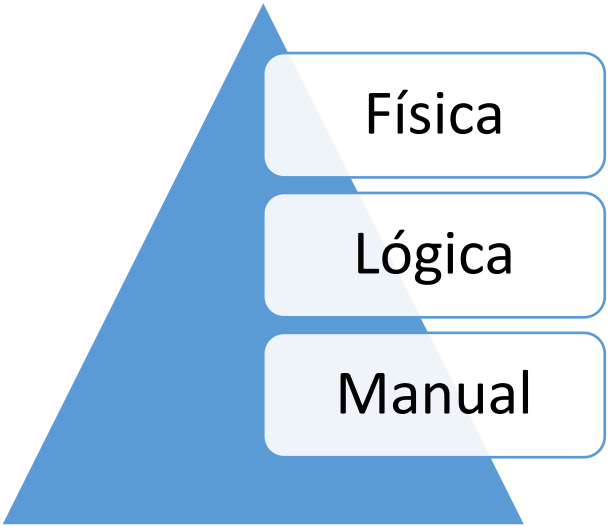


Figura 2. Tipos de adquisición

- **FÍSICA:** Requiere manipular el dispositivo y navegar su contenido
- **LOGICA:** Se emplean software y hardware
- **MANUAL:** Es una copia bit a bit del chip de almacenamiento de datos, esta técnica considera como la más compleja

3.15. EVIDENCIA

LA REAL ACADEMIA ESPAÑOLA (RAE) EN LA REFERENCIA [13] **DECLARA QUE:** La evidencia es un término del latín evidentĭa que nos permite confirmar una certeza aparente, que es innegable y está fuera de toda duda, en conocimiento público, revelando o demostrando algo.

Por lo que podemos interpretar que la evidencia es una prueba que nos permitirá confirmar, comprobar y establecer si algo es verdadero o no.

3.15.1. Evidencia digital

MALEZA JORGE, SANDOVAL KARINA, HIDALGO PABLO EN LA REFERENCIA [14] **DEDUCEN QUE:** Los elementos de prueba o evidencias dentro de un proceso judicial son de vital importancia, ya que mediante su investigación se puede llegar a determinar la confirmación o desvirtuación de una hipótesis o afirmación precedente de lo que corresponde a la verdad.

Es importante destacar, que, para garantizar una validez probatoria de la evidencia digital, esta debe cumplir con ciertos requerimientos como es: ser admisible, autentica, completa, creíble, segura y confiable. De igual forma cabe mencionar que la evidencia digital se clasifica en tres categorías:

- Registros almacenados en equipos de tecnología informática. Son todos los documentos creados y almacenados por el usuario en el equipo de tecnología informática[15].

- Registros generados por equipos de tecnología informática. Son todos los documentos que son el resultado del uso del equipo de tecnología informática, el usuario no los puede alterar[15].

- Registros híbridos. Conformados por los registros almacenados y generados por equipos de tecnología informática[15].

En consecuencia, la Evidencia Digital o también conocida como evidencia electrónica, no es fácil encontrar una definición única. Es más, desde la perspectiva del campo de la prueba, puede definirse como cualquier tipo de información digital almacenada o transmitida, que también puede ser tratada en un juicio si se demuestra que constituye una dependencia entre un delito y su implicado.

3.15.2. Evidencia digital jurídica

Son todas las pruebas, peritajes diligencias que se llevan dentro de un proceso que son validadas y aprobadas por un juez.

3.16. TSURUGI

UCAPEM GROUP-ECUADOR EN LA REFERENCIA [16] **DESCRIBE:** Que Tsurugi, Es una distribución más de Linux pero con una gran ventaja, ya que se trata de una Distro DFIR personalizada y sobre todo gratuita, Contiene varias herramientas personalizadas y de fácil administración, que no solo se basan en la típica consola de Linux, sino que se ejecutan en un ambiente gráfico y de sencilla operatividad.

TSURUGI OFICIAL EN LA REFERENCIA [17] **SOSTIENE :**Que Tsurugi es una distribución de Linux altamente personalizada diseñada para respaldar sus investigaciones DFIR , análisis de malware y actividades OSINT (Open Source INTelligence).

En resumen, La distribución de Tsurugi Linux es uno de los sistemas más completos para el análisis forense digital con sus múltiples herramientas que con como un mundo aparte junto a ello que es una distribución open source que cualquier área de trabajo podría implementarla.

3.16.1. Versiones de Tsurugi

Tabla 3. Versiones de Tsurugi [18].

VERSIÓN	FECHA DE LANZAMIENTO	OBSERVACIONES
2018.1	3 de noviembre de 2018 (edición especial)	• Primera Versión
2019.1	20 August 2019	• New Kernel 5.1.15 • New section "Computer Vision" • New Tsurugi device unlocker GUI
2019.1 VM	24 September 2019	• Exceptionally ONLY for this Virtual Machine • FIX iptables problem (with a kernel update) • FIX a minor problem about ntfs-3g • FIX plaso (with update dfdatetime library) • FIX RAM saturation workaround
2020.1	18 March 2020	• FIX Installer with UEFI system • Install android_triage • Update APOLLO • Update addons Firefox (DFIR & OSINT profiles)
Special BLACKHAT USA	4 August 2021 (special edition)	• Added many new tolos • Removed old no more maintained tolos
2021.1 VM	25 September 2021	• New Kernel 5.14.6 • New computer vision features • Removed old no more maintained tolos
Release 2022.1 VM	19 January 2022	• New custom Kernel 5.15.12 • Install Android File Transfer (MTP) • Install Android-PIN-Bruteforce • Install apollo • Install audit-P2SH-multisig • Full system update

3.16.2. Herramientas de Tsurugi

Tabla 4. Herramientas Tsurugi

TIPO	*NOMBRE*	*DESCRIPCIÓN*
IMAGING	Dd	Cuyo objetivo principal es convertir y copiar archivos.
	Dcfldd	Aplicar hash a los datos de entrada a medida que se transfieren, lo que ayuda a garantizar la integridad de los datos.
PASSWORD RECOVERY	Bruteforece-Wallet	Intenta descifrar una de las direcciones cifradas en la billetera probando todas las contraseñas posibles.
	hashcat utils	El descifrador de contraseñas más rápido del mundo.
TIMELINE	Plaso	Una herramienta llamada log2timeline es una herramienta desarrollada en Python que le permite extraer una línea de tiempo de todos los eventos que suceden en su sistema.
	Turbinia	Los trabajadores del grupo ejecutan tareas para procesar la evidencia una. Las tareas leen Evidencia del almacenamiento compartido o se copian del almacenamiento en la nube.
MOBILE FORENSICS	Fastboot	permite al usuario flashear varias particiones del sistema, incluida la recuperación. Puede controlar su teléfono en el modo "fastboot" usando la línea de comandos de Windows o Linux (similar a ADB).
	Apollo	Los datos de patrón de vida se pueden usar en muchos tipos de investigaciones para obtener información extremadamente detallada de los usuarios de dispositivos.

3.17. SISTEMAS OPERATIVOS PARA ANÁLISIS FORENSE DIGITAL

Sistemas operativos análisis forense

HERRAMIENTA	DESCRIPCIÓN
TSURUGI LINUX	Esta distribución basada en Ubuntu está diseñada para análisis forense digital y respuesta a incidentes.
SANTOKU	Funciones de seguridad, incluye herramientas de análisis forense móvil, como flasheo de firmware, RAM, tarjetas de medios y herramientas de imágenes NAND, fuerza bruta para el cifrado de Android, análisis de copias de seguridad de IPhone y más[19].
KALI LINUX (MODO FORENSE)	El disco duro del dispositivo permanece intacto, así como la partición de intercambio. El montaje automático para dispositivos externos también está deshabilitado para CD[20].
CAINE LIVE FORENSIC TOOL	Es otra distribución en vivo de Linux de análisis forense informático. Es una de las herramientas más populares en informática forense e incluye utilidades forenses de primer nivel como Autopsia[21].
HELIX E-FENSE LIVE RESPONSE	Esta herramienta forense en vivo desarrollada para unidades flash USB fue diseñada para recopilar datos volátiles antes de que una computadora se apague. Todos los datos se almacenan en la unidad flash USB. Esta es una de las herramientas más recomendadas para el primer acercamiento al dispositivo a investigar[22].
VOLATILITY FORENSIC TOOL	Es una herramienta interesante para analizar y diagnosticar la salud del dispositivo después de que se detecte un ataque, ya está incluida en todas las distribuciones de Linux que se enfocan en el análisis forense de computadoras mencionado anteriormente[23].

3.18. MODELOS DE ANÁLISIS DE DISPOSITIVOS MÓVILES

JAYA CÁCERES KATHERIN EN LA REFERENCIA [15] **MANIFIESTA QUE:** Los peritos informáticos necesitan modelos eficientes que, ayuden a mejorar los procedimientos a ejecutarse dentro del análisis forense, es necesario que, estas operaciones se sujeten a la normativa legal vigente, en la extracción de datos no se altera su estructura original para luego ser analizada y emitir el informe pericial. Se analiza los modelos existentes de diversos autores con el fin de, optar por los más eficientes, que, permitan obtener resultados óptimos en el análisis forense.

3.19. MODELO DFRWS (DIGITAL FORENSIC RESEARCH WORKSHOP)

JASON SACHOWSKI EN LA REFERENCIA TRADUCIDA [25] **SUSTENTA QUE :** El modelo aporta el concepto conocido como "Clases de Acción en la Investigación Digital". Estas "Clases de Acción" son técnicas que permiten clasificar por grupos las actividades en un proceso investigativo. El modelo establece que cada investigación se debe establecer de forma independiente y detallada en una matriz, indicando las actividades a realizar y la técnica que se implementará en la misma.

Figura 3. Fases de (DFRWS) [26].

1. **Identificación:** Esta etapa permite ejecutar el reconocimiento y determinar el tipo de suceso[12].
2. **Preservación:** Esta etapa contiene la cadena de custodia, para que, los datos no sean manipulados[12].
3. **Recolección:** Los datos son recolectados mediante la utilización de herramientas tecnológicas tanto de software como de hardware.

4. **Inspección:** Se analizan los datos recogidos los que, permitirán la reconstrucción de los hechos[12].
5. **Análisis:** Mediante el resultado del análisis de los datos se realiza la reconstrucción de los hechos[12].
6. **Presentación:** Se emite el informe pericial documentado con sus respectivas conclusiones[12].
7. **Decisión:** La información obtenida se constituye en un factor decisivo en el dictamen de la sentencia[12].

3.20. MODELO GCFIM (GENERIC COMPUTER FORENSIC INVESTIGATION MODEL)

MUSHTAQUE, KHURAM; AHSAN, KAMRAN; UMER, AHMER EN LA REFERENCIA TRADUCIDA [27] **MANIFIETAN QUE :** El modelo (GCFIM), propuesto por Yunus Yusoff y sus colaboradores, esta investigación fue analizada a partir de modelos forenses creados entre el año 1985 hasta el año 2011, el trabajo dio como resultado cinco etapas genéricas de los modelos que, le anteceden, de esta manera se da inicio a este nuevo modelo.

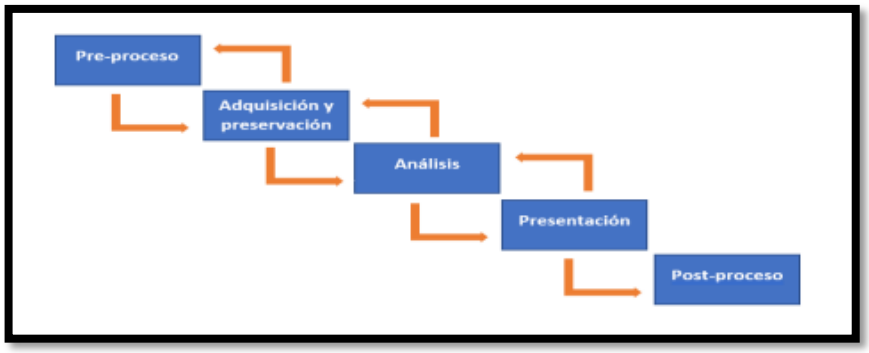


Figura 4. Fases del modelo (GCFIM) [26].

Tabla 5. Fases modelo (GCFIM)

NOMBRE DE LA FASE	DESCRIPCIÓN
Preproceso:	Esta etapa se constituye en el pilar para las siguientes fases, se verificará el cumplimiento del uso adecuado de las herramientas a emplearse que, el grupo forense se encuentre capacitado, además, se diligenciará los procesos necesarios para la aplicación en el análisis como; permisos, preferencias y consentimientos

Tabla 6. Fase modelo (GCFIM) (Continuación)

NOMBRE DE LA FASE	DESCRIPCIÓN
Preproceso:	Esta etapa se constituye en el pilar para las siguientes fases, se verificará el cumplimiento del uso adecuado de las herramientas a emplearse que, el grupo forense se encuentre capacitado, además, se diligenciará los procesos necesarios para la aplicación en el análisis como; permisos, preferencias y consentimientos
Adquisición y preservación:	A esta etapa se le atribuye subprocesos como el reconocimiento y recopilación de la prueba en el lugar de los hechos, la integridad de los datos será esencial en esta etapa, por lo que, se proporcionará seguridad en el transporte y almacenamiento para impedir cambios de la información obtenida que, será utilizada en la siguiente etapa
Análisis:	Se realizará una exploración a profundidad de los datos obtenidos en la etapa anterior y se ordena de acuerdo con la importancia con la que, se le considere para el análisis, además, se excluye información que, no sea relevante en el proceso
Presentación:	Se elabora la documentación; informes y reportes con respecto al análisis de los datos obtenidos en la etapa anterior.
Post proceso:	Etapa en la que, se presenta el informe pericial ante la función judicial. Lo que, ayudará a determinar si existe responsabilidad de él cometimiento de una infracción o delito así como los implicados en la investigación [27].

3.21. CÓDIGO INTEGRAL PENAL (COIP)

Establece una serie de sanciones relacionadas con los delitos informáticos y de telecomunicaciones en el Ecuador, entre ellos se destacan:

Artículo 69 (2a)

2. Comiso penal, procede en todos los casos de delitos dolosos y recae sobre los bienes, cuando estos son instrumentos, productos o réditos en la comisión del delito. No habrá comiso en los tipos penales culposos. En la sentencia condenatoria, la o el juzgador competente dispondrá el comiso de:

a) Los bienes, fondos o activos, o instrumentos equipos y dispositivos informáticos utilizados para financiar o cometer la infracción penal o la actividad preparatoria punible[28].

Artículo 103. - Pornografía con utilización de niñas, niño o adolescentes: La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o

adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años[28].

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años[28].

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años[28].

Artículo 178.- Violación a la intimidad: La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años[28].

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley[28].

La retractación no constituye una forma de aceptación de culpabilidad.

Artículo 354.- Espionaje: La o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando:

1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado[28].

2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial [28].

3. Envíe documentos, informes, gráficos u objetos que pongan en riesgo la seguridad o la soberanía del Estado, sin estar obligado a hacerlo o al haber sido forzado no informe inmediatamente del hecho a las autoridades competentes [28].

4. Oculte información relevante a los mandos militares o policiales nacionales[28].

5. Altere, suprima, destruya, desvíe, incluso temporalmente, información u objetos de naturaleza militar relevantes para la seguridad, la soberanía o la integridad territorial [28].

Si la o el servidor público realiza alguno o varios de estos actos en tiempo de conflicto armado, será sancionado con pena privativa de libertad de diez a trece años [28].

Artículo 456.- Cadena de custodia: Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio[28].

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[28].

Artículo 475.- Retención de correspondencia: La retención, apertura y examen de la correspondencia y otros documentos se regirá por las siguientes disposiciones:

1. La correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código[28].

2. La o el juzgador podrá autorizar a la o al fiscal, previa solicitud motivada, el retener, abrir y examinar la correspondencia, cuando haya suficiente evidencia para presumir que la misma tiene alguna información útil para la investigación[28].

3. Para proceder a la apertura y examen de la correspondencia y otros documentos que puedan tener relación con los hechos y circunstancias de la infracción y sus participantes, se notificará previamente al interesado y con su concurrencia o no, se leerá la correspondencia o el documento en forma reservada, informando del particular a la víctima y al procesado o su defensor público o privado. A falta de los sujetos procesales la diligencia se hará ante dos testigos. Todos los intervinientes jurarán guardar reserva[28].

4. Si la correspondencia u otros documentos están relacionados con la infracción que se investiga, se los agregará al expediente fiscal después de rubricados; caso contrario, se los devolverá al lugar de donde son tomados o al interesado[28].

5. Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará el desciframiento por peritos en criptografía o su traducción[28].

3.22. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS

La presente ley tiene como objeto regular y sancionar las infracciones que se atribuyen a lo relacionado con los sistemas de información, redes electrónicas e internet[29].

Art. 5.- Confidencialidad y reserva: Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada 25 conforme a lo dispuesto en esta ley y demás normas que rigen la materia [29].

Art. 8.- Conservación de los mensajes de datos: Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. Que la información que contenga sea accesible para su posterior consulta;

b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley[29].

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo[29].

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores[29].

Art. 10. - Procedencia e identidad de un mensaje de datos: Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para

actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje[29].

En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado[29].

Art. 52.- Medios de prueba: Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil[29].

Art. 55.- Valoración de la prueba: La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos[29].

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas[29].

3.22. DELITOS INFORMÁTICOS

En base a las observaciones anteriores, los delitos informáticos se pueden definir como es ilegal e inmoral en todos los aspectos Equipos de tecnología informática, red de datos y datos informáticos, cuando se trate de autores y víctimas.

3.22.1. Tipos de delitos informáticos

Tabla 7. Tipos de delitos informáticos [30].

TIPOS DE DELITOS	
NOMBRE	**SENTENCIA**
Pornografía infantil	De trece a dieciséis años de prisión.
Violación del derecho a la intimidad	de uno a tres años de prisión
Revelación ilegal de información de bases de datos	de uno a tres años de prisión
Interceptación de comunicaciones	de tres a cinco años de prisión
Pharming y Phishing	de tres a cinco años de prisión
Fraude informático	de tres a cinco años de prisión
Ataque a la integridad de sistemas informáticos	de tres a cinco años de prisión
Delitos contra la información pública reservada legalmente	de tres a cinco años de prisión
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	de tres a cinco años de prisión

4. MATERIALES Y MÉTODOS

4.1. TIPOS DE INVESTIGACIÓN

4.1.1. Investigación Exploratoria

Se ha realizado la investigación exploratoria, la que permitió plantear el problema de la investigación y donde se evidencio el desconocimiento del Sistema Operativo Tsurugi y sus herramientas para el análisis de dispositivos móviles en la obtención y verificación de pruebas digitales de los dispositivos móviles en la Oficina Técnica de la Unidad Judicial de Violencia. Así también la utilización de la investigación exploratoria nos ayudó a plantear la hipótesis.

4.1.2. Investigación Explicativa

Se ha optado por la Investigación explicativa debido a que permite familiarizarse con la situación del problema, identificando las variables más importantes y así plantear una hipótesis con el fin obtener de manera rápida ideas y conocimientos de la situación problemática u objeto de estudio. Por otro lado, la investigación explicativa nos permitió saber cómo funcionan las herramientas del Sistema Operativo Tsurugi.

4.1.3. Investigación Bibliográfica

Se aplicó la investigación bibliográfica debido a que se necesitó recolectar, recopilar y seleccionar información de distintas fuentes que sean de aportes en la realización del proyecto cómo por ejemplo el análisis de bibliografías, tesis, modelos, investigaciones, revistas científicas, artículos, libros, desarrollados para profundizar guías con relación al análisis de la investigación, con el fin de, dar un valor agregado al tema tratado, se profundiza el estudio de las leyes y normativas vigentes en nuestro país y los sistemas que se utilizan actualmente en los casos jurídicos que requieran una periscia informática.

4.1.4. Investigación descriptiva

La investigación descriptiva nos sirvió para dar a conocer que es el Sistema Operativo que investigamos, cuáles son sus herramientas más llamativas, como es su funcionamiento e indicar como se obtienen las evidencias en vivo.

4.2.MÉTODOS DE INVESTIGACIÓN

4.2.1. Experimental

Se implementó el método experimental con la justificación de enseñar cómo funciona las herramientas de Tsurugi junto a la presencia del equipo técnico de la oficina de violencia con esto se pudo ejercer una demostración en vivo de cómo utilizar y manipular el Triage de Android herramienta neta de Tsurugi obteniendo una respuesta rápida y favorable al equipo técnico que demostraron su apoyo a la investigación realizada.

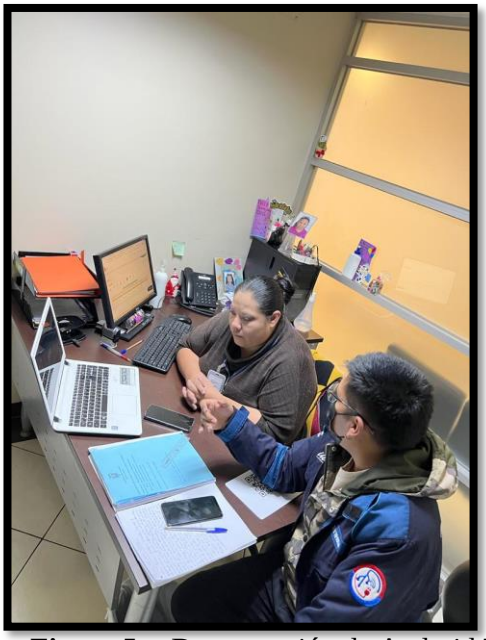


Figura 5. Demostración de Android Triage Tsurugi

4.3.TÉCNICAS DE INVESTIGACIÓN

4.3.1. Recopilación bibliográfica

Se utiliza este instrumento ya que nos permite obtener información valedera de documentos relacionados a la temática tratada.

4.3.2. Entrevista

Es un dialogo entre dos personas (entrevistado y entrevistador), el instrumento será un cuestionario estructurado el cual será elaborado por el investigador junto al tutor.

4.3.3. Encuestas

La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador.

4.4.Población y Muestra

Para conocer la población de la presente investigación se realizó un muestreo durante 1 mes en la oficina técnica de violencia donde se registraron 30 denuncias, lo que implicaba 30 dispositivos móviles a ser analizados, con esa referencia se procedió al cálculo de la muestra con una proyección de 30 casos mensuales.

4.5.Cálculo de la Muestra

Para el presente proyecto de investigación se seleccionó la fórmula de la muestra finita, tal como se detalla a continuación.

Tabla 8. Significado de los valores para el cálculo de la muestra

Parámetro	Significado	Valores
N	Tamaño de la población	30
Z	Nivel de confianza	1,960
Q	Probabilidad a favor	0,4
P	Probabilidad en contra	0,5
E	Error de muestra	0,3

$$n = \frac{N * Z_a^2 * p * q}{e^2 * (N-1) + Z_a^2 * p * q}$$

$$n = \frac{30 * 1.960_a^2 * 0.4 * 0.5}{0.3^2 * (30-1) + 1.960_a^2 * 0.4 * 0.5}$$

$$n = 27.77$$

Al ser la muestra igual a 27,77, se consideró que era mejor trabajar con la totalidad de la población o sea los 30.

5. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

5.1.1. Resultados de la Entrevista y Encuesta

5.1.2. Entrevista

El procedimiento que maneja el Equipo Técnico de la Oficina de la unidad Juridicial de Violencia la cual está compuesta por una psicóloga y una trabajadora social se realiza de la siguiente manera:

- Recepción de la disposición judicial
- Los peritos realizan un vaciado de expediente
- Agendamiento de la cita
- Entrevista psicosocial
- Aplicación de instrumentos de evaluación
- Recopilación de información,
- Triangulación y validación

Es aquí donde las profesionales recolectan la información que es proporcionada por las partes procesales, generalmente adicional a la entrevista las partes entregan información digital la cual terminan con la triangulación de la información y elaboración del informe.

Respectivamente a las respuestas emitidas por el Equipo Técnico de la Oficina de la unidad Juridicial de Violencia de Carcelén se ha aclarado el panorama del análisis de evidencias digitales, con ello se ha obtenido un resultado favorable a la implementación del sistema operativo Tsurugi el mismo que puede ser utilizado por los peritos para sus procesos de investigación.

Por siguiente las preguntas más relevantes en la entrevista realizada a las profesionales fueron:

Tabla 9. Pregunta 1 de la entrevista realizada

¿Cómo validan las evidencias digitales presentadas por los diferentes usuarios?	
Respuesta 1	**Respuesta 2**
Los usuarios envían capturas de pantallas, videos, audios los mismos que son entregados por medio de WhatsApp, USB o cd y es información que aparentemente no está adulterada.	Todo lo que nos envían receptamos de forma física y digital según presentan los usuarios.
Como resultado se pudo contemplar que al momento de la recepción de evidencias digitales la oficina técnica no tiene un rigor con los objetos que los usuarios presentan lo cual conlleva a que la gran mayoría de las evidencias presentadas no sean tomadas en el peritaje correspondiente.	

Tabla 10. Pregunta 2 de la entrevista

¿Tiene alguna dificultad al momento de utilizar los recursos tecnológicos?	
Respuesta 1	**Respuesta 2**
Si, porque muchas veces la evidencias no se abren, no se reproducen y desconocemos si han sido adulterada o no.	No.
Como resultado se conoce que una parte del equipo técnico de violencia sabe cómo utilizar los recursos tecnológicos al momento que los usuarios presentan las evidencias por otro lado se observa la falta de un informático forense al momento de tomar y dar validez a las evidencias presentadas.	

