UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES EN ENTORNOS ICLOUD

AUTOR

Pita Vera Carlos Adrián

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. HAZ LÓPEZ LIDICE

La Libertad, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. Jose Sanchez A. Msc.
DIRECTOR DE LA CARRERA

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Haz Lopez Lidice, Msi.
TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Ing. Daniel Quirumbay Yagual, Msia
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

Ing. Marjorie Coronel S. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por PITA VERA CARLOS ADRIAN, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 08 días del mes de diciembre del año 2023

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Haz López Lídice, Msi.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Pita Vera Carlos Adrián**

DECLARO QUE:

El trabajo de Titulación, "Análisis forense de evidencias digitales en entornos Icloud "previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 08 días del mes de diciembre del año 2023

EL AUTOR

Pita Vera Carlos Adrián

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis Forense de Evidencias Digitales en Entornos ICloud, presentado por el estudiante, PITA VERA CARLOS ADRIÁN fue enviado al Sistema Anti-plagio, presentando un porcentaje de similitud correspondiente al 1%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. HAZ LÓPEZ LÍDICE, MSI.

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Pita Vera Carlos Adrián**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción de este trabajo de titulación dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 08 días del mes de diciembre del año 2021

EL AUTOR

Pita Vera Carlos Adrián

AGRADECIMIENTO

Agradezco principalmente a Dios, fuente inagotable de sabiduría y guía, por otorgarme fortaleza y el discernimiento necesario para llevar a cabo el presente proyecto de titulación, su divina providencia ha sido mi faro en cada etapa de este proceso académico.

A mi familia, quienes han sido mi red de seguridad constante, les agradezco por si amor incondicional y por ser la fuente de mi inspiración, a mi madre Linda Vera, a mi padre Drino Pita, quienes me han ayudado a conseguir este logro gracias a su sacrificio y esfuerzo.

A la Universidad Estatal Península de Santa Elena, junto a mis docentes cuyos conocimientos y perspectivas enriquecieron significativamente mi conocimiento formándome como un futuro profesional

A mi docente tutor, Ing. Haz López Lidice, agradezco de manera especial por su dedicación y liderazgo, su orientación experta y compromiso han sido fundamentales para dar forma a este trabajo y llevarlo a buen puerto.

Carlos Adrián Pita Vera

DEDICATORIA

A Dios quien me dio sabiduría y ha iluminado mi camino y con su gracia ha sido mi fuerza en los momentos de desafío.

A mi Madre, por todo el cariño y amor que me ha brindado durante toda mi vida, que con su carácter me forjo como hombre de bien y me motivo en los momentos más difíciles cuando desistía, por aconsejarme, por regañarme, por siempre estar conmigo.

A mi Padre, quien me ha brindado todo lo que está a su alcance económicamente con la intensión de que no me falte nada en todo el proceso académico y por inculcarme valores y valentía para enfrentar obstáculo.

A mis Abuelos, Abg. Milton Vera, y Sra. Kelly Tómala, por acogerme en su morada y brindarme la estadía donde crecí y me formé como profesional, por sus valores y anécdota de cómo enfrentar la universitaria y la vida fuera de ella.

A mi pareja sentimental, Ing. Andrea Ramírez quien me ha brindado su apoyo contrastante en todas las facetas de mi vida universitaria.

Mi gratitud se extiende a mis seres queridos, amigos y compañeros de clase, quienes compartieron este viaje conmigo. Sus palabras de aliento, comprensión y apoyo moral fueron un bálsamo en momentos difíciles.

Carlos Adrián Pita Vera

RESUMEN

iCloud es un servicio de almacenamiento en la nube que permite a los usuarios almacenar, acceder y sincronizar sus datos, como videos, fotos, configuraciones y documentos desde diferentes dispositivos conectados a una cuenta de usuario. A pesar de los beneficios en términos de accesibilidad y conveniencia, iCloud ha enfrentado críticas que se relacionan con la seguridad, debido a que, sus datos no están cifrados de extremo a extremo, planteando preocupaciones sobre la privacidad, además de tener un riesgo potencial de accesos no autorizados y su dependencia a una conexión a Internet para utilizar sus funciones, exponiendo a los usuarios a posibles amenazas de seguridad.

Razón por la cual, se plantea el presente trabajo de investigación, el cual tiene como objetivo realizar un análisis de evidencias digitales iCloud a través de la implementación de diversos laboratorios forenses utilizando máquinas virtuales y herramientas de código libre, asociadas a la computación forense, el marco legislativo y tipos de servicios disponibles en la nube, como PaaS, SaaS e IaaS.

Este trabajo se desarrolla empleando la metodología descriptiva con aplicación de experimentos, junto con el diseño e implementación de tres ciber ataques en entornos controlados, con el objetivo de ejecutar un análisis forense de evidencias digitales, garantizando la integridad y asegurando la veracidad en la investigación. Para la ejecución del trabajo, se aplican las metodologías de investigación diagnóstica y exploratoria, recopilando la información necesaria para elaborar los requerimientos.