Fuente: Elaboración propia del investigador (2022)

Tabla 11. Pregunta 6 de la entrevista realizada

¿Qué tal le pareció Tsurugi?	
Respuesta 1	**Respuesta 2**
Me encanto es una herramienta ágil, accesible y de fácil uso al momento de ejecutar los diferentes momentos que se la requiera.	Muy interesante una herramienta optima y fácil de manipular.
Como resultado se obtuvo una respuesta favorable a las herramientas del sistema Tsurugi presentada a la oficina técnica de violencia claro con una demostración del funcionamiento de las mismas con ello la respuesta y apoyo a las herramientas presentadas.	

Fuente: Elaboración propia del investigador (2022)

Pregunta 7 de la entrevista realizada

Puede comentar sobre factores positivos que llevarían sus distintos peritajes con la herramienta Tsurugi	
Respuesta 1	**Respuesta 2**
Se valida la información en corto tiempo disminuyendo los tiempos procesales. Permite ampliar las investigaciones y tomar en cuenta las pruebas presentadas por los usuarios.	Es una herramienta fácil, creíble, rápida y aplicable en estos casos
Como resultado se obtiene una respuesta clara como la esperada “el equipo técnico sustenta que es fácil de usar y lo hace en un menor tiempo que es vital en este tipo de peritajes” muchas cualidades hacen que el equipo técnico quede sorprendido por la funcionalidad del Tsurugi.	

Fuente: Elaboración propia del investigador (2022)

5.1.3. Análisis e Interpretación Encuesta

¿Usted utiliza un dispositivo móvil?

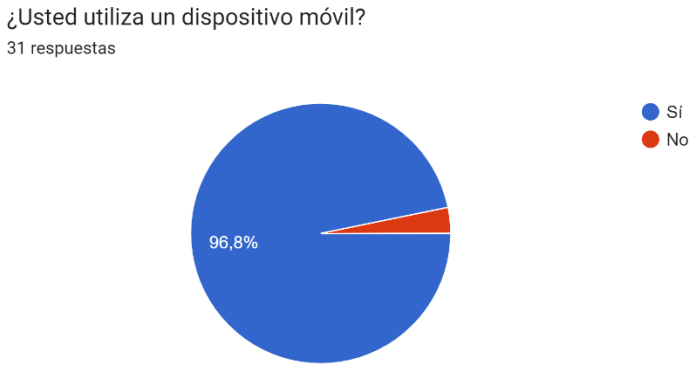


Figura 6. Uso de dispositivo móvil

Fuente: Elaboración propia del investigador (2022)

Los resultados obtenidos por esta grafica indican que la mayoría de empleados y usuarios de la oficina Técnica de violencia si utilizan un dispositivo móvil, ya que representa el 96.8% de las personas encuestadas, el otro porcentaje dice no utilizar un dispositivo móvil con un 3.2.

Como resultado tenemos que en la oficina técnica de violencia "Carcelén" la mayor parte de encuestados utilizan los dispositivos móviles, pero una persona nos informó que no le gustan los dispositivos móviles ya que expreso que son llamativos para que las personas sean víctimas de asaltos, con ello llegamos a la conclusión de que en ciertas personas existe un poco de brecha informática.

¿Qué dispositivo móvil utiliza?

Figura 7. Tipo de dispositivo móvil

Fuente: Elaboración propia del investigador (2022)

En esta gráfica se puede apreciar con mayor claridad cuantas personas prefieren el uso de los teléfonos inteligentes se puede ver que 29 personas de las 30 encuestadas, utilizan un celular con el 96,7% mientras que una persona encuestada manifestó que no posee un teléfono inteligente, sino que tiene uno para llamadas y por otro lado supo manifestar que utiliza más la computadora porque está familiarizada con ella, esta persona representa el 3.3% en la gráfica.

Como resultado tenemos que en la oficina técnica de violencia "Carcelén" la mayor parte de encuestados utilizan un teléfono inteligente como medio de comunicación principalmente sean estos por mensajería instantánea pero una persona nos informó que utiliza un dispositivo que solo sirve para llamadas y que utiliza la computadora para hacer sus asuntos informáticos con ello llegamos a la conclusión de que la mayoría de personas cuentan con un dispositivo móvil inteligente.

¿Qué sistema Operativo tiene su teléfono?

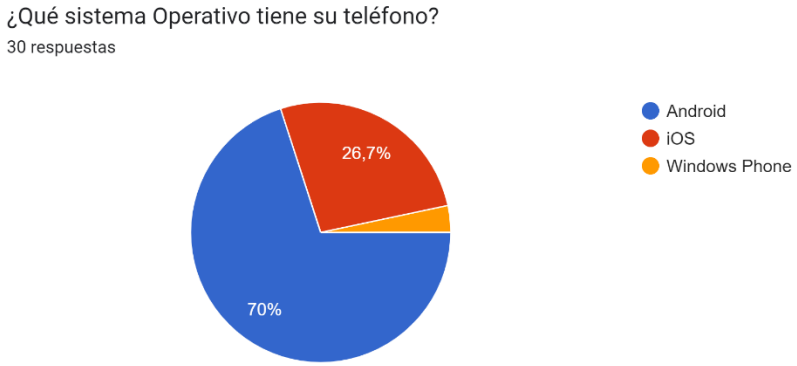


Figura 8. Sistemas operativos Móviles

Fuente: Elaboración propia del investigador (2022)

Esta gráfica indica que el sistema operativo Android es el más utilizado dentro de la oficina técnica que presenta un 70% que corresponde a 21 personas encuestadas, por otra parte, el segundo sistema operativo más utilizado es iOS que pertenece a los dispositivos IPhone con el 26.7% que corresponde a 8 personas encuestadas, por último, comprobamos que la persona que puso en la anterior pregunta que utilizaba una computadora establecida como sistema operativo Windows Phone con el 3.3%.

Como resultado se puede establecer que las herramientas elegidas van funcionar con toda normalidad basándonos en las encuestas tanto Android Triage como iOS Triage serán de gran utilidad para oficina técnica dado que la gran mayoría de usuarios presentarán sus dispositivos Android o iOS facilitando aún más el trabajo del análisis de los dispositivos y validando sus evidencias presentadas.

¿Qué aplicaciones utiliza?

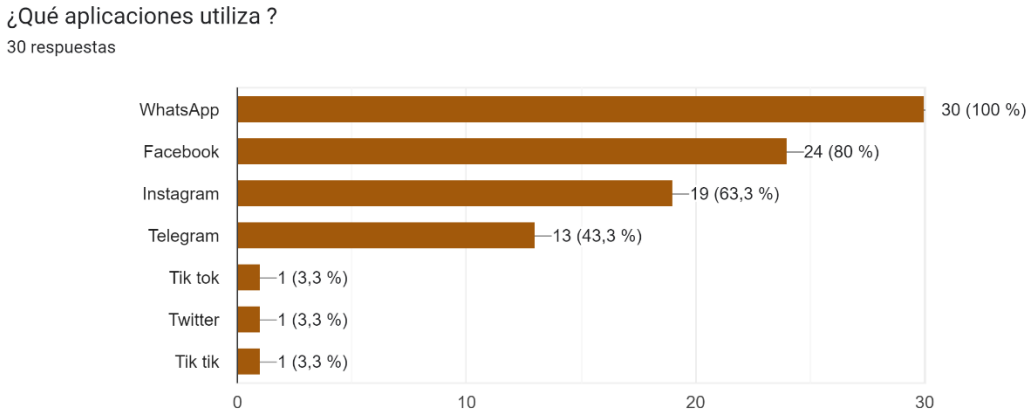


Figura 9. Aplicaciones móviles

Fuente: Elaboración propia del investigador (2022)

La gráfica representa que porcentaje de aplicaciones utilizan en la oficina técnica obteniendo en primer lugar WhatsApp con un 100% lo que representa a las 30 personas encuestadas, en segundo lugar Facebook tenemos con un 80% lo que representa a 24 personas encuestas, tercer lugar Instagram con 63.3% que representa a 19 personas encuestadas, cuarto lugar a Telegram con 43.3% que representa a 13 personas de las 30 encuestadas por ultimo con la respuesta que agregar otra aplicación obtuvimos un 9.9% lo que representa a 3 personas que utilizan Tik Tok, lo cual nos lleva a saber que la mayoría de usuarios presentan evidencias de WhatsApp a la oficina técnica de violencia lo cual las herramientas que se eligieron serán utilizadas de una forma rápida para la validación de las mismas.

Como resultado se puede establecer que la app de WhatsApp es de gran influencia en la oficina técnica para los casos que se presente alguna evidencia de esta aplicación el sistema Tsurugi tiene muchas herramientas para asegurar los mensajes y dar validez a los mismos.

¿Conoce a cerca del análisis forense de dispositivos móviles?

Figura 10. Conocimiento de análisis forense

Fuente: Elaboración propia del investigador (2022)

En está gráfica podemos observar que dentro del 73.3% de las personas encuestadas 22 no conocen sobre el análisis forense de dispositivos móviles ya que nunca han tenido un acercamiento a criminalística, mientras que el 26.7% que corresponde a 8 personas encuestadas conocen acerca del análisis forense se pudo conversar que la gran mayoría de ellas presentaron las denuncias a cerca de estafas en la cuarentena por lo que conocen un poco sobre la materia.

En consecuencia, se puede apreciar claramente que más de la mitad de encuestados tienen una breva tecnología sobre el tema forense mientras que el otro porcentaje de encuestados saben al menos los pasos que se debe seguir al momento de un análisis forense de dispositivos móviles.

¿Conoce que se puede recuperar sus datos del dispositivo móvil así sean borrados permanentemente?

Figura 11. Conocimiento de recuperación de datos

Fuente: Elaboración propia del investigador (2022)

La gráfica indica que 50% de las personas encuestadas si conocen que se puede recuperar alguna información borrada de sus dispositivos móviles mientras que el otro 50% no conocen o nunca han escuchado sobre recuperar alguna información borrada se puede determinar que alrededor de la mitad de usuarios alguna vez recuperaron algún dato con algún programa o pagaron por este trabajo de recuperación de dato.

En consecuencia, se puede apreciar que la mitad de los encuestados saben de alguna manera recuperar datos borrados por lo que se obtuvo una respuesta oportuna para establecer los modelos de adquisición de una imagen forense.

¿Conoce sobre algún programa que recupere sus datos de forma correcta?

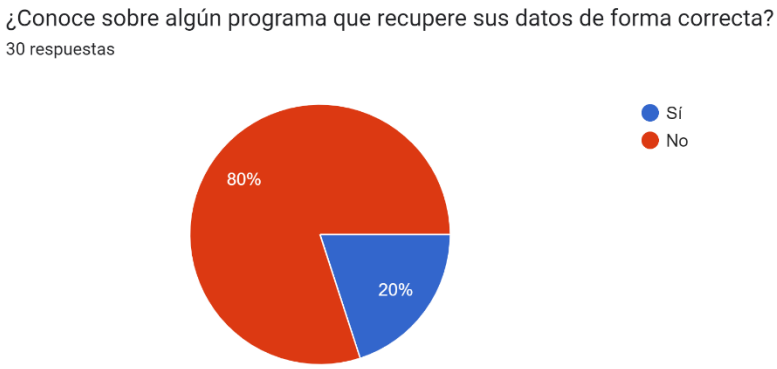


Figura 12. Programas conocidos de recuperación de datos

Fuente: Elaboración propia del investigador (2022)

Por un lado, el 80% de las personas encuestadas desconocen sobre algún programa para la recuperación, por otro lado, se conoce que cuando han recuperado la información de sus dispositivos han contratado personas extra y 20% de las personas encuestadas si conocen o han utilizado algún programa para recuperar sus datos.

En conclusión por los datos tabulados se puede ver con claridad que el panorama de análisis de los dispositivos móviles en este caso la recuperación de información o datos a veces es confundida por los encuestados con las herramientas de la nube ya que se puede crear una papelera y recuperar de allí los datos eliminados por otra parte los programas que nombraron los encuestados la mayoría no recupera en su totalidad los datos sino que solo recuperan partes de la información junto a ello tiene un costo elevado para recuperar todos los datos.

¿Ha presentado alguna evidencia digital?

Figura 13. Presentación de evidencia digital

Fuente: Elaboración propia del investigador (2022)

La gráfica indica que al 86.7% de las personas encuestadas nunca ha presentado alguna evidencia digital. En cuanto al aspecto de presentar evidencias digitales al 13.3% de las personas encuestadas si han presentado evidencias digitales y conocen cual es el procedimiento pertinente.

Como Resultado obtenemos la respuesta más concreta y esperada ya que en las preguntas anteriores se obtuvo un resultado algo similar por los casos que nos comentaban los usuarios que por casos de estafas conocen los pasas a seguir para el análisis y presentación de evidencias digitales.

¿Conoce sobre el proceso de extracción de evidencias?

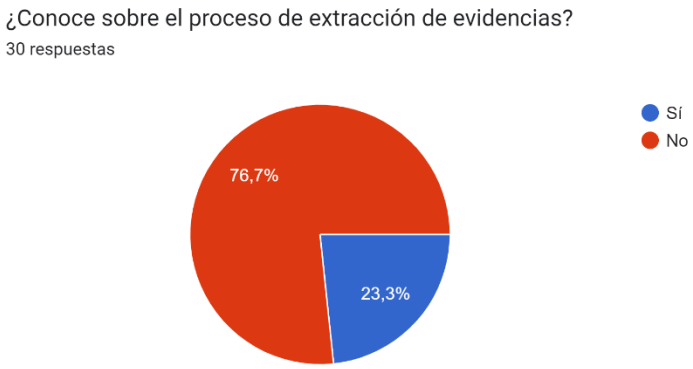


Figura 14. Proceso de extracción de evidencias

Fuente: Elaboración propia del investigador (2022)

El 76.7% afirma que no conocen sobre el proceso de extracción de evidencias dentro de la oficina técnica de violencia ya que no siempre las peritos establecen un proceso cuando entregan sus evidencias los usuarios mientras que el 23.3% de los encuestados nos indica que si conocen en una medida pequeña las diferentes etapas que conlleva la extracción de evidencias.

Como Resultado el proceso de extracción de evidencias es un tema que solo los profesionales dedicados al estudio de evidencias y más en el campo forense digital se debe conocer porque si te saltas una fase la evidencia receptada ya no tendrá valor lo cual solo pocos encuestados saben sobre las fases y procesos de extracción de evidencias.

¿Conoce que las pruebas presentadas de su dispositivo móvil pueden ser tomadas en cuenta dentro de su proceso legal?

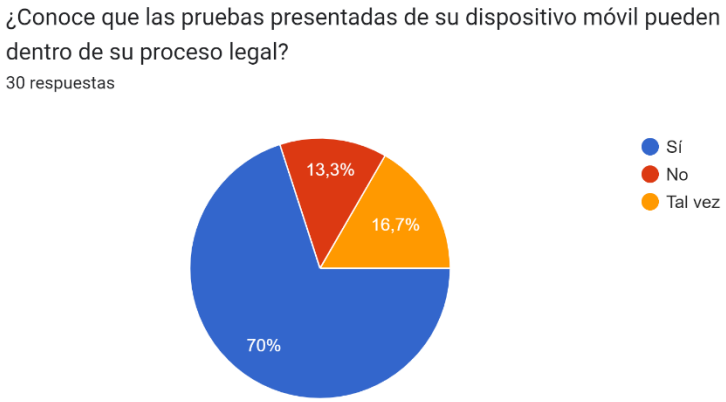


Figura 15. Proceso legal de pruebas digitales

Fuente: Elaboración propia del investigador (2022)

El 70% de las personas encuestadas conocen el panorama del proceso legal con un dispositivo móvil el cual tiene validez siempre y cuando un perito informático entregue su informe sobre las pruebas requerida, mientras que el 16.7% conocen que las evidencias digitales son parte de un proceso legal o que tiene validez en los procesos y tan solo el 13.3% no saben que las pruebas digitales pueden influir en un proceso legal.

En conclusión, la mayoría de personas dentro del área jurídica saben que toda evidencia prestada tendrá un valor agregado para dictar una sentencia del juez por ende se debe establecer una metodología y modelo para la extracción, validación y exposición de los informes creados por los peritos informáticos.

5.2.Herramientas de análisis forense de dispositivos móviles

Herramientas de análisis forense de dispositivos móviles

NOMBRE	DESCRIPCIÓN
AVILA FORESE	Herramienta forense móvil gratuita que le permite: • Whatsapp . transcripción de audio opus y trama de transcripción en CHATS HTML PARSER • Backup ADB • Parser Chats WhatsApp[31].
ANDRILLER CE	Es una utilidad de software con una colección de herramientas forenses para teléfonos inteligentes. Realiza solo lectura, forense sonido, adquisición no destructiva de dispositivos Android. Tiene características, como un potente descifrado de Lockscreen para Pattern, código PIN o contraseña; decodificadores personalizados para datos de aplicaciones de bases de datos de Android (algunos iOS y Windows de Apple) para decodificar comunicaciones. Extracción y descodificación de informes en formato HTML y Excel[32].
MAGNET ACQUIRE	Combina una interfaz de usuario intuitiva con extracciones confiables y rápidas, brindándole los datos de manera rápida y sencilla. Además de eso, la calidad de los datos que obtendrá se maximizará y el registro de actividad y la documentación le permitirán comprender qué métodos se utilizaron[33].
ANDROID TRIAGE	Un script bash que automatiza muchas operaciones necesarias para recopilar información del dispositivo, uno de los puntos clave en este proceso es la adquisición , donde extraemos una copia de los datos almacenados en el dispositivo móvil[34].
iOSTRIAGE	Un Bash script para extraer datos de un dispositivo iOS "checkra1ned" El programa extraerá, procesará e informará (incluidas las diferencias) en la telemetría de dispositivos iOS y aplicaciones[35].

Fuente: Elaboración propia del investigador (2022)

5.3. SEGUIMIENTO DE LA METODOLOGÍA FORENSE

La metodología es aquella rama lógica que se encarga de realizar un estudio de diferentes métodos con la finalidad de llegar al conocimiento crítico y reflexivo que permita generar fundamentación de la ciencia y todo saber.

5.3.1. Metodología General Forense

Aunque no existe una metodología que sea única y universal en el análisis forense, a tener la documentación existente y tomando en consideración la normativa leal y los estándares vigentes a nivel internacional, se puede decir que existen una serie de fases o puntos importantes que se tiene que tomar en consideración para que el análisis forense sea adecuado y sirva como elemento probatorio ante un incidente, violación de derechos y caso flagrante[36].

Figura 16. Metodología General Forense

Fuente: Elaboración propia del investigador (2022)

5.3.2. Fases de la metodología General Forense

Tabla 12. Fases de la metodología general forense

FASE	DESCRIPCIÓN
1. Adquisición:	Obtener copias de la información sospechosa de ser relevante para el incidente. De esta forma, es necesario evitar modificar datos de cualquier tipo, copiando siempre uno a uno con las herramientas y equipos adecuados. Se recomienda la utilización de: • Guantes • Bolsas antiestáticas • Jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas como son los celulares.
2. Preservación:	Se debe garantizar que la información recopilada no será destruida o alterada. En otras palabras, no se debe realizar ningún análisis en una muestra confiscada, se debe copiar y realizar la pericia en esa copia Se recomienda: • El concepto de cadena de custodia (a excepción de utilizar el modelo Triage) • Acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra • Utilizar las técnicas de Hashes • No vale congelar ni fecha ni hora • Video de todo lo que hagamos

Fuente: Elaboración propia del investigador (2022)

Tabla 13. Fases de la metodología forense (Continuación)

FASE	DESCRIPCIÓN
3. Análisis:	Después de obtener y preservar la información, pasamos a la parte más complicada. Podría decirse que es la fase más técnica, utilizando hardware y software específicamente diseñados para el análisis forense. Existen métricas y métodos que ayudan a construir el trabajo de campo, pero puede haber muchas variaciones según las herramientas utilizadas y la habilidad y experiencia del analista. Se recomienda las herramientas: • Autopsy • Ftk • Win – X
4. Documentación:	Registre todas las acciones, si es posible, a medida que ocurren. Aquí, hemos sido claros a partir de nuestro análisis de lo sucedido y hemos tratado de centrarnos en las cuestiones importantes relacionadas con la causa. Debemos citar y adjuntar toda la información obtenida, establecer una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación.
5. Presentación:	Varios modelos se utilizan comúnmente para presentar este documento. Por un lado, se presenta un informe ejecutivo que muestra las características más importantes de manera resumida y ponderada en la investigación sin entrar en detalles técnicos. Este informe debe ser muy claro, preciso y conciso, sin incluir preguntas cuestionables.

5.3.3. Definición del modelo de análisis de dispositivos móviles

5.3.3.1. Modelo the computer forensics field triage process model (CFFTPM)

Se utiliza en investigaciones que, requieren resultados de manera inmediata porque se estudia los datos en el lugar de los hechos, lo que impide realizar un análisis detallado, la aplicación de este dependerá del caso que vaya a ser analizado por el perito utilizando las herramientas de análisis de dispositivos móviles.

Se ha optado por utilizar el modelo presentado ya que en la gran mayoría de evidencias presentadas hacia las profesionales de la oficina técnica; tanto la trabajadora social como la psicóloga receptan las mismas de manera empírica

Este modelo es de gran ayuda ya que se adapta de forma correcta con las herramientas que se utilizarán en el análisis de dispositivos móviles, por consecuencia los usuarios que tengas su evidencia podrán tener la confianza de que su dispositivo tendrá un gran valor jurídico al momento de la investigación y podrán solicitar al juez pertinente el procedimiento para su validación. Para consiguiente nos permitirá:

• Analizar y recopilar pruebas inmediatamente.

• Identificar víctimas en riesgo.

• Valorar la amenaza del infractor para las personas perjudicadas.

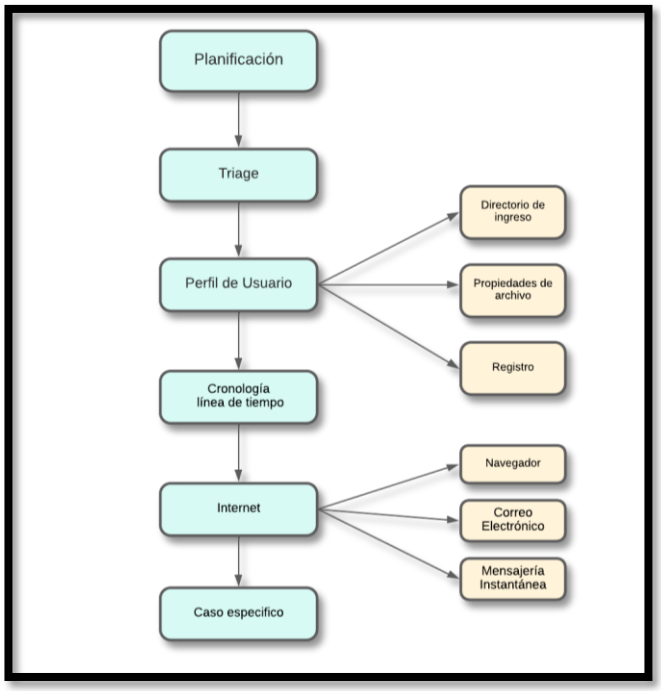


Figura 17. Fases del modelo (CFFTPM)

Fuente: Elaboración propia del investigador (2022)

5.3.3.2. Fases del modelo (CFFTPM)

Tabla 14. Fases del modelo (CFFTPM)

FASES	
NOMBRE	**DESCRIPCIÓN**
PLANIFICACIÓN	Al ser esta la primera etapa se realiza una matriz de cuantificación de los elementos del acontecimiento, que, permita precisar lo conocido y desconocido. Esta matriz contendrá los sucesos, los infractores, evidencia digital.
TRIAGE	Esta fase es una de las más importantes debido a que es fundamental para el modelo de proceso y junto con planificación es la base sobre la que se construyen las otras fases, se relacionan con resaltar las evidencias físicas, digitales que presenten los usuarios. Teniendo en cuenta que la evidencia digital podría tener un periodo corto de duración.

Fuente: Elaboración propia del investigador (2022)

Tabla 15. Fases del modelo (CFFTPM) (Continuación)

FASES	
NOMBRE	**DESCRIPCIÓN**
PERFIL DE USUARIO	Con la combinación de las fases anteriormente nombras y puestas en ejecución se realiza la reconstrucción de los acontecimientos y se establece una relación con el damnificado de las evidencias digitales que quiere presentar, lo cual conllevará a que llene una declaración de consentimiento informado donde expresa su voluntad para luego emplear las herramientas del sistema Tsurugi junto a ello el uso del dispositivo móvil no siempre será personal, por consiguiente se realizara un análisis de perfiles de usuarios que contenga el dispositivo móvil a analizar.
DIRECTORIO DE INICIO	En los sistemas operativos Microsoft Windows el directorio de inicio contiene varias carpetas como, por ejemplo; documentos, escritorio, imágenes, música, etc., para un usuario en específico, Esto sirve como medio probatorio del acto ilícito cometido por el o los sospechosos, cada usuario cuanta con una estructura de subdirectorios y solamente aquel que inicie sesión tendrá acceso a los archivos [12].
PROPIEDADES DE ARCHIVOS	Estas resultan muy útiles porque revelan información del usuario que lo creó, es decir, cada archivo que, se genere se guarda con los datos del usuario que inicio sesión y no se modifica a menos que, tenga derechos administrativos [12].
REGISTRO	El registro puede ser una trampa, causando el gasto innecesario de tiempo valioso, si el examinador no tiene una idea precisa de lo que están buscando exactamente dónde ir a encontrarlo. Por otro lado, un examinador experto con una visión clara de qué información quieren recuperar puede encontrar severa en nuestro caso será un factor determinante el tiempo porque gracias a los usuarios ingresaremos directamente a los datos que requieren una validez en el análisis forense.
LÍNEA DE TIEMPO	El alcance cronológico de la investigación puede ser definido por el caso inteligencia, En una investigación, la evidencia digital se define por su tiempo MAC Sin entrar en narración de los detalles de los tiempos MAC específicamente a cada sistema operativo, la siguiente: • Modificación se define por cuando se ha cambiado el contenido de un archivo • El tiempo de acceso se define por cuando se vio un archivo • Tiempo creado se define por cuando se creó un archivo
INTERNET	No en todos los casos, pero una pequeña parte del análisis de dispositivos móviles requerirán un examen de los artefactos asociados con actividad en Internet, como mensajería instantánea, correo electrónico y navegación web, El valor, el costo de tiempo y la criticidad del tiempo variarán ampliamente, dependiendo de circunstancias, incluidas las solicitudes específicas, tipo de actividad.

Tabla 16. Fases del modelo (CFFTPM) (Continuación)

FASES	
NOMBRE	**DESCRIPCIÓN**
NAVEGADOR	Es importante analizar la información contenida en el navegar como, por ejemplo, las cookies que, muestran el localizador uniforme de recursos (URL) del sitio visitado el cual, indica la fecha y hora de acceso, También, se encuentra evidencia en la cache de navegación, donde se descarga información como las imágenes de páginas visitadas, El archivo index.dat igualmente, contiene información relevante como; sitios visitados y correo electrónico basado en web [12].
CORREO ELECTRÓNICO	Artefactos de correo electrónico pueden ser de enorme valor probatorio, pero puede requerir una inversión costosa en tiempo Procedimientos para examinar el correo electrónico y extraer datos útiles suelen ser específicos para el cliente de correo electrónico en particular, y puede ser el tiempo consumo para implementar. Si la extracción de correo electrónico es exitosa, incluso un cursor cribado de todo el correo electrónico en el buzón de un sospechoso podría tomar muchas horas.
MENSAJERÍA INSTANTÁNEA	Las aplicaciones de mensajería generalmente guardan la información en sus servidores, por lo que, dificultan el acceso directo a los datos, lo que, complica la extracción de estos, en ciertas aplicaciones se mantiene registros de información que, son analizados por el investigador.
CASO ESPECÍFICO	La destreza del investigador juega un papel importante en cada una de las investigaciones puesto que, existe una variedad de casos a ser tratados y analizados de manera personalizada, el tiempo es uno de los factores primordiales en la investigación.

5.4. TABLAS COMPARATIVAS

5.4.1. Comparación de sistemas operativos forenses para dispositivos móviles

Tabla 17. Cuadro comparativo de sistemas operativos Forenses

NOMBRE	HERRAMIENTAS	VENTAJAS	DESVENTAJAS
Tsurugi Linux	Mas de 30 herramientas de análisis de dispositivos móviles.	Diferentes herramientas paras los sistemas operativos móviles más demandados en el mercado.	Es un sistema nuevo por lo cual no existe mucha información de las herramientas.

Fuente: Elaboración propia del investigador (2022)

Tabla 18. Cuadro comparativo de sistemas operativos Forenses (Continuación)

NOMBRE	HERRAMIENTAS	VENTAJAS	DESVENTAJAS
Kali Linux	6 herramientas de análisis de dispositivos móviles	Excelente para auditorias informáticas	Tiene muchas herramientas para hacking porque para eso fue creada por otro lado su limitado listado de herramientas forenses para análisis de dispositivos móviles
Santoku	12 herramientas de análisis de dispositivos móviles	Herramientas con las que poder analizar tanto la memoria interna como la ROM y la RAM en busca de información residente en dichas memorias.	No cuenta con herramientas para el sistema operativo Android.
Caine live forensic tool	5 herramientas de análisis de dispositivos móviles	Ofrece un entorno amigable que le proporciona al investigador forense toda la ayuda necesaria en el momento de resolver un caso.	Demora en descargar, requiere buenos conocimientos en el manejo de Linux.

5.4.2. Comparación de Herramientas forenses

Tabla 19. Comparación de herramientas Forenses

Nombre	OpenSource	Imagen Forense	Hash	Tiempo Backup
AndroidTriage	X	X	X	10 min a 20 min
IosTriage	X	X	X	10 min a 20 min
Andriller	X	X	X	30 minutos según la información del dispositivo.
Magnet acquire		X	X	50 minutos o más por backup de dispositivo.

Por siguiente se pondrá en acción Tsurugi Linux con la ayuda de las 2 herramientas AndroidTriage y Andriller por ser los que menor tiempo consumen para obtener una imagen forense y con ello empezar al análisis de la evidencia.

5.4.3. Comparación de modelos Forenses

Tabla 20. Comparación de fases de modelos forenses

FASES		
CFFTPM	**DFRWS**	**GCFIM**
➢ Planificación ➢ Triage ➢ Perfil de usuario ➢ Cronología de línea de tiempo ➢ Internet ➢ Caso especifico	➢ Identificación ➢ Preservación ➢ Recolección ➢ Inspección ➢ Análisis ➢ Presentación ➢ Decisión	➢ Pre-proceso ➢ Adquisición y preservación ➢ Análisis ➢ Presentación ➢ Post-proceso

Fuente: Elaboración propia del investigador (2022)

Como resultado para el caso práctico y de demostración se selecciona el modelo Triage visto que la mayoría de los casos los usuarios llegan puntualmente a la oficina técnica con las evidencias digitales lo cual es muy favorable para el modelo Triage por consecuencia que las evidencias se toman en el lugar de los hechos en este caso la oficina técnica.

5.5. APLICACIÓN DEL MODELO

En este punto se resaltará la utilización de software netamente dedicado al análisis forense de dispositivos móviles por consecuencia que junto al mismo se utilizará el modelo adecuado para que la adquisición de la información sea de una manera rápida y eficiente consecuencia de la elección de los instrumentos específicos de modo que se pondrá en práctica las técnicas mencionadas en un escenario de prueba el que permitirá un resultado esperado.

5.6.ESPACIO Y HERRAMIENTAS

Tabla 21. Herramientas implementadas en el caso practico

HERRAMIENTAS	
SOFTWARE	➢ Tsuguri Linux 2022.1
HERRAMIENTAS FORENSES	➢ AndroidTriage ➢ AndrillerGUI
RESPALDO DE DATOS	➢ AndroidTriage
CLAVES HASH	➢ Hash Tsurugi

Fuente: Elaboración propia del investigador (2022)

5.7.CASO DE PRUEBA

Cabe recalcar que el caso de prueba presentado fue parte de una demostración del sistema operativo Tsurugi hacia la oficina técnica de violencia “Carcelén” por lo cual se realizó en un campo de práctica controlado en presencia de la Psicóloga Dra. Teresa Almeida y la Lic. Patricia Díaz como evidencia se sustenta las imágenes de evidencia presentados en los gráficos.

5.7.1. Planificación

En este punto se hará llenar los formularios correspondientes a los usuarios que desean presentar sus evidencias digitales para si tener un consentimiento sobre los artefactos y datos que se obtendrán.

Como primer paso tendremos que llenar el formulario de recepción de dispositivo que se aprecia en la tabla 19.

Tabla 22. Características del dispositivo receptado

ESTADO Y CARACTERISTICAS DEL DISPOSITIVO				
Estado del dispositivo	**Encendido**	**X**	**Apagado**	
Protegido por algún tipo de clave	**SI**	**X**	**NO**	
EN CASO DE TENER PROTECCIÓN (TIPO)				
Patrón				
PIN	1971			
Contraseña				
Huella digital				
Reconocimiento Facial				
CARACTERÍSTICAS DEL DISPOSITIVO				
Marca del teléfono	SAMSUMG			
Modelo del teléfono	J2 PRIME			
Número de teléfono	0984943056			
Operadora del servicio	MOVISTAR			
Numero serial IMEI	358212080461584			
DOCUMENTACIÓN EXTRA DEL DISPOSITIVO				
	SI		**NO**	
Memorias extraíbles (micro sd)			**X**	
Cargador	**X**			
Códigos de acceso			**X**	
RECEPCIÓN				
Receptado por: Kevin Tipanta				
Revisado por: Kevin Tipanta				
Autorizado por: Dra. Teresa Almeida				

5.7.2. Triage

En esta fase se requiere hacer una tabla de importancia de datos por siguiente se informa al usuario que datos presentara de evidencia y donde están los mismo con el fin de precautelar los datos. Por siguiente se interviene con obtener un backup de los datos del teléfono.

Se requiere:

- El dispositivo desbloqueado
- El dispositivo en modo avión
- El dispositivo en modo desarrollador
- Activar depuración por USB
- Activar que no se bloque el dispositivo durante el backup

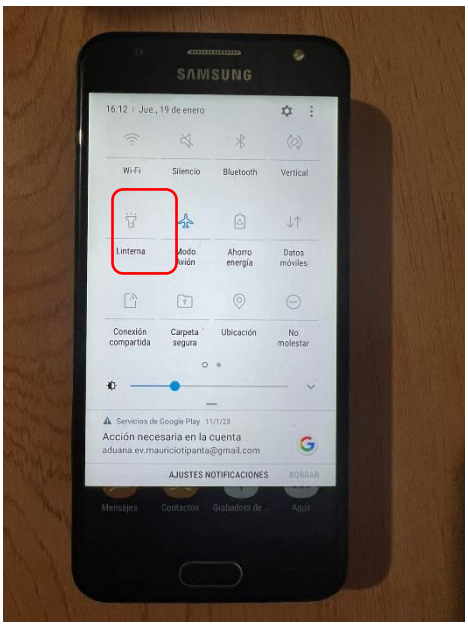


Figura 18. Dispositivo en modo avión

Fuente: Elaboración propia del investigador (2022)

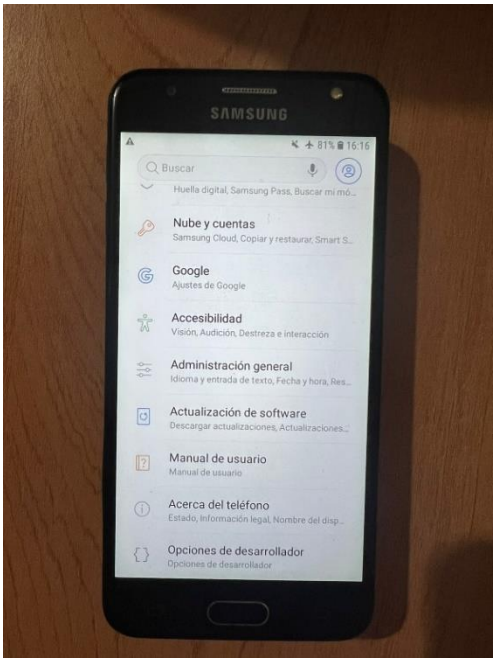


Figura 19. Dispositivo móvil en modo desarrollador (ADB)

Fuente: Elaboración propia del investigador (2022)

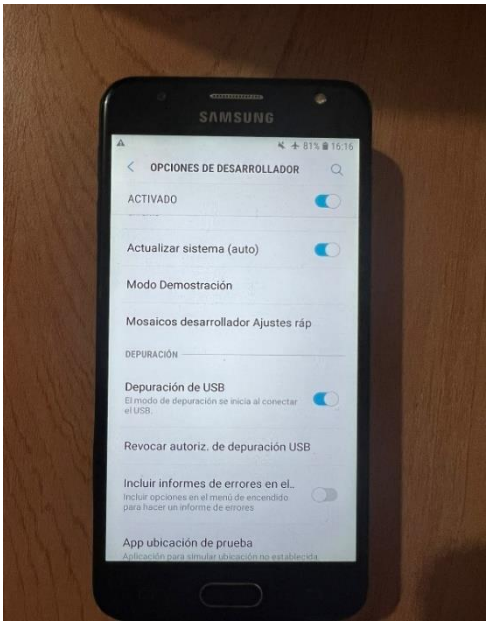


Figura 20. Modo depuración por USB del dispositivo

Fuente: Elaboración propia del investigador (2022)

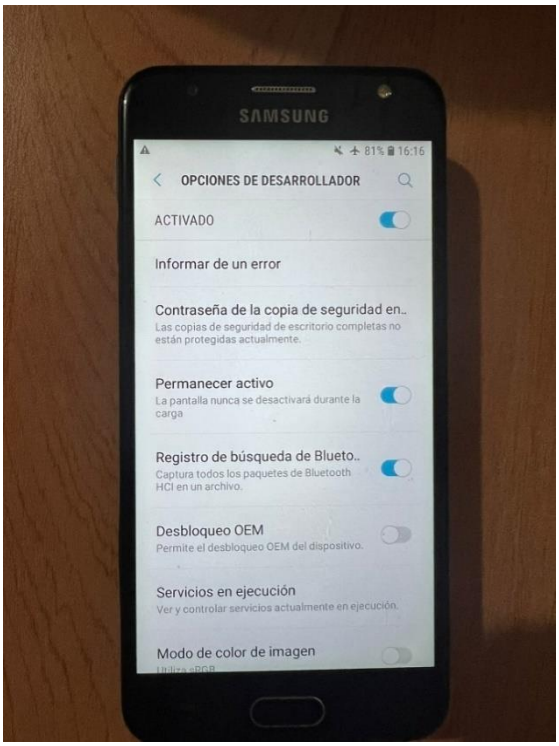


Figura 21. Activación del modo permanecer activo

Fuente: Elaboración propia del investigador (2022)

Siguiente paso debemos abrir nuestra máquina virtual para iniciar con la obtención de un backup de los datos requeridos por los usuarios:

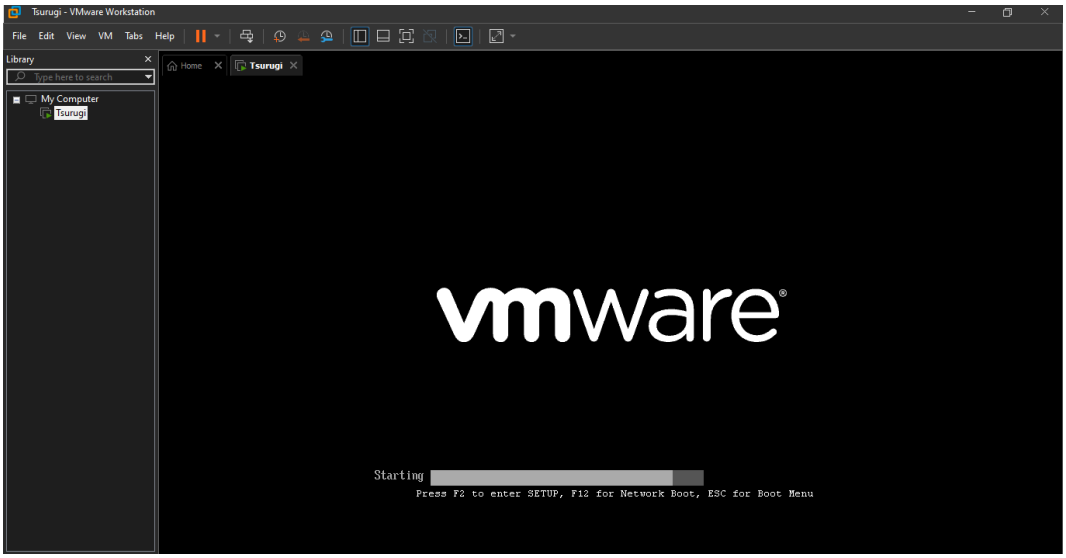


Figura 22. Iniciamos la máquina virtual

Fuente: Elaboración propia del investigador (2022)

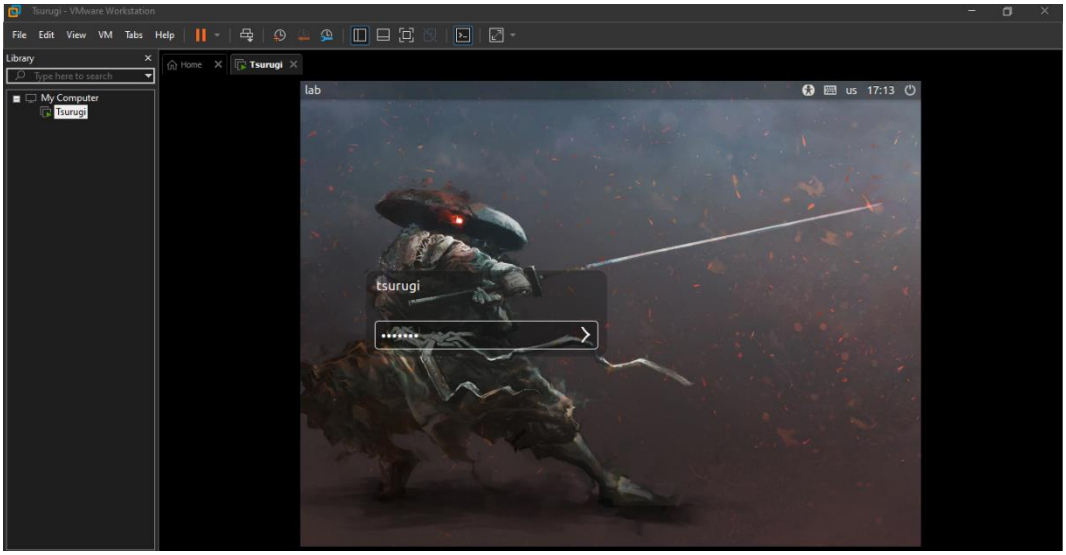


Figura 23. Inicio de Sesión de Tsurugi en vivo

Fuente: Elaboración propia del investigador (2022)

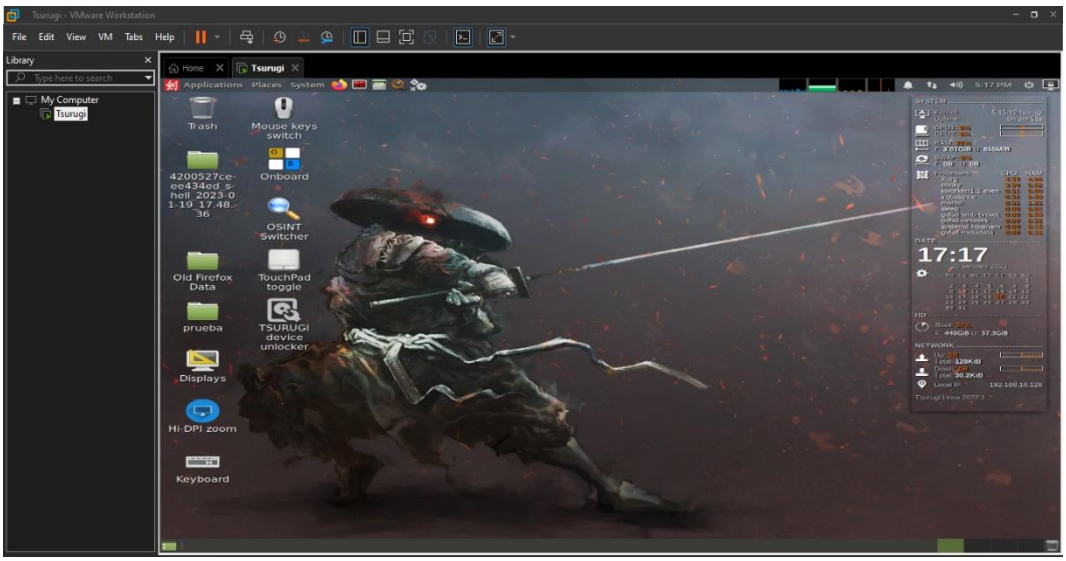


Figura 24. Pantalla principal de Tsurugi Linux

Fuente: Elaboración propia del investigador (2022)

Después de iniciar nuestra máquina virtual procedemos a conectar el dispositivo para el reconocimiento del Tsurugi, una particularidad porque elegir la herramienta VMware y no Virtual Box en sencillo ya que en VMware no requiere de bajar tantos drives para permitir la conexión de otros dispositivos a la máquina virtual mientras que VMware los reconoce inmediatamente.

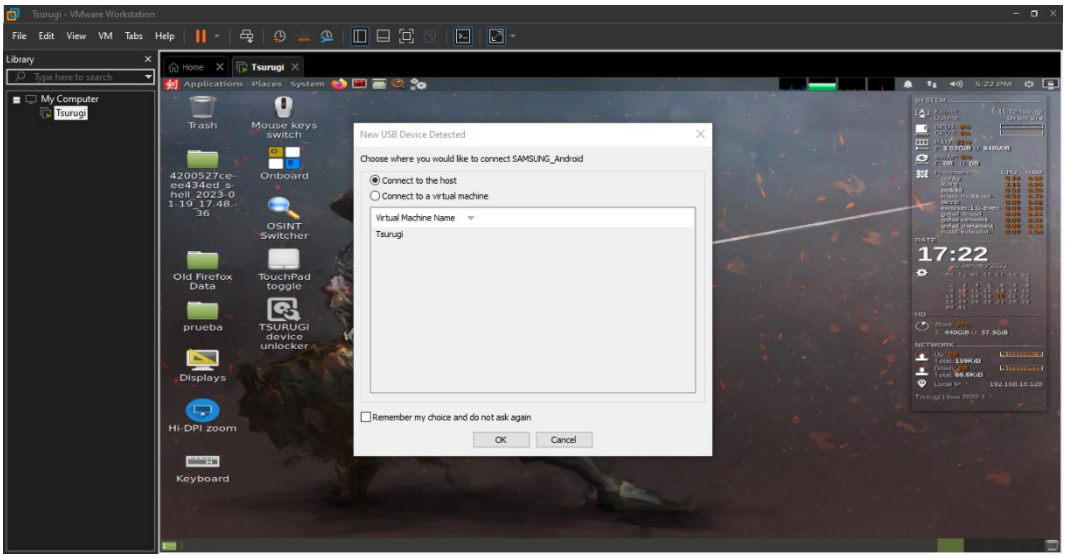


Figura 25. Reconocimiento inmediato del dispositivo por parte de Tsurugi

Fuente: Elaboración propia del investigador (2022)

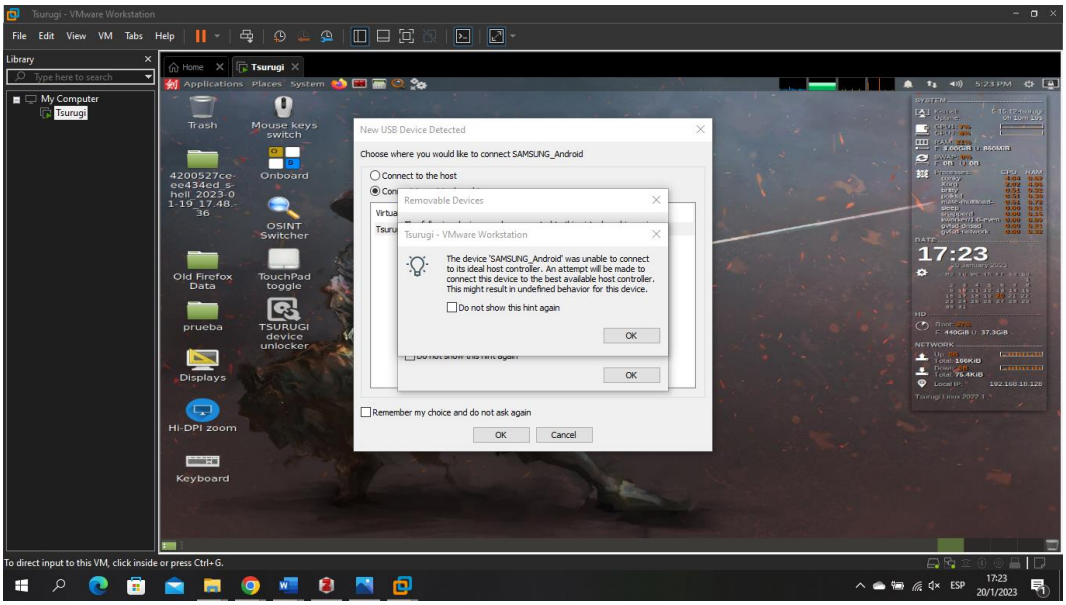


Figura 26. Mensaje de alerta por parte del sistema operativo

Fuente: Elaboración propia del investigador (2022)

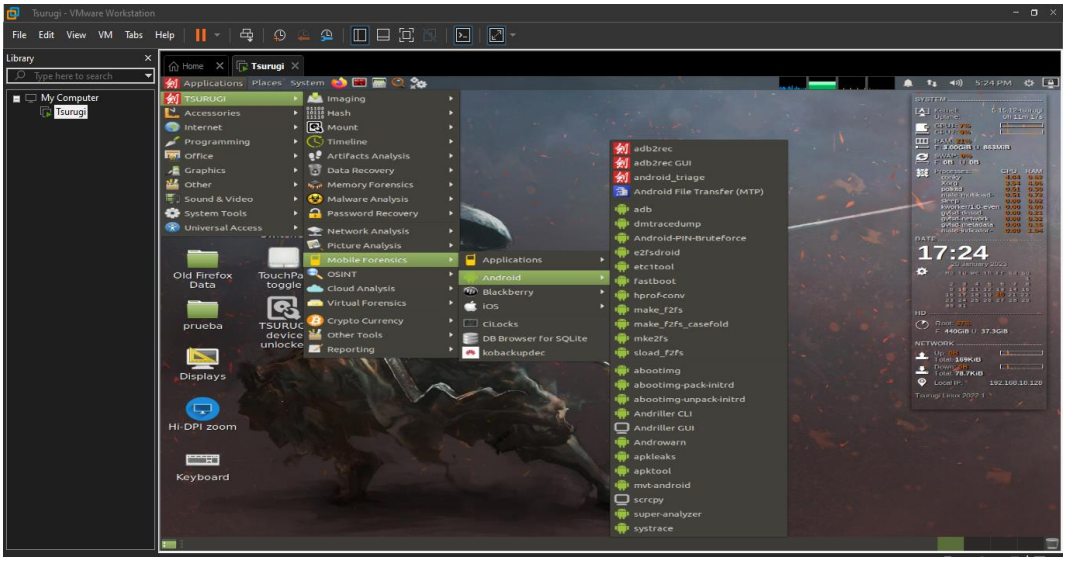


Figura 27. Herramientas de Tsurugi junto con el sistema operativo Android

Fuente: Elaboración propia del investigador (2022)

Acontinuacion procedemos a hacer backup del dispositivo utilizando la herramienta Android Triage:

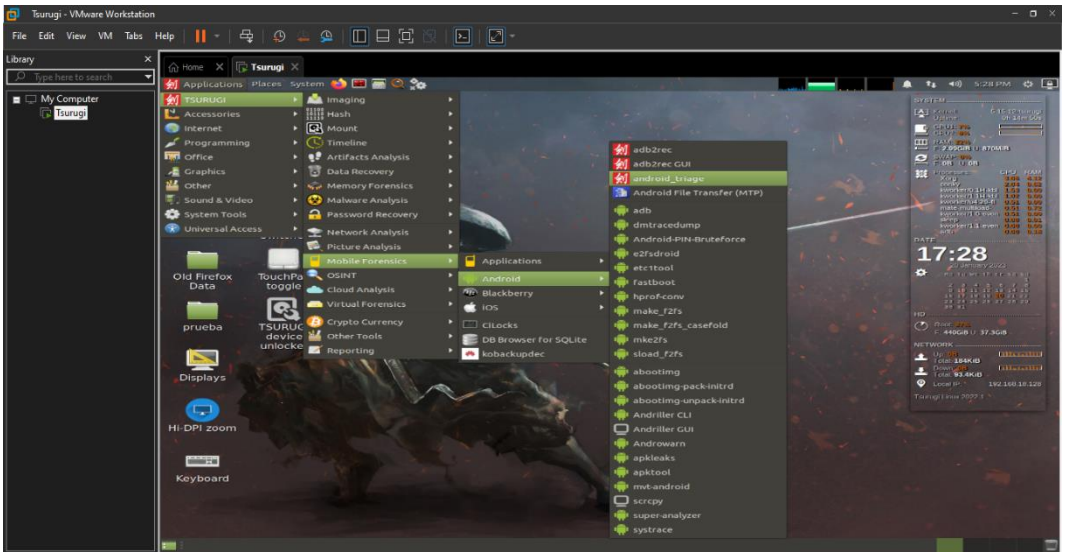


Figura 28. Abrimos la herramienta AndroidTriage

Fuente: Elaboración propia del investigador (2022)

A continuación, se presenta un mensaje de alerta en el dispositivo móvil el cual debemos aceptar:

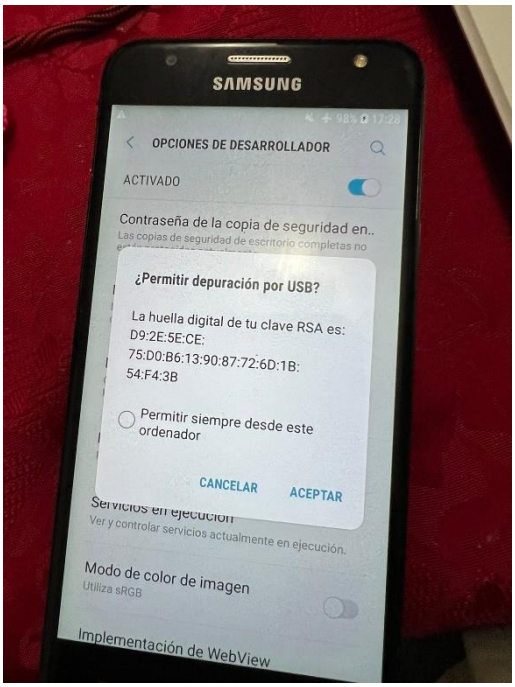


Figura 29. Mensaje de alerta por parte del dispositivo

Fuente: Elaboración propia del investigador (2022)

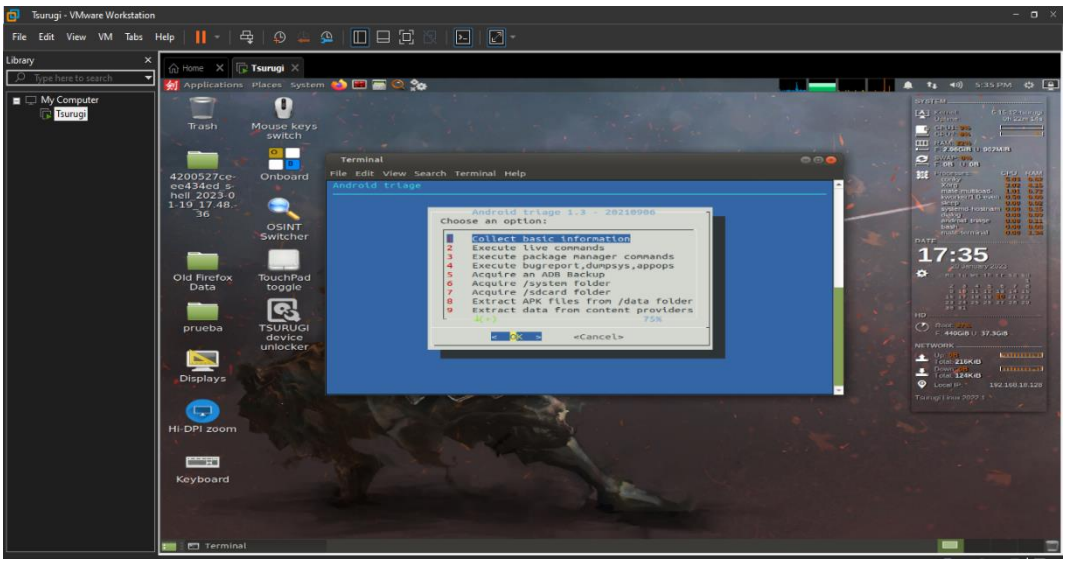


Figura 30. Interfaz gráfica del AndroidTriage

Fuente: Elaboración propia del investigador (2022)

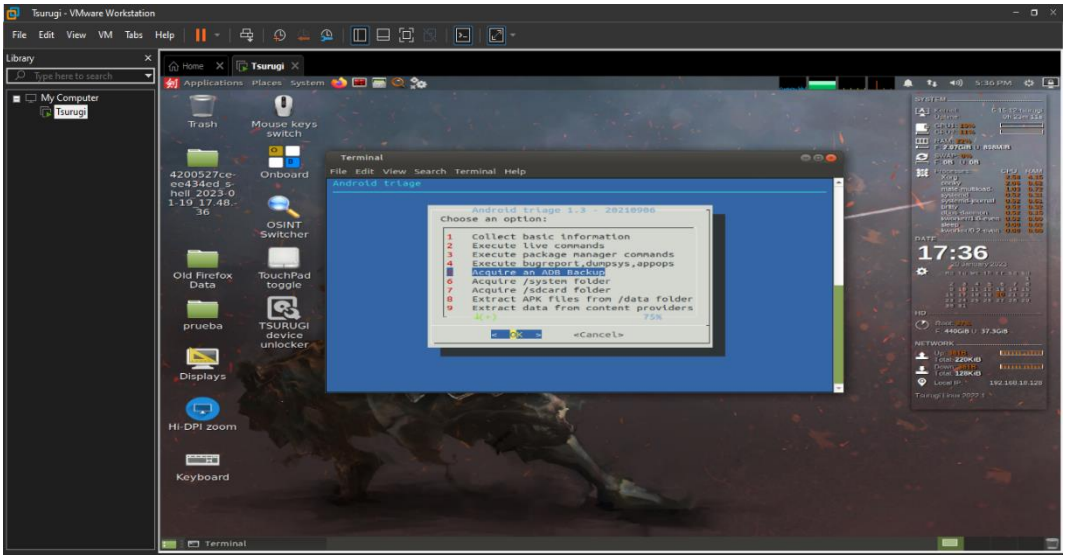


Figura 31. Seleccionamos la quinta opción (Arquire and ADB backup)

Fuente: Elaboración propia del investigador (2022)

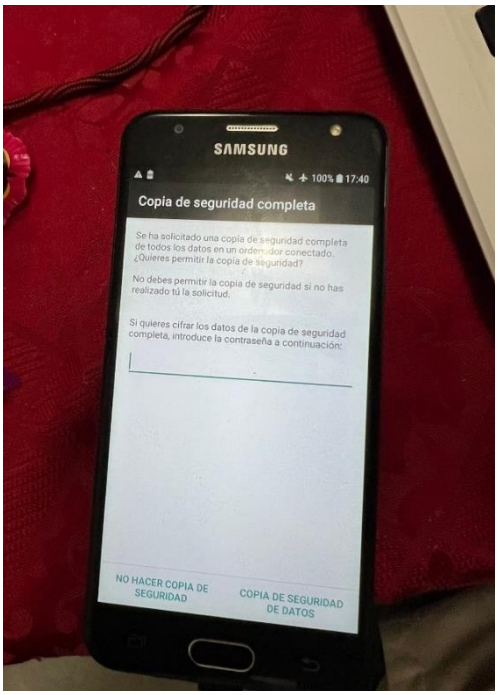


Figura 32. Mensaje de confirmación de copia de seguridad

Fuente: Elaboración propia del investigador (2022)

Este punto es muy importante consecuencia de este mismo nuestro primer backup se guardará en con el nombre de la fecha y hora que se está realizando el mismo:

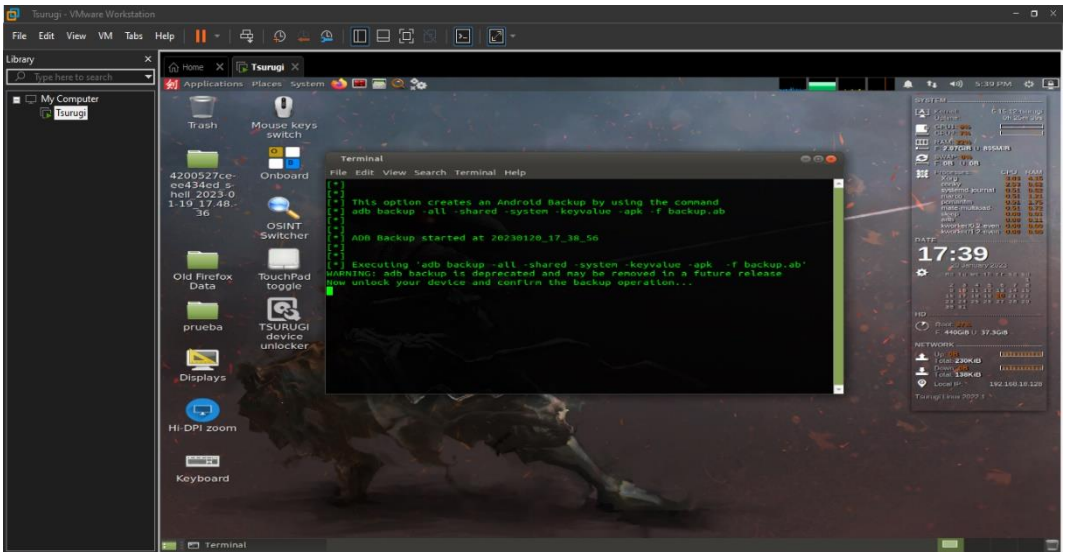


Figura 33. Inicia el backup de AndroidTriage

Fuente: Elaboración propia del investigador (2022)

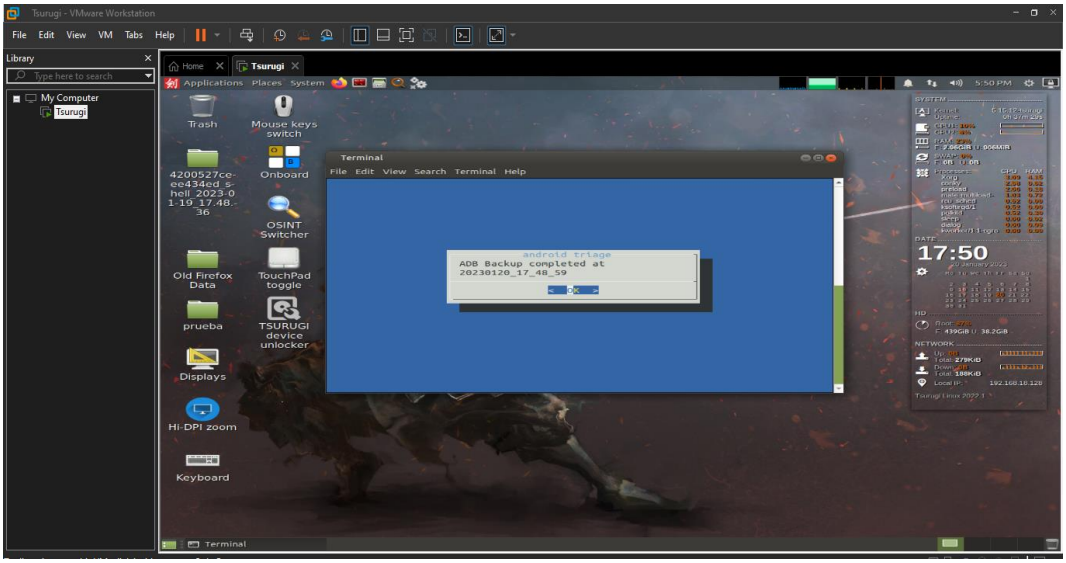


Figura 34. Backup completo por AndroidTriage

Fuente: Elaboración propia del investigador (2022)

Ingresamos a la carpeta /home/tsurugi/ y encontraremos nuestro backup

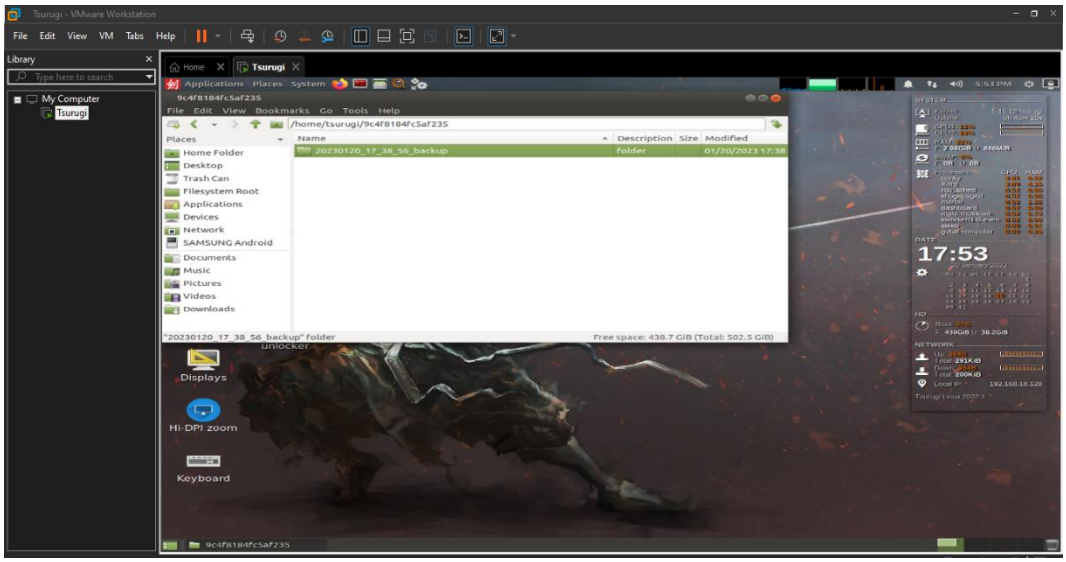


Figura 35. Backup localizado

Fuente: Elaboración propia del investigador (2022)

Obtendremos dos archivos los cuales deben tener un hash para cuidar la integridad de los datos acompañando al backup se utilizará un hash:

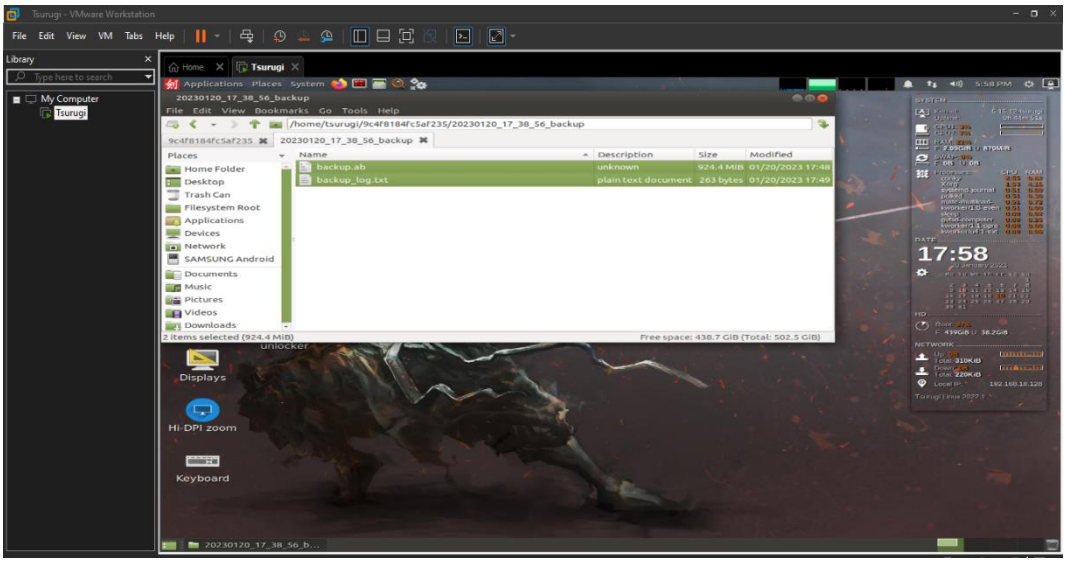


Figura 36. Obtención de dos archivos

Fuente: Elaboración propia del investigador (2022)

A continuación, crearemos una carpeta en el escritorio de Tsurugi para facilitar la creación del hash la carpeta se llamará evidencia1 y tendrá la siguiente ruta **/home/tsurugi/Desktop/evidencia1:**

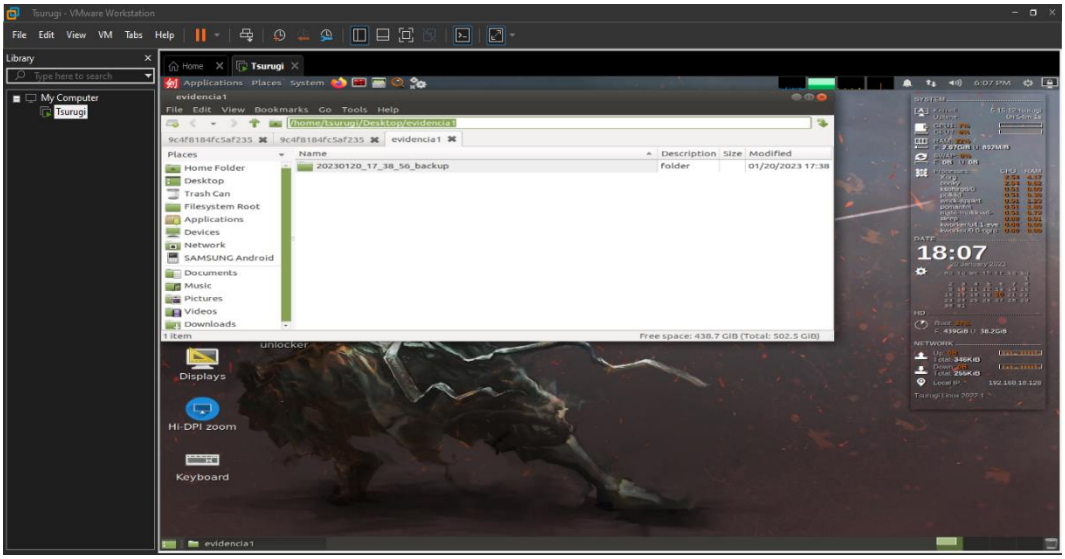


Figura 37. Creación de carpeta nueva con la carpeta del backup

Fuente: Elaboración propia del investigador (2022)

Se abre las herramientas de Tsurugi y se selecciona la opción de hash y la herramienta ssdeep:

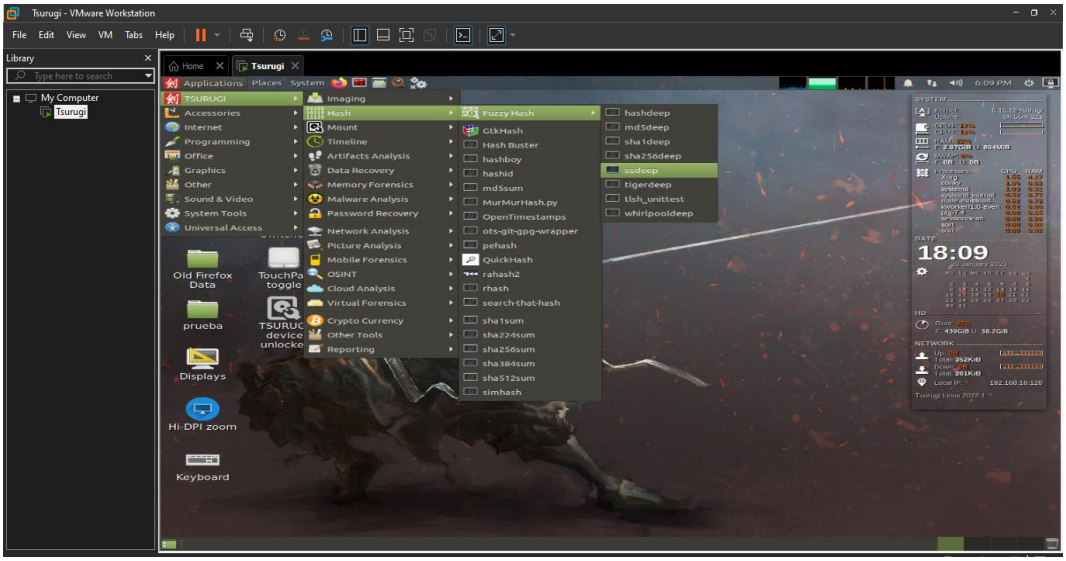


Figura 38. Selección de hash

Fuente: Elaboración propia del investigador (2022)

- Se ingresa el siguiente comando para ingresar a la carpeta creada
- **cd Desktop/evidencia1**
- siguiente de eso ingresamos un **ls** para ver los archivos que tenemos y verificar que sea el backup

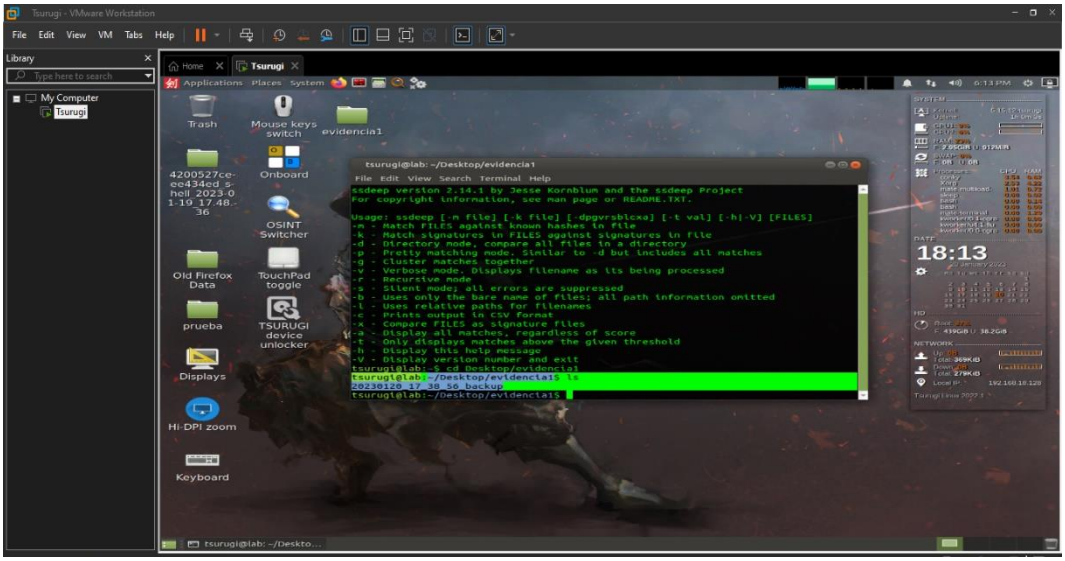


Figura 39. Ingresamos los comandos para acceder a la carpeta

Fuente: Elaboración propia del investigador (2022)

Para obtener un hash md5 procedemos a ingresar el siguiente código:

- **md5sum***

junto a ello para obtener en tipo txt ingresamos

- **md5sum* >hash.txt**

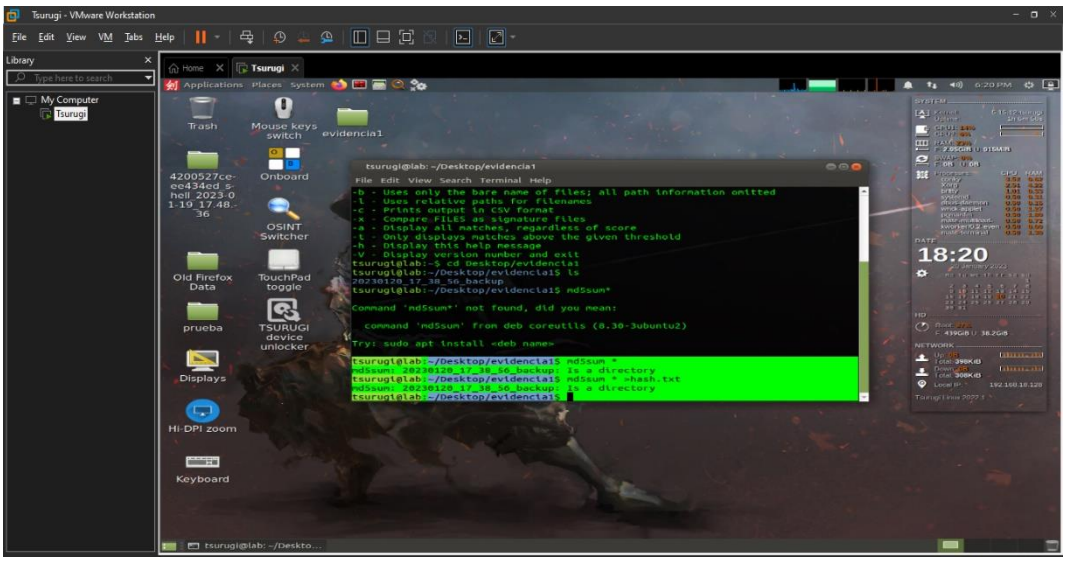


Figura 40. Creación del hash

Fuente: Elaboración propia del investigador (2022)

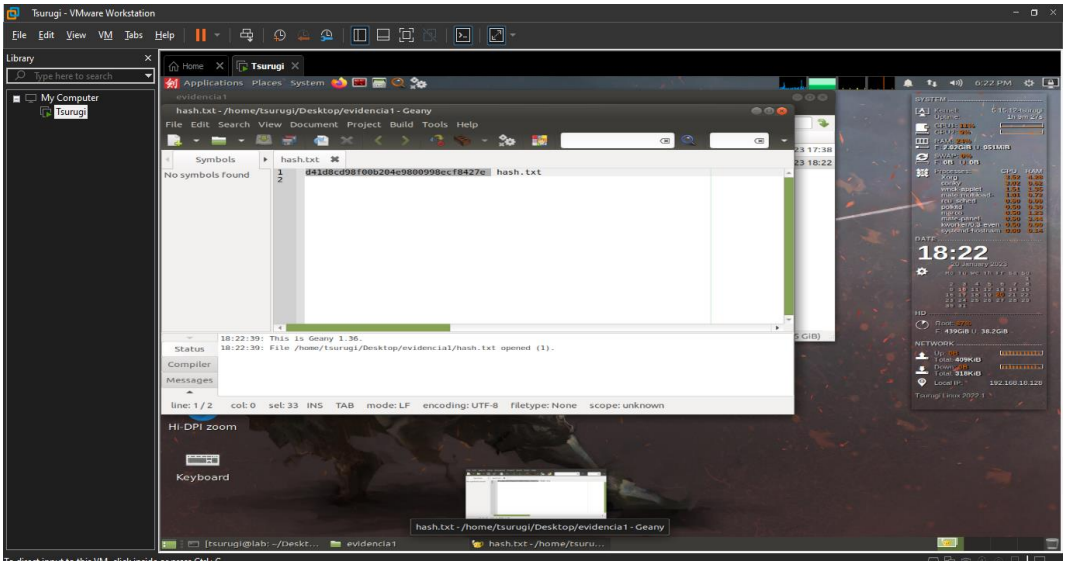


Figura 41. Obtención del hash en un txt

Fuente: Elaboración propia del investigador (2022)

5.7.3. Perfil de usuarios

En esta fase se procederá a establecer como primer paso se procede a pregunta a los usuarios si su dispositivo es propio o no, para establecer los parámetros para la obtención de base de datos de mensajes que serán de gran utilidad para el análisis forense. Se optará para realizar el segundo backup correspondiente pero esta vez se utilizará la herramienta Andriller ya que esta cuenta con un reporte HTML de las evidencias encontradas.

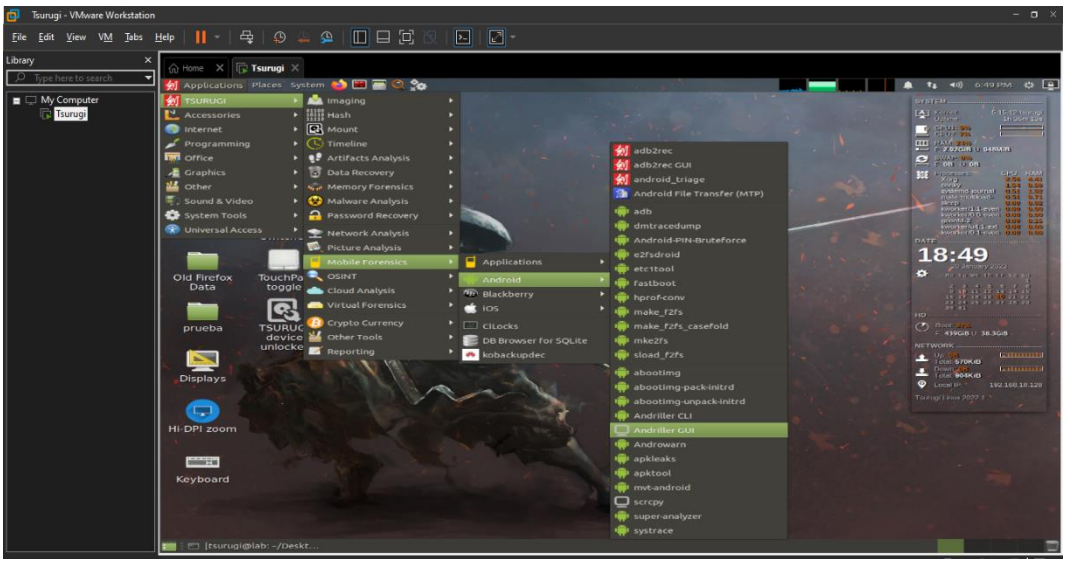


Figura 42. Selección de la herramienta andriller

Fuente: Elaboración propia del investigador (2022)

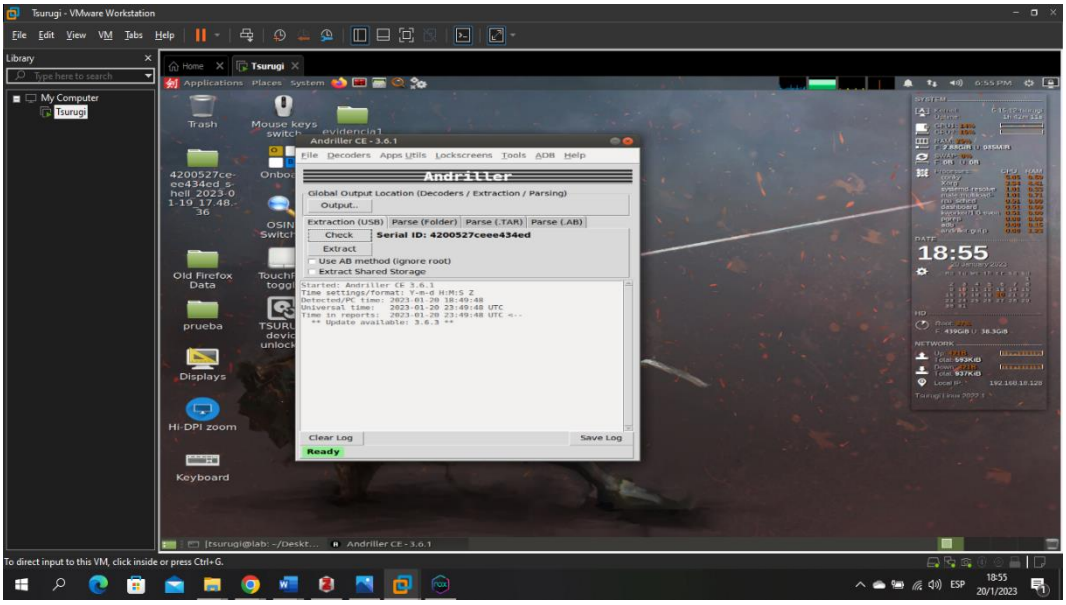


Figura 43. Interfaz gráfica de Andriller

Fuente: Elaboración propia del investigador (2022)

Procedemos a seleccionar:

- La ruta donde se guardará nuestro segundo backup
- Dar click en check y observar que se muestre un serial
- Seleccionar las 2 opciones motivo que se extraerá todos los datos que tenga el dispositivo.

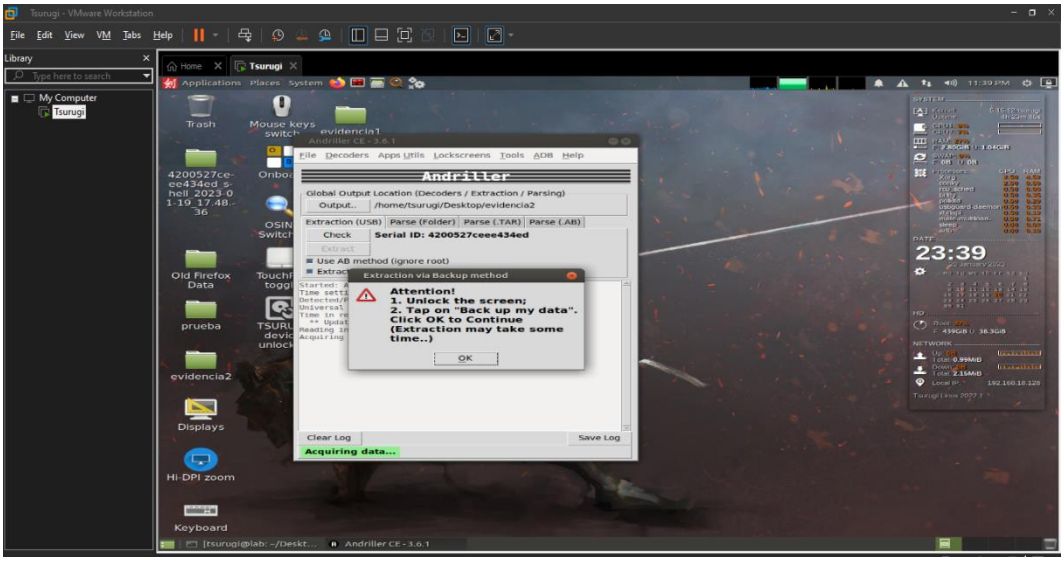


Figura 44. Mensaje de alerta de Andriller

Fuente: Elaboración propia del investigador (2022)

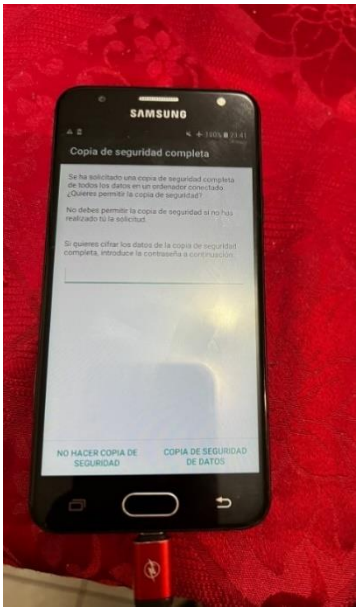


Figura 45. Mensaje de confirmación de copia de seguridad

Fuente: Elaboración propia del investigador (2022)

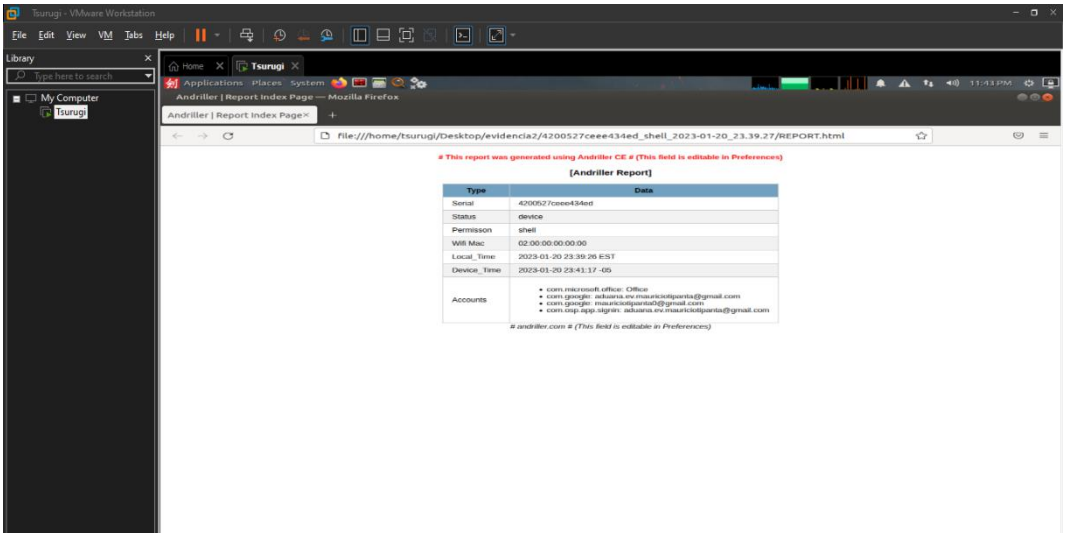


Figura 46. Reporte de Andriller para verificar que cuentas tiene el dispositivo móvil

Fuente: Elaboración propia del investigador (2022)

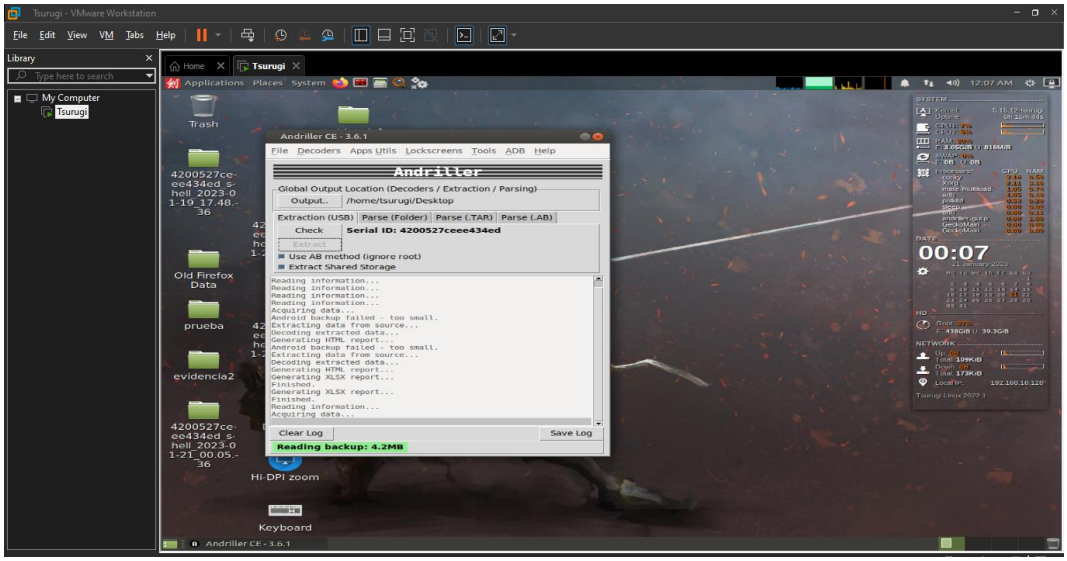


Figura 47. Empieza el backup con Andriller

Fuente: Elaboración propia del investigador (2022)

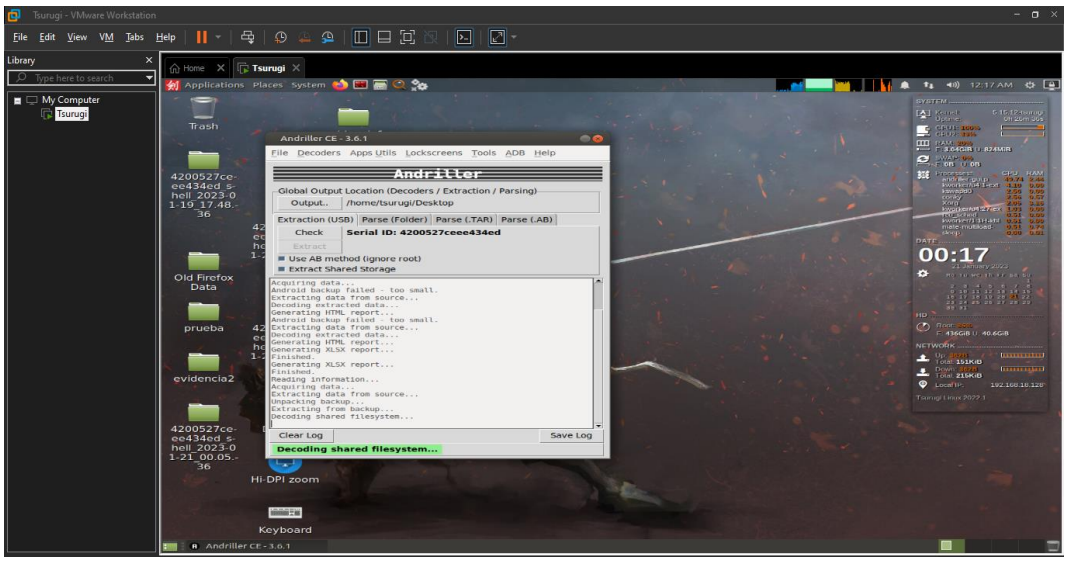


Figura 48. Backup completo por Andriller

Fuente: Elaboración propia del investigador (2022)

Por último, se tiene como evidencia un respaldo completo del dispositivo y con ello un hash md5:

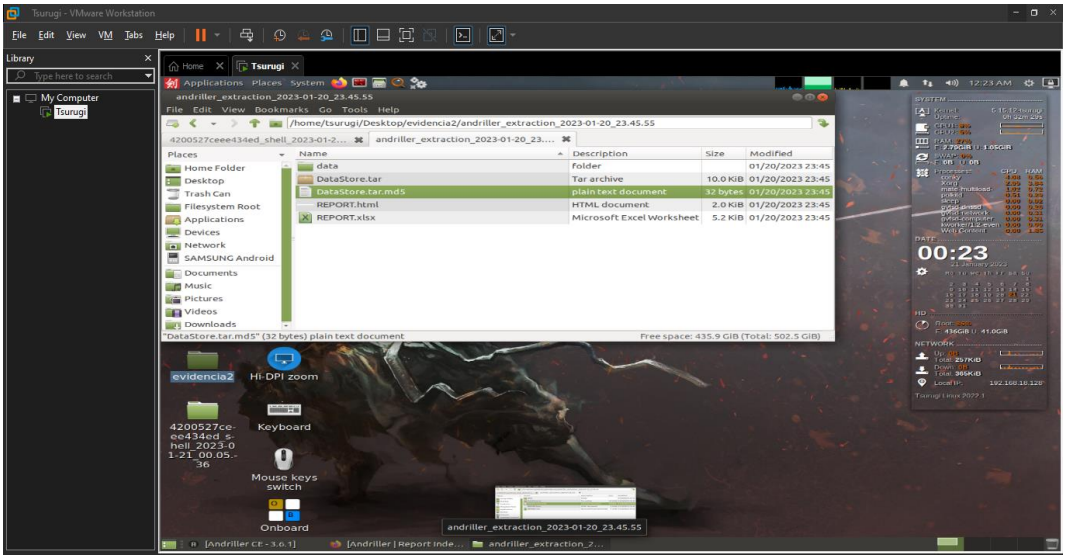


Figura 49. Carpeta donde se guardó el backup de Andriller

Fuente: Elaboración propia del investigador (2022)

5.7.4. Cronología

Tabla 23. Caso número 1 Android Triage

LÍNEA DE TIEMPO BACKUP	
Perito informático	Kevin Tipanta
Número de caso	001
Fecha	20/01/2023
Hora	17:35
Hash	d41d8cd98f00b204e9800998ecf8427e
Estado del respaldo	Satisfactorio
Herramienta utilizada	AndroidTriage y FuzzyHash ssdeep
Observaciones	Ninguna

Fuente: Elaboración propia del investigador (2022)

Tabla 24. Caso número 1.1 Andriller

LÍNEA DE TIEMPO BACKUP	
Perito informático	Kevin Tipanta
Número de caso	001.1
Fecha	20/01/2023
Hora	23:35
Hash	1276481102f218c981e0324180bafd9f
Estado del respaldo	Satisfactorio
Herramienta utilizada	Andriller, md5
Observaciones	Ninguna

Fuente: Elaboración propia del investigador (2022)

5.7.5. Internet

En esta fase es clave puesto que la gran mayoría de datos analizados aquí son de mensajería instantánea por ejemplo WhatsApp, Messenger entre los más reconocido también entran en el grupo los correos enviados, recibidos y spam.

Como es de conocimiento este caso fue de prueba y se evidencio el poder enorme que tienen las herramientas seleccionadas por motivos que se presenció por la oficina técnica de violencia se pudo rescatar los calendarios de Google que tiene conexión con las cuentas vinculadas del dispositivo puesto que el caso presentado fue una demostración en vivo se obtuvo una gran acogida al software Tsurugi con sus distintas herramientas.

5.7.6. Caso especifico

Se pudo obtener fechas registradas en la cuenta vinculada del dispositivo móvil como evidencia del análisis del segundo backup:

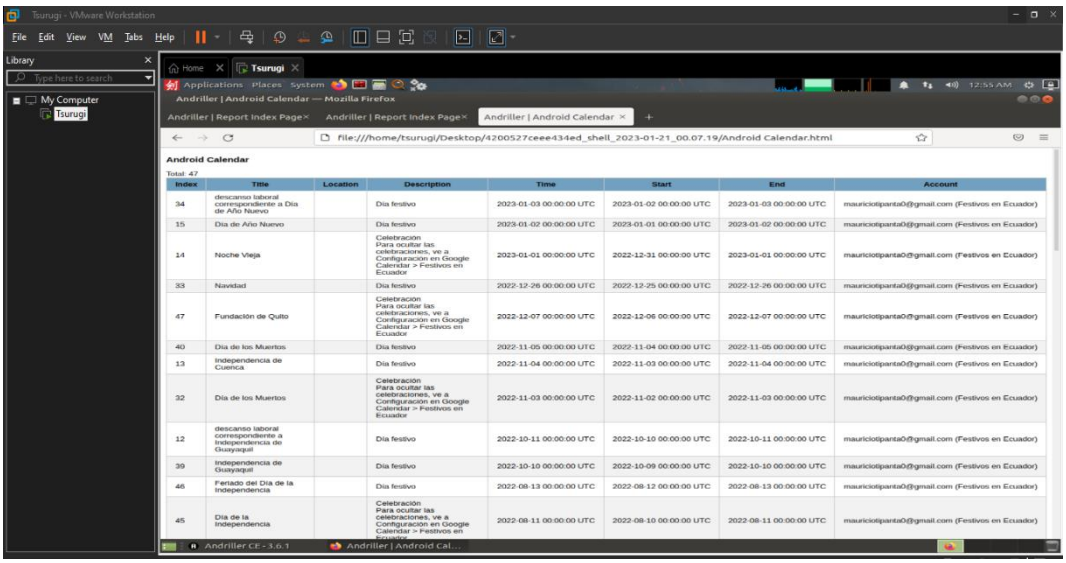


Figura 50. Evidencia obtenida por andriller

Fuente: Elaboración propia del investigador (2022)

En consecuencia, de las herramientas investigadas, presentadas y puestas en acción en un caso de prueba se concluye que las herramientas de análisis forense de dispositivos móviles seleccionadas junto al modelo de proceso de Triage de campo forense cibernético o conoció por sus siglas (CFFTPM), se comprueba la validez del modelo propuesto este es flexible en los diversos casos de investigación y aplicable más en los dispositivos móviles con sistema operativo Android, consecuencia que la mayoría de los usuarios cuentan con sistemas operativos Android lo cual lleva que el modelo propuesto este al nivel de las peticiones de la

oficina técnica siendo el mismo de gran ayuda ya que es un modelo que se implementa junto en el lugar de los hecho facilitando así el trámite clásico del análisis de dispositivos móviles.

Figura 51. Demostración de Android Triage a la oficina Técnica

Fuente: Elaboración propia del investigador (2022)

Figura 52. Demostración a la Psicóloga el funcionamiento del sistema

Fuente: Elaboración propia del investigador (2022)

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- El modelo de análisis forense informático fue desarrollado de acuerdo a las necesidades de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia". y basándose en las herramientas AndroidTriage, iOSTriage y Andriller del Sistemas Operativo Tsurugi mismas que aplican los estándares internacionales en cuanto a seguridad informática y recolección de evidencia digital.

- La fundamentación teórica permitió proponer un marco de trabajo que podrá ser utilizada para realizar investigaciones forenses a dispositivos móviles debido a que la misma tiene una alta posibilidad de ser aceptada en una corte judicial debido a que fue desarrollada bajo directrices proporcionadas por peritos informáticos de la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia". El presente Marco de trabajo contiene referencias hacia artículos presentes en el Código Orgánico Integral Penal (COIP) vigente en el Ecuador, de esta forma se trabaja bajo el marco legal Ecuatoriano, haciendo que la metodología sea más funcional no solo en el ámbito técnico sino que ante una corte judicial este tendrá mayor valor jurídico.

- La cadena de custodia durante una investigación forense a dispositivos móviles es vital, por lo que el marco de trabajo creado contiene diferentes herramientas que podrán ser utilizadas a lo largo de la investigación con el fin de que al culminar dicha investigación, de esta manera se puede presentar una documentación precisa y completa de cada una de las acciones realizadas sobre la evidencia recogida, haciendo que los resultados obtenidos de la investigación tengan mayor probabilidad de ser aceptados en una corte judicial.

6.2. RECOMENDACIONES

- Para la aplicación del análisis forense a dispositivos móviles es recomendable que la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia" implemente un Departamento Forense Técnico con la utilización del Sistema Operativo Tsurugi y sus herramientas, para de esta manera validar la calidad de las evidencias presentadas.

- Para el uso apropiado del Sistema Operativo Tsurugi y sus herramientas para el análisis forense es recomendable que el personal del área a cargo del mismo esté capacitado, para evitar errores al manejar la evidencia que puedan comprometerla y por efecto sea inválida para un proceso judicial o que de falsos resultados.

- Se recomienda que la Oficina Técnica de la Unidad de Violencia Carcelén" Casa de Justicia" realizar capacitaciones relativas a la seguridad tecnológica para todo el personal de la institución, teniendo en mente que la mejor seguridad de cualquier institución o empresa son los empleados.

7. BIBLIOGRAFÍA

[1] S. X. Caraguay Ramírez, «Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019», *Estado Comunes Rev. Políticas Probl. Públicos*, vol. 2, n.º 11, pp. 135-153, jul. 2020, doi: 10.37228/estado_comunes.v2.n11.2020.178.

[2] R.- ASALE y RAE, «análisis | Diccionario de la lengua española», *«Diccionario de la lengua española» - Edición del Tricentenario*. https://dle.rae.es/análisis (accedido 7 de noviembre de 2022).

[3] R.- ASALE y RAE, «digital | Diccionario de la lengua española», *«Diccionario de la lengua española» - Edición del Tricentenario*. https://dle.rae.es/digital (accedido 7 de noviembre de 2022).

[4] R.- ASALE y RAE, «dispositivo, dispositiva | Diccionario de la lengua española», *«Diccionario de la lengua española» - Edición del Tricentenario*. https://dle.rae.es/dispositivo (accedido 20 de octubre de 2022).

[5] M. Fernández-González y A. J. Torres-Gil, «Los dispositivos tecnológicos cotidianos en libros de texto. Presencia y análisis de las exposiciones», *Rev. Eureka Sobre Enseñ. Divulg. Las Cienc.*, vol. 11, n.º 3, pp. 290-302, 2014, doi: 10.25267/Rev_Eureka_ensen_divulg_cienc.2014.v11.i3.02.

[6] Ó. A. Claros, «MATRIX DEL DISPOSITIVO MÓVIL», *Razón Palabra*, n.º 85, 2013, Accedido: 20 de octubre de 2022. [En línea]. Disponible en: https://www.redalyc.org/articulo.oa?id=199531506027

[7] «Mensajes Directos Evidencia», *Safety Net Project*. https://www.techsafety.org/mensajes-directos-evidencia (accedido 20 de octubre de 2022).

[8] M. G. V. Bucheli y F. A. B. Terán, «WhatsApp como recurso para el trabajo grupal en estudiantes universitarios», *Apert. Guadalaj. Jal*, vol. 12, n.º 2, pp. 74-93, oct. 2020.

[9] J. C. M. López y M. L. Trujillo, «Análisis de datos para el marketing digital emprendedor: Caso de estudio del Parque de Innovación Empresarial de Manizales», *Univ. Empresa*, vol. 22, n.º 38, pp. 65-78, 2020.

[10] N. T. Machado, F. R. M. Basile, F. C. Amate, y L. J. R. López, «Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta», *Rev. Científica Gen. José María Córdova*, vol. 19, n.º 33, pp. 181-203, mar. 2021.

[11] Y. L. Li, «Estudio y evaluación de aplicaciones para el análisis forense de dispositivos móviles bajo Android en la Ciudad de Ambato», bachelorThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería en Sistemas Informáticos y Computacionales, 2013. Accedido: 7 de diciembre de 2022. [En línea]. Disponible en: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/4957

[12] K. W. Beltrán Tapia, «Modelo para análisis forense en dispositivos móviles con sistema operativo Android», masterThesis, Pontificia Universidad Católica del Ecuador, 2021. Accedido: 15 de diciembre de 2022. [En línea]. Disponible en: https://repositorio.pucesa.edu.ec/handle/123456789/3293

[13] R.- ASALE y RAE, «evidencia | Diccionario de la lengua española», *«Diccionario de la lengua española» - Edición del Tricentenario*. https://dle.rae.es/evidencia (accedido 27 de noviembre de 2022).

[14] M. Jorge, S. Karina, y H. Pablo, «ESTUDIO Y ANÁLISIS DE EVIDENCIA DIGITAL EN TELÉFONOS CELULARES CON TECNOLOGÍA GSM PARA PROCESOS JUDICIALES», p. 12.

[15] K. Alexandra, «Desarrollo de una Guía de Procedimientos en base al estudio de Modelos de Análisis Forense de Datos, aplicada en análisis a Dispositivos Móviles».

[16] *TSURUGI LINUX | Intalación*, (9 de julio de 2021). Accedido: 24 de octubre de 2022. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=ioWtoruX0Yc

[17] «Tsurugi Linux | Digital Forensics, Osint and malware analysis Linux Distribution». https://tsurugi-linux.org/index.php (accedido 21 de octubre de 2022).

[18] «Documentation Tsurugi Linux». https://tsurugi-linux.org/documentation_tsurugi_linux_changelog.php# (accedido 1 de febrero de 2023).

[19] «About Santoku · Santoku Linux». https://santoku-linux.com/about-santoku/ (accedido 26 de octubre de 2022).

[20] «Kali Docs | Kali Linux Documentation», *Kali Linux*. https://www.kali.org/docs/ (accedido 26 de octubre de 2022).

[21] «Manual y políticas - Caine». https://www.caine-live.net/page8/page8.html (accedido 26 de octubre de 2022).

[22] «e-fense :: Cyber Security & Computer Forensics Software». https://www.e-fense.com/index.php (accedido 26 de octubre de 2022).

[23] «The Volatility Foundation - Open Source Memory Forensics», *volatilityfoundation*. https://www.volatilityfoundation.org (accedido 26 de octubre de 2022).

[24] «Estación de trabajo SIFT | Instituto SANS». https://www.sans.org/tools/sift-workstation/ (accedido 26 de octubre de 2022).

[25] J. Sachowski, «Chapter 1 - Understanding Digital Forensics», en *Implementing Digital Forensic Readiness*, J. Sachowski, Ed. Boston: Syngress, 2016, pp. 3-16. doi: 10.1016/B978-0-12-804454-4.00001-0.

[26] «Alexandra - Desarrollo de una Guía de Procedimientos en base a.pdf». Accedido: 15 de diciembre de 2022. [En línea]. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/13484/Trabajo%20de%20Disertaci%c3%b3n%20-%20Katherine%20Jaya.pdf?sequence=1&isAllowed=y

[27] K. Mushtaque, K. Ahsan, y A. Umer, «Digital Forensic Investigation Models: An Evolution Study», *JISTEM J. Inf. Syst. Technol. Manag.*, vol. 12, n.º 2, pp. 233-243, 2015.

[28] «COIP_act_feb-2021.pdf». Accedido: 15 de diciembre de 2022. [En línea]. Disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

[29] «Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf». Accedido: 15 de diciembre de 2022. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

[30] R. Ramirez, «Delitos informáticos establecidos en el COIP y como prevenirlos», *Policia Nacional del Ecuador*, 27 de diciembre de 2017. https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/ (accedido 20 de enero de 2023).

[31] D. Avilla, «Avilla Forensics 3.0 - Translated into english (v1_0_0_204)». 5 de enero de 2023. Accedido: 10 de enero de 2023. [En línea]. Disponible en: https://github.com/AvillaDaniel/AvillaForensics

[32] D. Sazonov, «Andriller CE (Community Edition)». 9 de enero de 2023. Accedido: 10 de enero de 2023. [En línea]. Disponible en: https://github.com/den4uk/andriller

[33] «Magnet ACQUIRE», *Magnet Forensics*. https://www.magnetforensics.com/resources/magnet-acquire/ (accedido 10 de enero de 2023).

[34] «Triaging modern Android devices (aka android_triage bash script)». https://blog.digital-forensics.it/2021/03/triaging-modern-android-devices-aka.html (accedido 10 de enero de 2023).

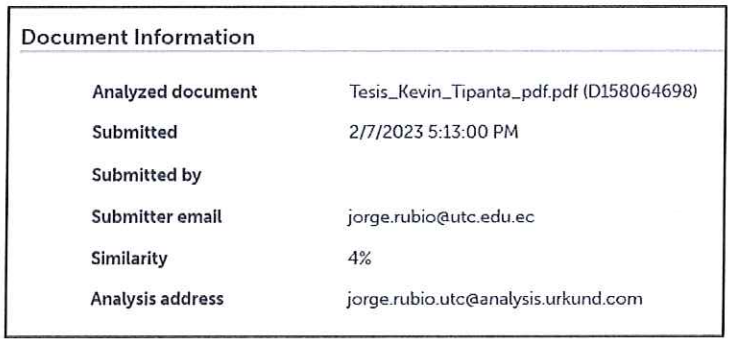
[35] «iOS Triage». RealityNet, 29 de octubre de 2022. Accedido: 10 de enero de 2023. [En línea]. Disponible en: https://github.com/RealityNet/ios_triage

[36] «Análisis Forense en Dispositivos Móviles (Latam)-20221114.mp4». https://ucapem-my.sharepoint.com/personal/contenido_ucapem_academy/_layouts/15/stream.aspx?id=%2Fpersonal%2Fcontenido%5Fucapem%5Facademy%2FDocuments%2FVideos%2FTaller%20AFDM22%2FLATAM%2FAn%C3%A1lisis%20Forense%20en%20Dispositivos%20M%C3%B3viles%20%28Latam%29%2D20221114%2Emp4&ga=1 (accedido 28 de diciembre de 2022).

ANEXO A. INFORME ANTI PLAGIO PROYECTO DE TITULACIÓN

Facultad:	Ciencias de la Ingeniería y Aplicadas
Carrera:	Ingeniería en Sistemas de Información
Nombre del docente evaluador que emite el informe:	Ing. Jorge Bladimir Rubio Peñaherrera, Mgs.
Documento evaluado:	Proyecto de investigación presentado previo a la obtención del Título de Ingeniero en Sistemas de Información.
Autor del documento:	Sr. Tipanta Díaz Kevin Mauricio
Programa de similitud utilizado:	Sistema URKUND
Porcentaje de similitud según el programa utilizado:	4 %
Observaciones: Calificación de originalidad atendiendo a los siguientes criterios: • El documento cumple criterios de originalidad, sin observaciones. • El documento cumple criterios de originalidad, con observaciones. • El documento no cumple criterios de originalidad.	 -X- --- ---
Fecha de realización del informe:	2/7/2023 5:13:00 PM

Captura de pantalla del documento analizado:



Document Information

Analyzed document	Tesis_Kevin_Tipanta_pdf.pdf (D158064698)
Submitted	2/7/2023 5:13:00 PM
Submitted by	
Submitter email	jorge.rubio@utc.edu.ec
Similarity	4%
Analysis address	jorge.rubio.utc@analysis.urkund.com

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs.
Director del Proyecto de Investigación

Document Information

Analyzed document	Tesis_Kevin_Tipanta_pdf.pdf (D158064698)
Submitted	2/7/2023 5:13:00 PM
Submitted by	
Submitter email	jorge.rubio@utc.edu.ec
Similarity	4%
Analysis address	jorge.rubio.utc@analysis.urkund.com

Sources included in the report

SA	**3. Borrador2-TFM_Cap1 (2).docx** Document 3. Borrador2-TFM_Cap1 (2).docx (D53936709)	2
SA	**Actividad+3_IIBimestre_HugoXavierDefazVizcaino.pdf** Document Actividad+3_IIBimestre_HugoXavierDefazVizcaino.pdf (D125217456)	1
SA	**M1.833_20212_PEC 1 Plan de trabajo_16758053.txt** Document M1.833_20212_PEC 1 Plan de trabajo_16758053.txt (D129468438)	1
W	URL: https://tsurugi-linux.org/documentation_tsurugi_linux_changelog.php Fetched: 2/7/2023 5:15:00 PM	1
W	URL: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Ele... Fetched: 2/7/2023 5:15:00 PM	2
SA	**M1.881_20221_PEC 3 Seguimiento de la memoria_18855063.txt** Document M1.881_20221_PEC 3 Seguimiento de la memoria_18855063.txt (D154492525)	2
W	URL: https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/ Fetched: 2/7/2023 5:16:00 PM	1
SA	**81.625_20221_PEC3 - Entre el 80% y el 90% de todo el TFG_18857849.txt** Document 81.625_20221_PEC3 - Entre el 80% y el 90% de todo el TFG_18857849.txt (D154498916)	1
W	URL: https://repositorio.pucesa.edu.ec/handle/123456789/3293 Fetched: 2/7/2023 5:14:00 PM	1
SA	**MSIA.docx** Document MSIA.docx (D14348133)	1
W	URL: https://tsurugi-linux.org/index.php Fetched: 2/7/2023 5:15:00 PM	1
W	URL: https://blog.digital-forensics.it/2021/03/triaging-modern-android-devices-aka.html Fetched: 2/7/2023 5:18:00 PM	1

ANEXO B: **Hoja de vida del tutor**

CURRÍCULUM VITAE

1. DATOS PERSONALES

NOMBRE COMPLETO:	Jorge Bladimir Rubio Peñaherrera.
CEDULA DE IDENTIDAD:	050222229-2
FECHA DE NACIMIENTO:	Pujilí, 16 de mayo de 1976.
EDAD:	46 años.
ESTADO CIVIL:	Casado.
DIRECCIÓN:	Pujilí, Calle Gabriel Álvarez 1-13 y Juan José Merizalde.
NÚM. CELULAR:	(593)0995220308
E-MAIL:	jorge.rubio@utc.edu.ec jbladimirrp@hotmail.com
COLEGIO PROFESIONAL:	# 15 - 05029 Conferida por la Sociedad de Ingenieros del Ecuador
Orcid:	https://orcid.org/0000-0001-9620-1437

2. ESTUDIOS REALIZADOS

- **CUARTO NIVEL:** Pontificia Universidad Católica del Ecuador
- **TERCER NIVEL:** Universidad Técnica de Cotopaxi.
- **NIVEL SECUNDARIO:** Instituto Tecnológico "Vicente León".

3. TÍTULOS

POSTGRADO: Magister en Gerencia Informática, mención Desarrollo de Software y Redes – PUCE-SA

- Año de obtención: 2010
- Número de Registro: **1027 - 10 – 712825**

POSTGRADO: Diplomado Superior en Gerencia Informática - PUCE-SA

- Año de obtención: 2007
- Número de Registro: **1027 – 07 - 669360**

PREGRADO: Ingeniero en Informática y Sistemas Computacionales

- Año de obtención: 2003
- Número de Registro: **1020 – 03 – 459773**

4. EXPERIENCIA LABORAL

- **Universidad Técnica de Cotopaxi**
  Docente Titular Agregado 1 (Nombramiento).

- **Instituto Universitario de Innovación, Ciencia y Tecnología INUDI-PERÚ.**
  Docente Investigador (2020 – Actualidad).
- **Pontificia Universidad Católica del Ecuador sede Ambato**
  Docente de Postgrados (2011 - 2019).
- **Pontificia Universidad Católica del Ecuador sede Ibarra**
- Docente de Postgrados (2011 - 2019).
- **Universidad Tecnológica Indoamérica, Quito**
  Docente de Pregrado Modalidad Semipresencial (2008 - 2013).
- **Universidad Politécnica Salesiana**
  Docente (2003 - 2005).
- **Universidad Técnica Particular de Loja. Centro asociado Latacunga** Docente (2004 - 2008).
- **Instituto Tecnológico Superior Aeronáutico. ITSA**
  Docente (2009 - 2010).
- **Instituto Tecnológico Victoria Vásconez Cuvi.**
  Docente – Coordinador de Carrera (2001 - 2007).
- **Cooperativa de Ahorro y Crédito "Andina" Ltda.**
  Jefe de Sistemas (2010).
- **Babel Software**
  Programador – Desarrollador (2008 - 2009).

5. CARGOS DESEMPEÑADOS

- **COORDINADOR DE LA CARRERA DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES– UA-CIYA.**
  Universidad Técnica de Cotopaxi, septiembre 2015 hasta 30 de septiembre del 2016.

- **COORDINADOR DE TRABAJO DE GRADO DE LA UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS – CIYA.**
  Universidad Técnica de Cotopaxi, Septiembre 2011 hasta 30 DE Septiembre del 2015.

- **COORDINADOR DE INVESTIGACIÓN DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES – CIYA.**
  Universidad Técnica de Cotopaxi, Marzo 2011 hasta Septiembre 2011.

6. CERTIFICACIONES

- **CERTIFICACIÓN CISCO CyberOps, para Instructores.**
  Cisco ESPOL – Octubre del 2021.

- **CERTIFICACIÓN CISCO DevNet, para Instructores.**
  Cisco ESPOL – Junio del 2021.

- **CERTIFICACIÓN CISCO CCNAv7: Bridging (Instructor) Actualización.**
  Cisco ESPOL – Mayo del 2020.

- **CERTIFICACIÓN CISCO CCNAv6_Mod_4 para Instructores.**
  Cisco ESPOL – Enero del 2020.

- **CERTIFICACIÓN CISCO CCNA v6_Mod_3 para Instructores.**
  Cisco ESPOL – Noviembre del 2019.

- **CERTIFICACIÓN CISCO CCNA v6_Mod_2 para Instructores.**
  Cisco ESPOL – Octubre del 2019.

- **CERTIFICACIÓN CISCO CCNA v6_Mod_1 para Instructores.**
  Cisco ESPOL – Agosto del 2019.

- **CERTIFICACIÓN EN SEGURIDAD INFORMÁTICA Y ETICAL HACKING**
  Colombia – Agosto del 2015

- **CERTIPORT MICROSOFT**
  IBEC del Ecuador – Agosto del 2012.

- **IC3 INTERNET AND COMPUTING CORE CERTIFICATION**
  IBEC del Ecuador – Agosto del 2012.

7. PARTICIPACIÓN EN PROYECTOS DE INVESTIGACIÓN

- **RED DE ESTUDIOS CIENCIOMÉTRICOS (REDEC).**
  Universidad Técnica de Cotopaxi – Departamento de Investigación UTC

- **IDENTIFICACIÓN DE SISTEMAS DE INFORMACIÓN QUE CONTRIBUYAN CON LA ORGANIZACIÓN Y GOBIERNO ELECTRÓNICO.**
  Facultad de Ciencias de la Ingeniería y Aplicadas, Carrera de Ingeniería en Informática y Sistemas Computacionales.
  Investigación Formativa.

- **"TIC´S EN LA EDUCACIÓN SUPERIOR E INNOVACIÓN DEL DOCENTE DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI"**
  Universidad Técnica de Cotopaxi – Departamento de Investigación 2012.

- **DESARROLLO E IMPLEMENTACIÓN DE UN SOFTWARE DE AYUDA EN EL APRENDIZAJE DE CÓDIGO BRAILLE, APLICANDO LA TECNOLOGÍA VISUAL 6.0, MEDIANTE UN CIRCUITO ELECTRÓNICO CONECTADO AL PUERTO PARALELO DEL COMPUTADOR, DIRIGIDO AL INSTITUTO DE EDUCACIÓN ESPECIAL DE NO VIDENTES DE LA PROVINCIA DE COTOPAXI.**
  Universidad Técnica de Cotopaxi – Departamento de Investigación 2011 - 2012.

8. LIBROS PUBLICADOS

- **"SISTEMAS DE COMUNICACIÓN Y REDES INFORMÁTICAS"**
  ISBN 978-9978-395-41-7

  Editorial UTC

  Autor

  http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/11/13/45-1

- **"TIC + Información + Conocimiento=Inteligencia Organizacional: Una Excelente Fórmula para la Toma de Decisiones acertadas"**
  ISBN 978-9978-395-41-7

  Editorial UTC

  Co-Autor

  http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/15/17/61-1

- **"LAS TRES CAPAS DE LOS SISTEMAS DE INFORMACIÓN WEB CON (una) JAVA"**
  ISBN 978-9978-395-41-7

Editorial UTC

Co-Autor

http://investigacion.utc.edu.ec/libros/index.php/libros/catalog/view/8/10/33-1

CAPÍTULO DE LIBROS

- **"INSTRUCCIÓN HÍBRIDA: LA EDUCACIÓN CON MIRAS AL FUTURO TECNOLÓGICO "**
  ISBN 978-958-56608-7-8

  Editorial Corporación CIMTED

  La Ceja, Antioquia – Colombia

  Páginas: 260 - 273

  http://memoriascimted.com/wp-content/uploads/2018/11/libro-coincom-congreso-2018.pdf

9. ARTÍCULOS PUBLICADOS (Publicaciones Científicas)

- **ANÁLISIS DEL USO DE TECNOLOGÍAS SEMÁNTICAS PARA LA GESTIÓN DE REDES INFORMÁTICAS EN LA EMPRESA HISPANOROSES Cia. Ltda. DE LA CIUDAD DE LATACUNGA**
  ISSN: 2306-2495 I RNPS 2343 – Vol. 14 No. 12, Diciembre, 2021, Pág. 166 – 186.
  Grupo editorial "ediciones Futuro" Universidad de Ciencias Informáticas UCI
  La Habana – Cuba / Serie Científica
  Link de la publicación
  https://publicaciones.uci.cu/index.php/serie/article/view/999

- **TÉCNICAS DE VIRTUALIZACIÓN UTILIZANDO EL IMPREVISOR CITRIX PARA LA OPTIMIZACIÓN DE EQUIPOS OBSOLETOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.**
  ISSN: 2306-2495 I RNPS 2343 – Vol. 14 No. 12, Diciembre, 2021, Pág. 206 – 224.
  Grupo editorial "ediciones Futuro" Universidad de Ciencias Informáticas UCI
  La Habana – Cuba / Serie Científica
  Link de la publicación
  https://publicaciones.uci.cu/index.php/serie/article/view/1005

- **EXPERIMENTACIÓN EN UN PROTOTIPO DE TECNOLOGÍA LI -FI PARA MEDIR SU CAPACIDAD DE ALCANCE EN AMBIENTES CON LUZ ARTIFICIAL**
  ISSN: 2588-0748 – Vol. 1 No. 3 (2020)
  Link de la publicación
  https://reciamuc.com/index.php/RECIAMUC/article/view/500

- **CARACTERIZACIÓN DE LA GESTIÓN BASADA EN TECNOLOGÍAS SEMÁNTICAS PARA LA ADMINISTRACIÓN DE REDES INFORMÁTICAS**
  ISSN: 2602-8255 - Vol. 2 No. 1
  Revista CIYA – UTC - indexada en DRJI
  Link de la publicación
  http://investigacion.utc.edu.ec/revistasutc/index.php/ciya

- **GENXMLDC: SOFTWARE PARA MOSTRAR EL USO DE TECNOLOGÍAS DE LA WEB SEMÁNTICA.**
  ISSN: 2602-8255 - Vol. 1 No. 1
  Revista CIYA – UTC - indexada en DRJI
  Link de la publicación
  http://investigacion.utc.edu.ec/revistasutc/index.php/ciya/article/view/72/70

- **PLATAFORMA CON INFORMACIÓN GEOGRÁFICA, DE APOYO AL PLAN DE EVACUACIÓN LATACUNGA, EN CASO DE ERUPCIÓN DEL VOLCÁN COTOPAXI.**
  ISSN: 1390 1117- Vol. 1 No. 1
  Revista Ciencias ESPE. (Escuela Politécnica del Ejército)
  Bases de Datos Indexada
  Latindex.
  Link de la publicación
  https://ia601508.us.archive.org/30/items/Articulo8_201705/Arti%CC%81culo%208.pdf

- **LAS AUDITORÍAS DEL CONOCIMIENTO COMO HERRAMIENTAS DE APOYO A LA ORGANIZACIÓN Y GESTIÓN DEL CONOCIMIENTO: UN ESTUDIO DE CASO**
  ISSN 2346-9161 - Vol. 7 No. 1
  IBEROAMERICAN JOURNAL OF PROJECT MANAGEMENT.
  Bases de Datos Indexada
  Latindex e Index Copernicus.
  Link de la publicación
  http://www.ijopm.org/index.php/IJOPM/article/view/254/333

- **LEVELS OF SIMILARITY IN USER PROFILES BASED CLUSTER TECHNIQUES AND MULTIDIMENSIONAL SCALING**
  ISSN: 2074-1308 - Volumen 10, 2016
  INTERNATIONAL JOURNAL OF SYSTEMS APPLICATIONS, ENGINEERING & DEVELOPMENT
  Bases de Datos Indexada
  Inspec - The IET, Index Copernicus.
  Link de la publicación
  http://www.naun.org/main/UPress/saed/2016/a202014-058.pdf

- **METAHEURISTIC ALGORITHMS HELPING TO TAKE DECISIONS IN INVESTMENT PORTFOLIOS.**
  ISSN: 2309-0685 - Vol. 4 No. 2016
  INTERNATIONAL JOURNAL OF ECONOMICS AND STATISTICS.
  Bases de Datos Indexada
  German National Library of Economics e Index Copernicus
  Link de la publicación
  http://www.naun.org/main/NAUN/economics/2016/a082015-063.pdf

- **Guía virtual interactiva en Android a través de códigos QR en el Museo de la Escuela Fiscal Isidro Ayora del Ecuador.**
  ISSN: 0864 - 4659 - Volumen 47, N° 3 septiembre – diciembre, Pág. 9 - 17
  Redalyc

Link de la publicación
https://www.redalyc.org/articulo.oa?id=181452084002

OTRAS PUBLICACIONES EN REVISTAS REGIONALES O LOCALES

- **SEMILLERO DE ROBÓTICA**
  Revista Alma Mater, N° 10, Universidad Técnica de Cotopaxi, 2013, Pág. 343.
  ISBN: 978-9978-395-08-0

- **DESARROLLO DE UNA APLICACIÓN SOFTWARE Y HARDWARE PARA LA ENSEÑANZA DEL CÓDIGO BRAILLE PARA PERSONAS CON DEFICIENCIA VISUAL.**
  Revista Alma Mater, N° 10, Universidad Técnica de Cotopaxi, 2013, Pág. 343.
  ISBN: 978-9978-395-08-0

- **RECURSOS EDUCATIVOS WEB 2.0 PARA MEJORAR EL PROCESO DE ENSEÑANZA APRENDIZAJE.**
  Revista Alma Mater, N° 10, Universidad Técnica de Cotopaxi, 2013, Pág. 343.
  ISBN: 978-9978-395-08-0

- **IPV6, LA NUEVA VERSIÓN DEL INTERNET.**
  Revista Desafíos, N° 2, enero del 2013, Pág. 18 - 19.

- **ESTUDIO COMPARATIVO ENTRE J2EE Y .NET PARA EL DESARROLLO DE APLICACIONES WEB.**
  Revista de Investigación Científica N°1 UTCiencia
  Universidad Técnica de Cotopaxi - 2011
  ISSN: 1390 - 6909

- **LINUX, UN NUEVO SISTEMA OPERATIVO**
  Revista Alma Mater #6
  Universidad Técnica de Cotopaxi.

10. PONENCIAS EN CONGRESOS NACIONALES E INTERNACIONALES

- **LIFI la Tecnología del Futuro**
  Autor: Jorge Rubio.
  Congreso de Ciencia, Tecnología e Innovación "Vicente León" 2022
  Instituto Superior Tecnológico "Vicente León" Ecuador.

- **EXPERIMENTACIÓN EN UN PROTOTIPO DE TECNOLOGÍA LI -FI PARA MEDIR SU CAPACIDAD DE ALCANCE EN AMBIENTES CON LUZ ARTIFICIAL**

Autor: Jorge Rubio.
IX Congreso Internacional en Tecnologías de la Información y Comunicación - TAYACAJA – PERÚ 2021.
Universidad Nacional de Huancavelica Perú.

- **TECNOLOGÍA Y SOCIEDAD**
  Autor: Jorge Bladimir Rubio Peñaherrera.

  Seminario Tecnología y Sociedad 2021, **Buenaventura - Colombia** – 26 de enero del 2021.

- **GUÍA VIRTUAL INTERACTIVA EN ANDROID A TRAVÉS DE CÓDIGOS QR EN EL MUSEO DE LA ESCUELA ISIDRO AYORA DEL ECUADOR**
  Autores: Jorge Rubio, Fausto Vizcaíno, Gustavo Rodríguez.

  Congreso Internacional de Información INFO´ 2016, **La Habana - Cuba** – 2 de noviembre del 2016.

- **A WEB PLATAFORM WITH GEOGRAPHIC INFORMATION, TO SUPPORT EVACUATION CONTINGENCY PLAN OF LATACUNGA, IN THE CASE OF COTOPAXI VOLCANO ERUPTION**
  Autores: Alex Cevallos, Jorge Rubio, Gustavo Rodríguez.

  Congreso Internacional de Innovación y Transferencia del Conocimiento CIITC 2016, Quito - Ecuador del 25 al 27 de octubre del 2016.

13. RECONOCIMIENTOS

- **REVISTA VITEC**
  Reconocimiento por la contribución como parte del **Comité Científico de la Revista. (Par Evaluador).**

- **UNIVERSIDAD NACIONAL DE HUANCAVELICA_PERU – FACULTAD DE INGENIERÍA ELECTRÓNICA Y SISTEMAS**
  RECONOCIMIENTO Y FELICITACIÓN, con cargo a dar cuenta en el próximo Consejo de Facultad, al MG. Jorge Bladimir RUBIO PEÑAHERRERA, quien realizó la **ponencia** con el tema titulado "PROTOTIPO EXPERIMENTAL DE TECNOLOGÍA LI FI PARA MEDIR SU CAPACIDAD DE ALCANCE EN AMBIENTES CERRADOS CON LUZ ARTIFICIAL", el día martes 16 de noviembre de 2021, durante el desarrollo del "IX CONGRESO INTERNACIONAL EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN TAYACAJA - 2021 –MODALIDAD VIRTUAL, organizado por la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería Electrónica – Sistemas de la Universidad Nacional de Huancavelica.

ANEXO C: **Hoja de vida del investigador**

TIPANTA DIAZ KEVIN MAURICIO

DATOS PERSONALES

Edad: 23 años Email: tipanta63@gmail.com

Dirección: Sangolquí Juan Genaro Idiomas: español, ingles

Jaramillo y Quito Teléfono: 233-6344/0983382250

FORMACIÓN ACADÉMICA

Primaria-Secundaria

Academia militar del valle

Titulo obtenido: Bachiller en ciencias generales

Universidad

Universidad técnica de Cotopaxi / Actualmente cursando último semestre

EXPERIENCIA ACEDEMICA

Modelado UML

Especificación de requerimientos de software

Desarrollador front-end (CSS, HTML JavaScript, bootstrap)

Análisis forense de dispositivos móviles con Tsurugi

EXPERIENCIA LABORAL

Mantenimiento preventivo y correctivo de computadores

INTERESES

Seguridad informática

Análisis Forense Digital

CERTIFICADOS OBTENIDOS

- "I Congreso internacional multidisciplinario de vinculación con la sociedad “experiencias, resultados e impactos de los proyectos de vinculación de las ies", UTC. 2021.

- “II Feria Virtual de Emprendimiento e Innovación UTC 2021”, en la categoría prototipo, con el proyecto “TORC”, UTC. 2021.

- "Mantenimiento PC: Hardware y Software", UTC. 2021.

ANEXO D: Formulario de Encuesta

Preguntas de la encuesta realizada	
1.	¿Usted utiliza un dispositivo móvil?
2.	¿Qué dispositivo móvil utiliza?
3.	¿Qué aplicaciones utiliza?
4.	¿Conoce a cerca del análisis forense de dispositivos móviles?
5.	¿Conoce que se puede recuperar sus datos del dispositivo móvil así sean borrados permanentemente?
6.	¿Conoce sobre algún programa que recupere sus datos de forma correcta?
7.	¿Ha presentado alguna evidencia digital?
8.	¿Conoce sobre el proceso de extracción de evidencias?
9.	¿Conoce que las pruebas presentadas de su dispositivo móvil pueden ser tomadas en cuenta dentro de su proceso legal?

Fuente: Elaboración propia del investigador (2022)

ANEXO E: Formulario de Entrevista

Formulario de entrevista para la oficina técnica de violencia sobre como llevan a cabo los análisis de evidencias digitales y que les parece la herramienta Tsurugi
La siguiente entrevista va dirigida exclusivamente a los miembros de la oficina técnica de violencia de la "Casa de Justicia" consejo de judicatura Carcelén con el fin de obtener un criterio sobre la herramienta investigada y proponiendo el uso de la misma en los casos flagrantes.
Entrevistada/o: Perito () / Psicóloga/o
Cargo:
Fecha: 28/12/2022
1. ¿Cómo validan las evidencias digitales presentadas por los diferentes usuarios?
2. ¿Tiene alguna dificultad al momento de utilizar los recursos tecnológicos?
3. ¿Conoce sobre los diferentes métodos de análisis de dispositivos móviles?
4. ¿Ha utilizado alguna herramienta para la validación de evidencias?
5. ¿Conoce sobre el software libre?
6. ¿Qué tal le pareció Tsurugi?
7. Puede comentar sobre factores positivos que llevarían sus distintos peritajes con la herramienta Tsurugi
8. Del 1 al 10 qué tan útil piensa usted que es Tsurugi referente al caso práctico presentado.
9. Recomendaría a otras oficinas técnicas de violencia el software Tsurugi

Fuente: Elaboración propia del investigador (2022)

ANEXO F: Estimación de gastos

1.1.GASTOS DIRECTOS

RECURSOS	CANTIDAD	UNIDAD	V. UNITARIO	V. TOTAL
INTERNET	200	HORAS	0.60	120.00
IMPRESIONES	120	HOJAS	0.10	12.00
CUADERNOS	2	UNIDAD	1.50	3.00
ESFEROS	4	UNIDAD	0.50	2.00
CARPETA	2	UNIDAD	0.50	1.00
CAPACITACION TSURUGI	168	HORAS	100.00	100.00
TOTAL				**238**

Fuente: Elaboración propia del investigador (2022)

1.2. GASTOS INDIRECTOS

RECURSOS	CANTIDAD	UNIDAD	V. UNITARIO	V. TOTAL
GASOLINA	800	GALONES	2.40	1920.00
ARRIENDO	5	MESES	100.00	500.00
ALIMENTACION	80	Almuerzos	2.00	160.00
TOTAL				**2580.00**

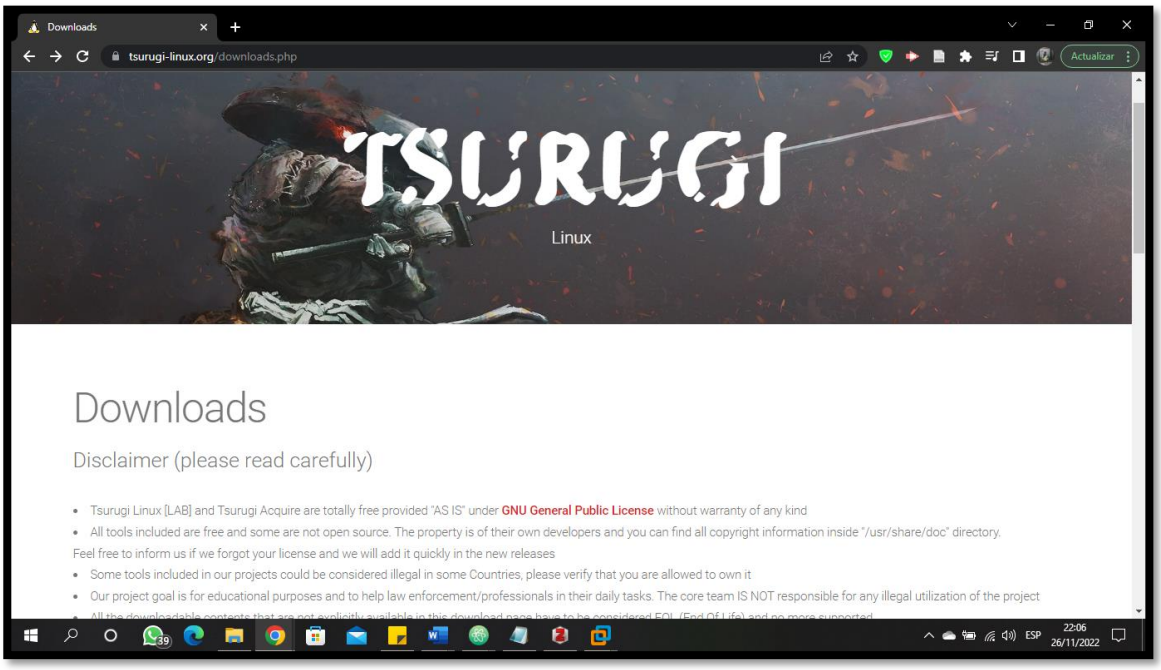
Fuente: Elaboración propia del investigador (2022)

1.3. TOTAL DE GASTOS

RECURSOS	PRESUPUESTO DEL PROYECTO DE INVESTIGACION
	VALORES TOTALES
GASTOS DIRECTOS	**238**
GASTOS INDIRECTOS	**2580**
GASTOS IMPREVISTOS	**100**
TOTAL	**2918.00**

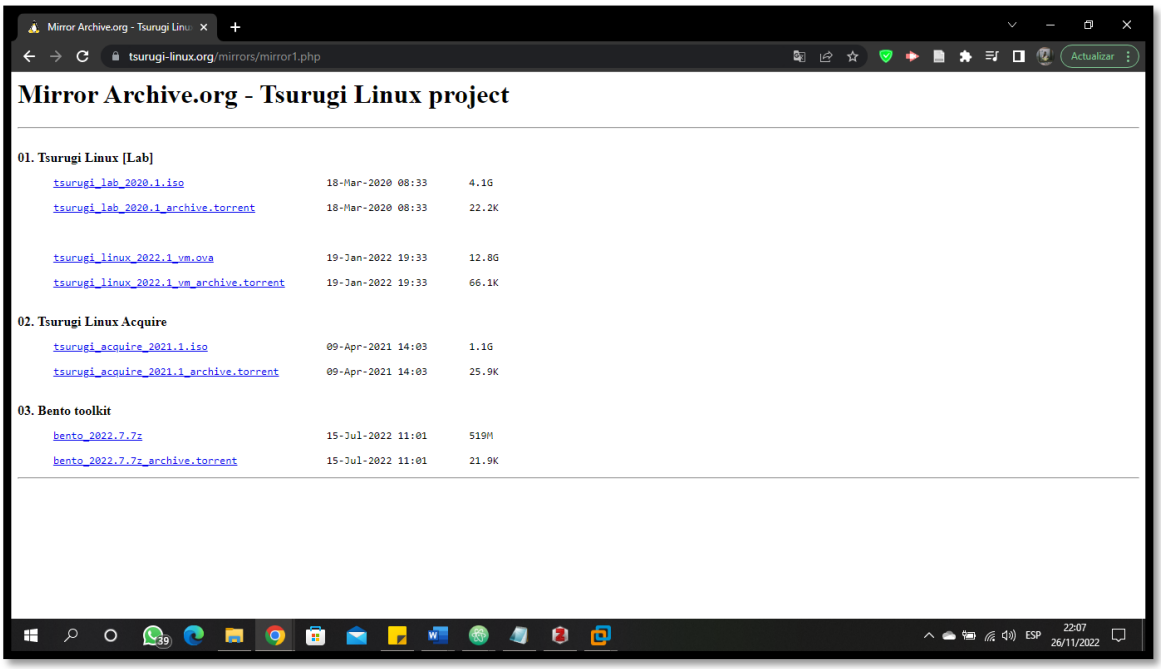
ANEXO G: Instalación de Tsurugi en una máquina virtual

6.1. BUSQUEDA DE TSURUGI DE SU PAGINA OFICIAL



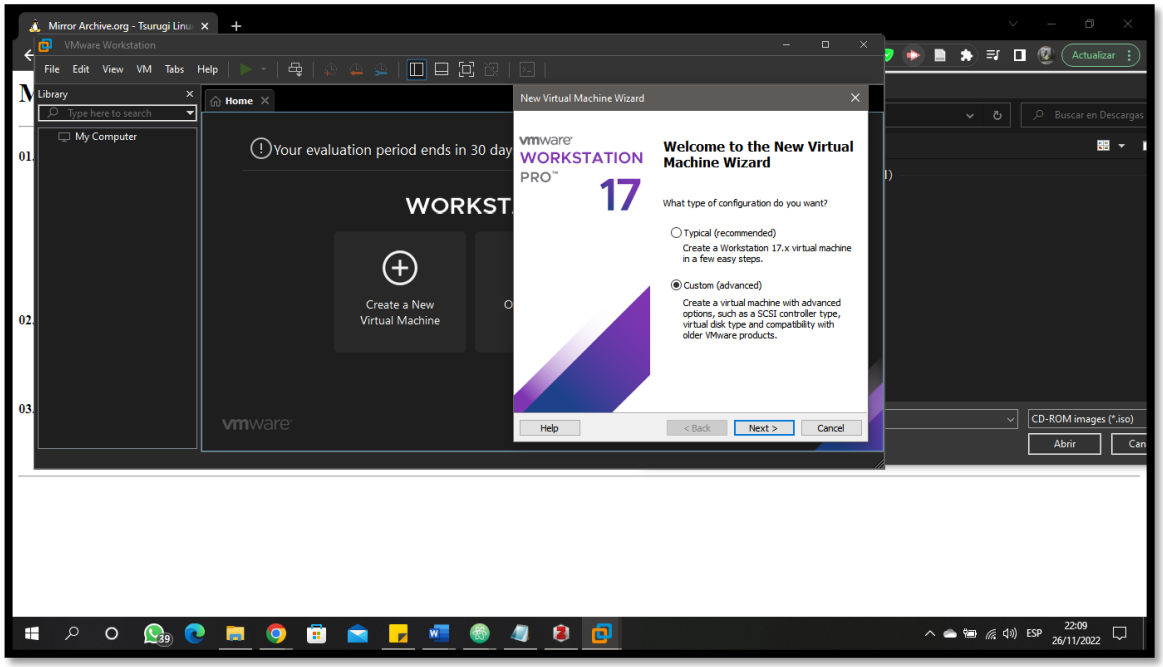
Fuente: Elaboración propia del investigador (2022)

6.2. DESCARGA DE TSURUGI DE SU PAGINA OFICIAL

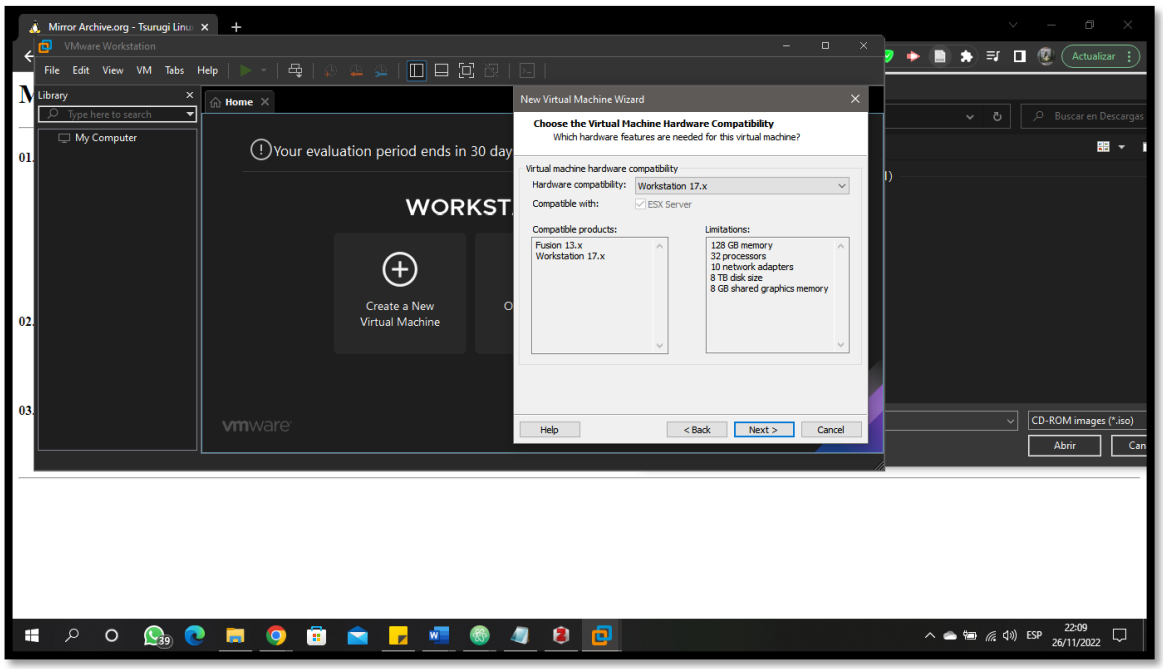


Fuente: Elaboración propia del investigador (2022)

6.3.CRECIÓN DE UNA MAQUINA VIRTUAL

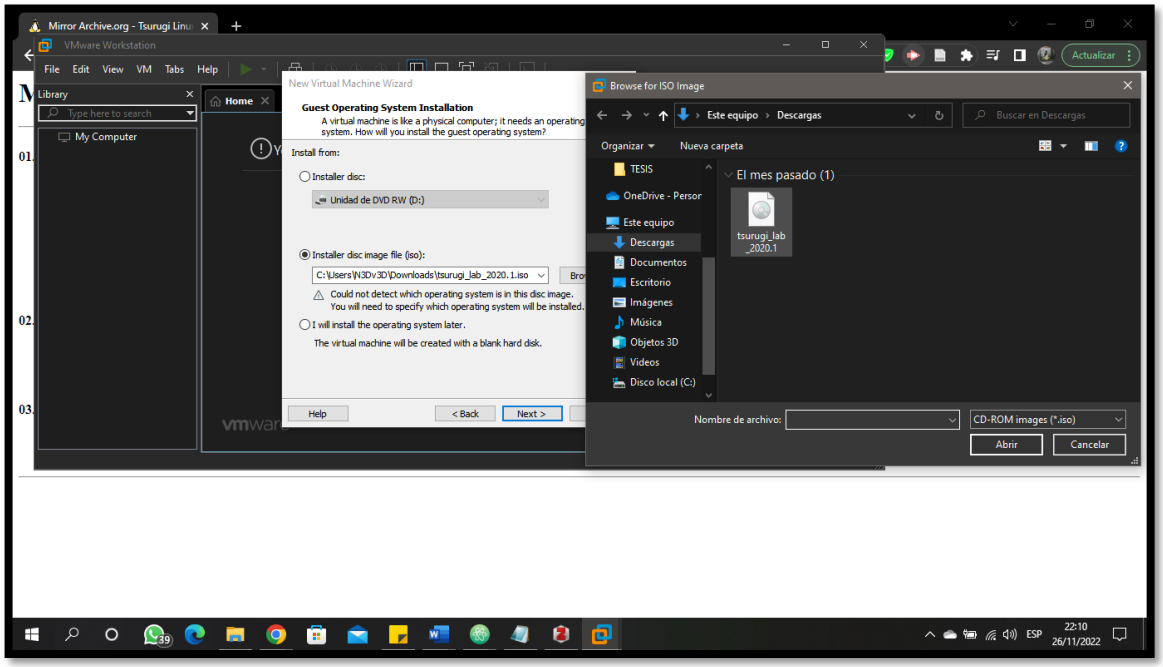


Fuente: Elaboración propia del investigador (2022)



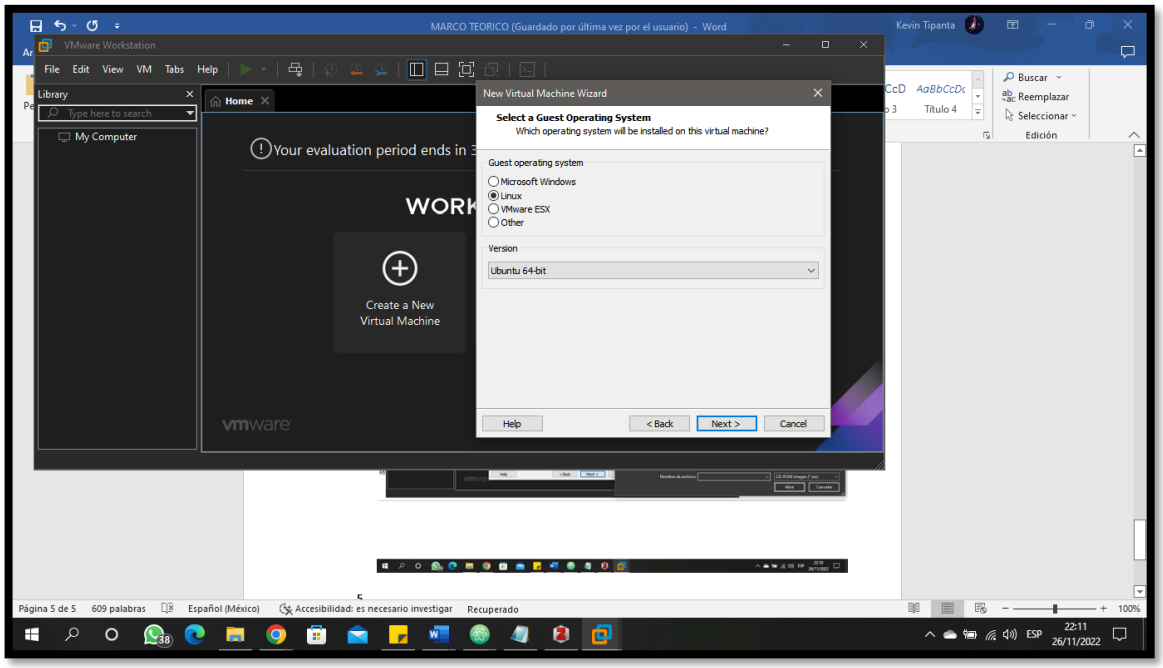
Fuente: Elaboración propia del investigador (2022)

6.4.SELECCIÓN DE LA ISO DE TSURUGI



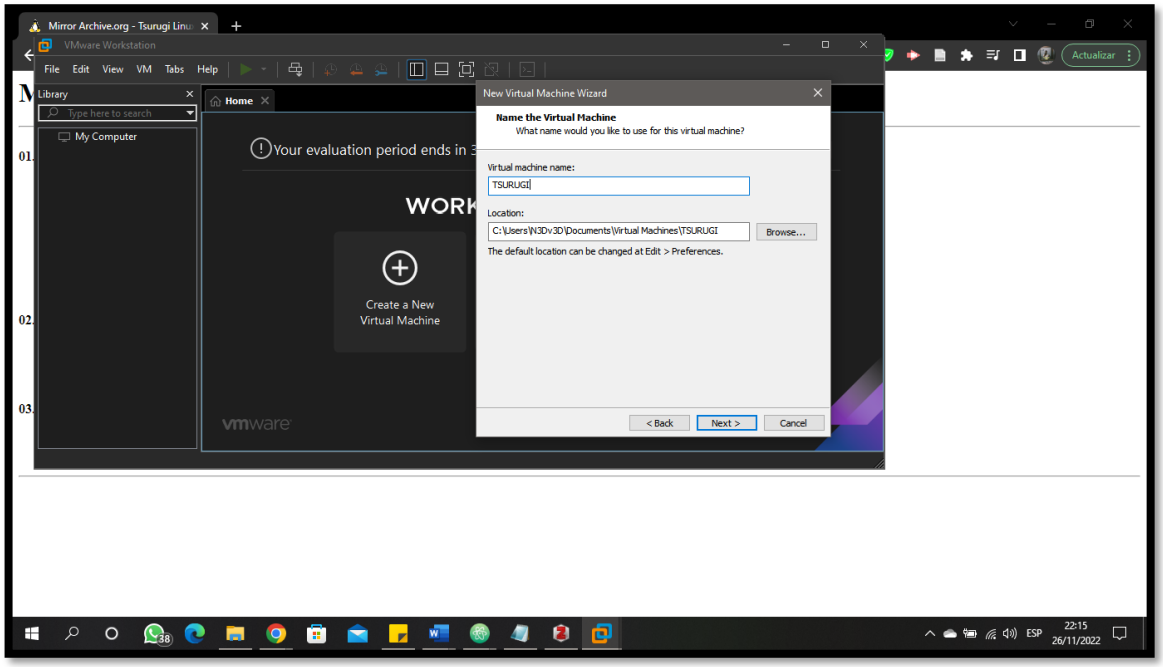
Fuente: Elaboración propia del investigador (2022)

6.5.SELECCIÓN DEL SISTEMA OPERATIVO



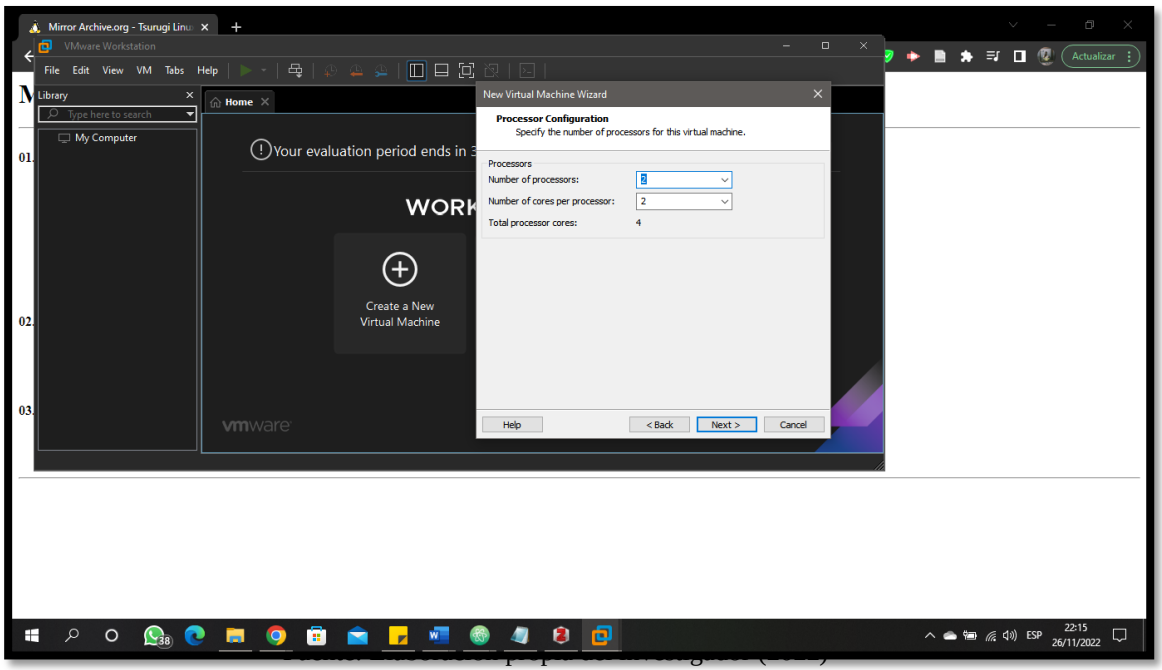
Fuente: Elaboración propia del investigador (2022)

6.6.NOMBRAMOS LA MAQUINA VIRTUAL

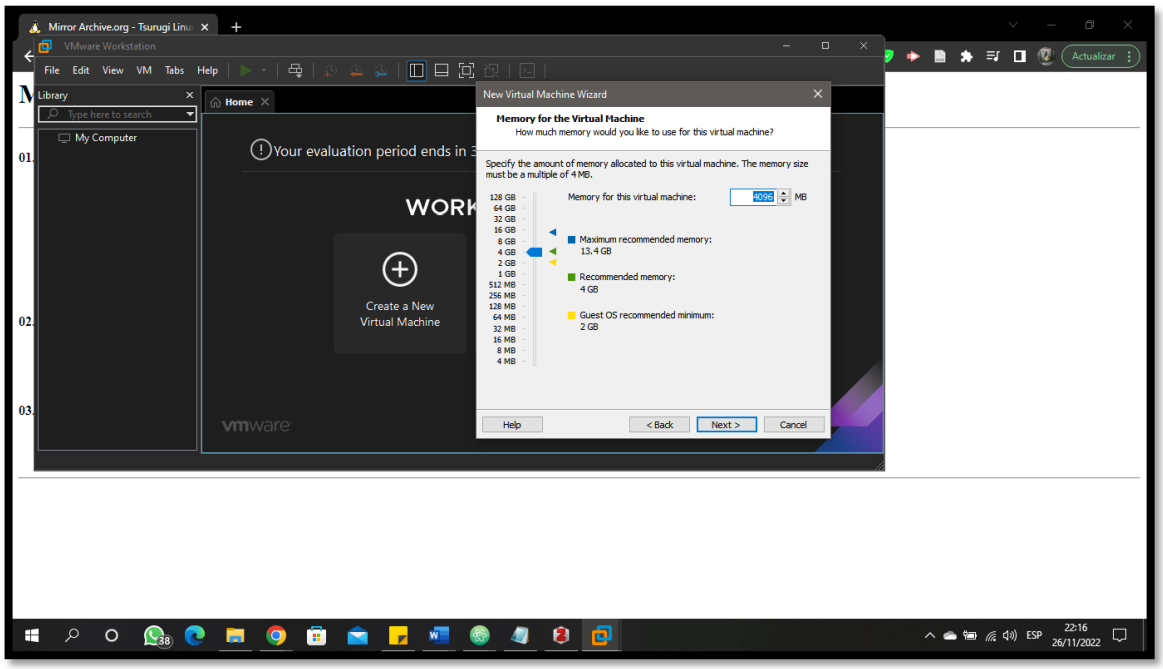


Fuente: Elaboración propia del investigador (2022)

6.7.ESTABLECEMOS EL NUMERO DE PROCESADORES Y CORES

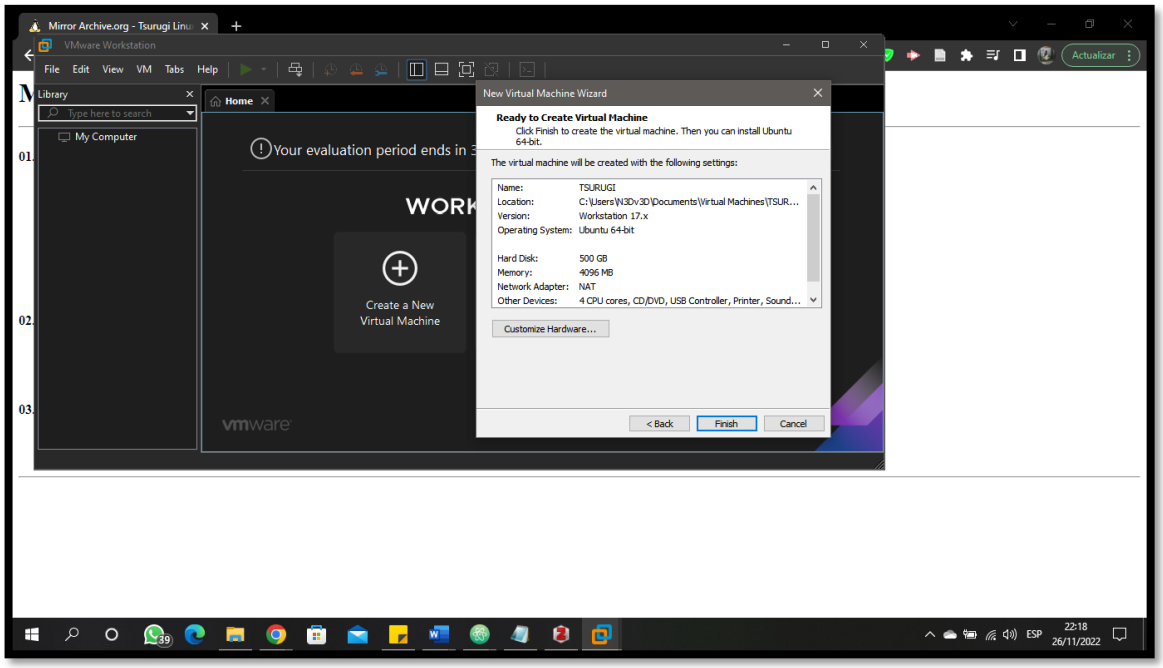


6.8. ESTABLECEMOS EL NUMERO DE MEMORIA



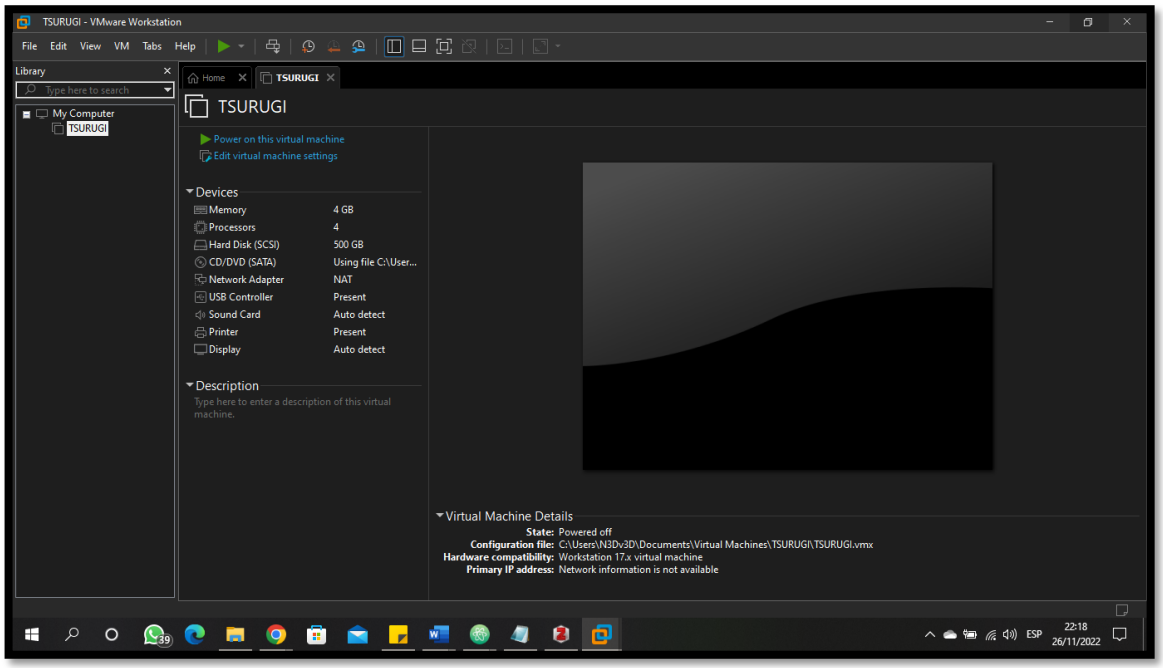
Fuente: Elaboración propia del investigador (2022)

6.9. POR ÚLTIMO, DAMOS EN FINALIZAR



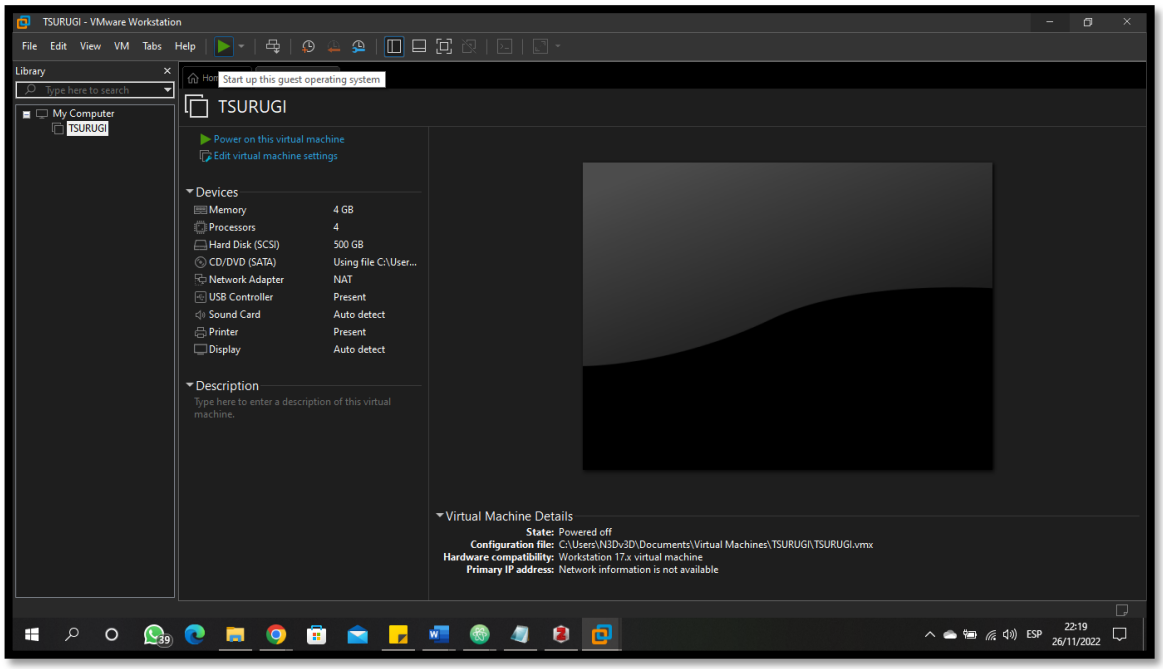
Fuente: Elaboración propia del investigador (2022)

6.10. NUESTRA MAQUINA VITUAL CREADA



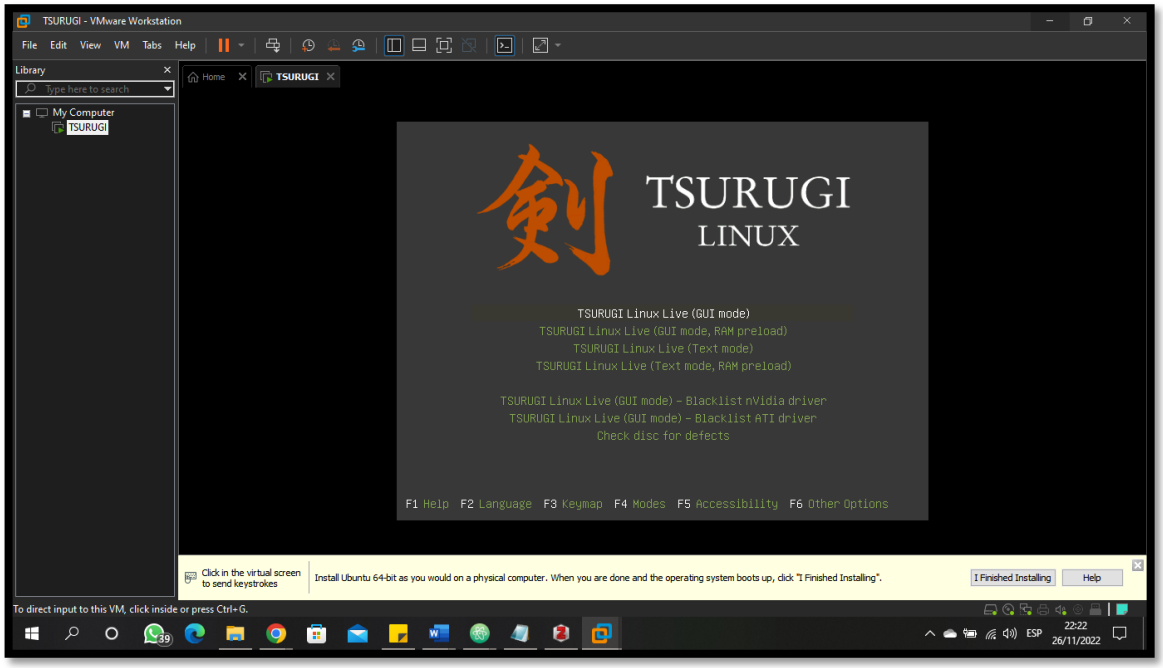
Fuente: Elaboración propia del investigador (2022)

6.11. INICIAMOS NUESTRA MAQUINA VIRTUAL

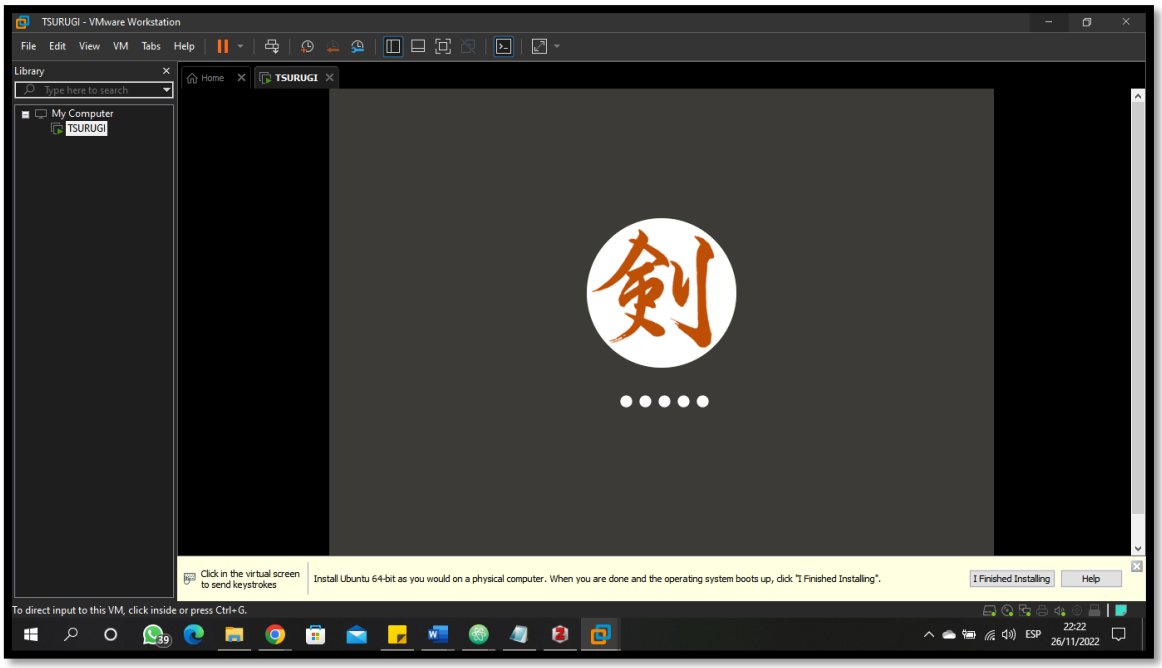


Fuente: Elaboración propia del investigador (2022)

6.12. INSTALAMOS EL SISTEMA OPERATIVO EN MODO VIVO

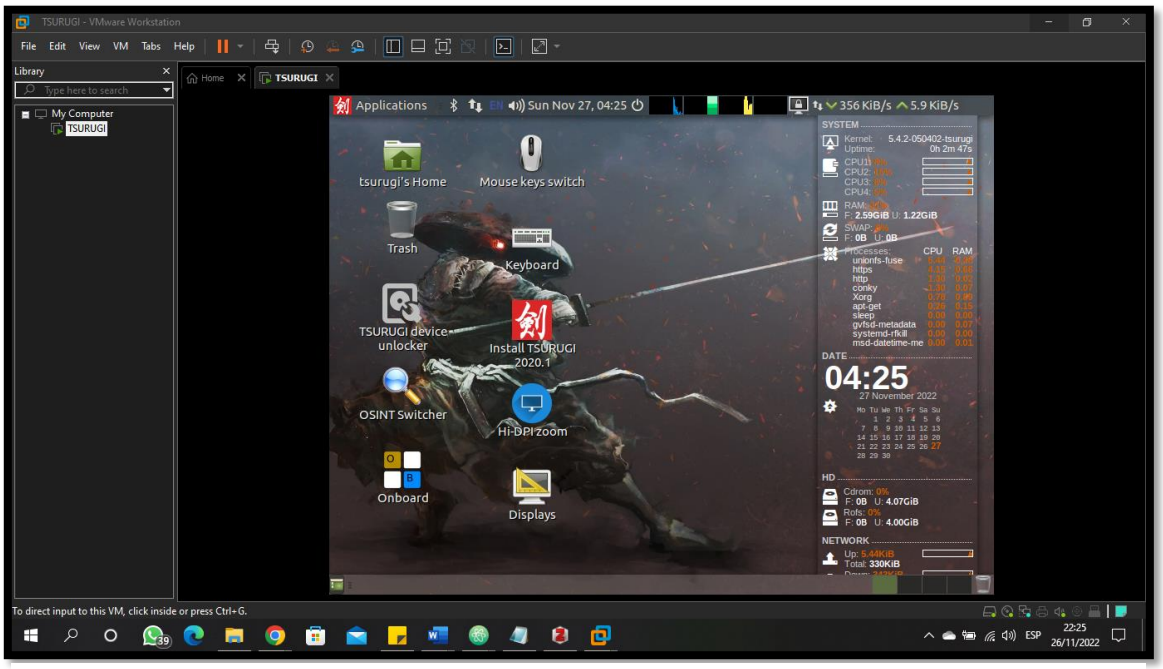


Fuente: Elaboración propia del investigador (2022)



Fuente: Elaboración propia del investigador (2022

6.13. INSTALACION COMPLETA



Fuente: Elaboración propia del investigador (2022)

ANEXO H: FORMATO DE DECLARACIÓN DE VOLUNTAD

DECLARACIÓN DE VOLUNTAD Y CONSENTIMIENTO INFORMADO ANÁLISIS DE DISPOSITIVOS MÓVILES
Formulario dirigido a las PARTES PROCESALES que acuden A la Unidad Violencia Contra La Mujer O Miembros Del Núcleo Familiar, que se someten al análisis de dispositivos móviles para la validación de evidencias.
En la ciudad de _____, a, los _____días, del mes de_____, del año _____. Yo, _____, portador de CC: _____ por mis propios derechos, en pleno uso de mis capacidades legales, de manera libre y voluntaria, luego de recibir la información completa que implica este análisis de dispositivo móvil, así como la metodología e instrumentos a aplicar, declaro bajo juramento QUE AUTORIZO SE REALICE EL MISMO de conformidad con la orden emitida por la autoridad competente. Sometiéndome a la legislación vigente que regula este tipo de actividades. Observaciones: _____ _____ _____ En la ciudad de_____, a, los _____días, del mes de _____, del año_____. Yo, _____, portador de CC: _____ por mis propios derechos, en pleno uso de mis capacidades legales, de manera libre y voluntaria, luego de recibir la información completa que implica este análisis, **ME NIEGO A REALIZAR EL ANALISIS DE DISPOSITIVO MOVIL** dispuesto por los siguientes motivos: _____ _____ _____ _____ _____

FIRMA O HUELLA DIGITAL		N CÉDULA DE CIUDADANÍA/PASAPORTE
NOMBRE DEL PERITO		N ACREDITACIÓN PERICIAL
FIRMA DEL PERITO		

Fuente: Elaboración propia del investigador (2022)

ANEXO I: FORMULARIO DE IDENTIFICACIÓN DEL DISPOSITIVO

ESTADO Y CARACTERISTICAS DEL DISPOSITIVO				
Estado del dispositivo	**Encendido**		**Apagado**	
Protegido por algún tipo de clave	**SI**		**NO**	
EN CASO DE TENER PROTECCIÓN (TIPO)				
Patrón				
PIN				
Contraseña				
Huella digital				
Reconocimiento Facial				
CARACTERÍSTICAS DEL DISPOSITIVO				
Marca del teléfono				
Modelo del teléfono				
Número de teléfono				
Operadora del servicio				
Numero serial IMEI				
DOCUMENTACIÓN EXTRA DEL DISPOSITIVO				
	SI		**NO**	
Memorias extraíbles (micro sd)				
Cargador				
Códigos de acceso				
RECEPCIÓN				
Receptado por:				
Revisado por:				
Autorizado por:				

ANEXO J: IMÁGENES DE ENTREVISTA Y DEMOSTRACIÓN DEL SISTEMA OPERATIVO TSURUGI

Figura 53. Entrevista con la perito intrafamiliar

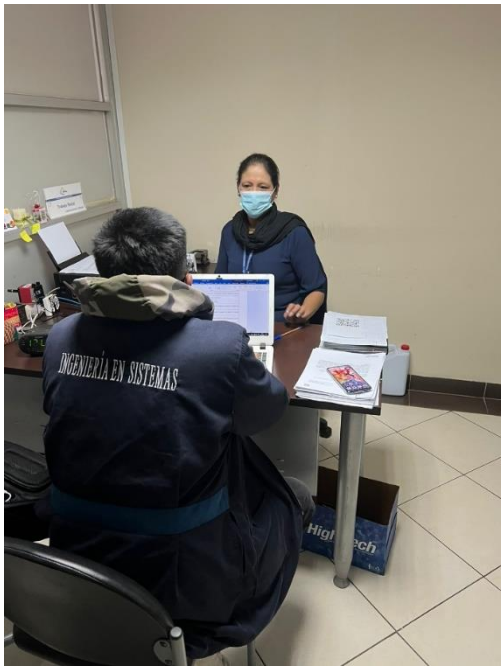


Figura 54. Entrevista

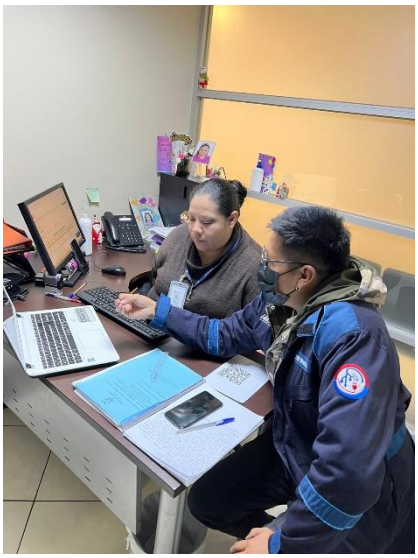


Figura 55. Entrevista con la Psicóloga

Figura 56. Reconocimiento de la oficina técnica de violencia y Casa de Justicia