Los objetivos del trabajo radican en analizar la legislación vigente con respecto al desarrollo de un análisis forense en los entornos Cloud a través del ordenamiento de la protección de los datos; clasificar las amenazas cibernéticas más comunes que afectan a los servicios Cloud públicos y privados; diseñar escenarios experimentales y elaborar un informe que describa los resultados metodológicos de la investigación forense.

Como resultados de la investigación, se garantizó la legalidad y ética en los entornos Cloud, comprendiendo las leyes de protección de datos; así mismo, se clasificaron las amenazas cibernéticas, anticipando a posibles riesgos y desarrollando estrategias seguras; finalmente, se realizó un informe detallado describiendo los resultados y detallando recomendaciones para fomentar las prácticas seguras.

Palabras clave: Cloud, Ciberseguridad, Forense.

ABSTRACT

iCloud is a cloud storage service that allows users to store, access and sync their data such as videos, photos, settings and documents from different devices connected to a user account. Despite the benefits in terms of accessibility and convenience, iCloud has faced criticism that relates to security, because your data is not end-to-end encrypted, raising privacy concerns, in addition to having a potential risk of unauthorized access and its dependence on an Internet connection to use its functions, exposing users to possible security threats.

For this reason, the present research work is proposed, which aims to carry out an analysis of iCloud digital evidence through the implementation of various forensic laboratories using virtual machines and open-source tools, associated with forensic computing, the legislative framework and types of services available in the cloud, such as PaaS, SaaS and IaaS.

This work is developed using descriptive methodology with the application of experiments, along with the design and implementation of three cyber-attacks in controlled environments, with the objective of executing a forensic analysis of digital evidence, guaranteeing integrity and ensuring veracity in the investigation. To carry out the work, diagnostic and exploratory research methodologies are applied, collecting the necessary information to develop the requirements.

The objectives of the work lie in analyzing current legislation regarding the development of forensic analysis in Cloud environments through data protection regulations; classify the most common cyber threats that affect public and private Cloud services; design experimental scenarios and prepare a report that describes the methodological results of the forensic investigation.

As results of the research, legality and ethics in Cloud environments were guaranteed, including data protection laws; Likewise, cyber threats were classified, anticipating possible risks and developing secure strategies; Finally, a detailed report was made describing the results and detailing recommendations to promote safe practices.

Keywords: Cloud, Cyber security, Forensic.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

iCloud es un servicio de almacenamiento de la nube, propiedad de la compañía Apple, lanzado en el año 2012, dirigido principalmente a dispositivos con el sistema operativo iOS, como iPhone, iPod y iPad, ofreciendo el almacenamiento gratuito de archivos personales, incluyendo contenido multimedia en diferentes formatos. No obstante, también es utilizado para respaldar los dispositivos mencionados anteriormente, lo cual ha dado lugar a varios inconvenientes. En relación con la seguridad de los datos, se hallan varios aspectos negativos que se asocian con iCloud; este es el caso de que la información almacenada en este servicio no se cifra, lo que implica riesgos para su privacidad. Además, la carga de documentos en la nube puede resultar en un consumo de datos significativo, requiriendo conexión a Internet para su funcionamiento.

Por tal motivo, se propone el presente trabajo de investigación, el cual tiene como objetivo realizar un análisis de evidencias digitales iCloud a través de la implementación de diversos laboratorios forenses utilizando máquinas virtuales y herramientas de código libre, asociadas a la computación forense, el marco legislativo y tipos de servicios disponibles en la nube, como PaaS, SaaS e IaaS.

Este estudio está desarrollado aplicando la metodología descriptiva con aplicación de experimentos, diseñando e implementando tres ciber ataques en entornos controlados, con el propósito de ejecutar un análisis forense de evidencias digitales, garantizando la integridad y asegurando la veracidad en la investigación. Para la elaboración del trabajo, se utilizan las metodologías de investigación diagnóstica y exploratoria, recopilando la información necesaria para elaborar los requerimientos.

Así mismo, se pretende analizar la legislación vigente con respecto al desarrollo de un análisis forense en los entornos Cloud a través del ordenamiento de la protección de los datos; clasificar las amenazas cibernéticas más comunes que afectan a los servicios Cloud públicos y privados; diseñar escenarios experimentales y elaborar un informe que describa los resultados metodológicos de la investigación forense.

El presente informe, se estructura de la siguiente forma:

El capítulo I, presenta los antecedentes, descripción del proyecto, objetivos de la investigación, justificación, alcance y metodología.

El capítulo II de la propuesta, contiene el marco contextual, marco conceptual, marco teórico y requerimientos.

El capítulo III abarca la simulación de los ataques en servicios iCloud y la identificación de incidentes y análisis forense.

Finalmente, en el capítulo IV se muestran los resultados de la investigación, incluyendo las encuestas realizadas y la guía de buenas prácticas para la implementación de la arquitectura Cloud Computing.

1.1. Antecedentes

iCloud es un servicio de almacenamiento en la nube, propiedad de la empresa Apple, lanzado al mercado en octubre del 2012 para los dispositivos con sistema operativo IOS, es decir, iPod, iPhone y iPad; el cual se encarga de almacenar archivos personales de forma gratuita, por ende, conserva contenido multimedia de diversos formatos, no obstante, también se utiliza para guardar copias de seguridad de los dispositivos en cuestión, misma razón que trae consigo diversos inconvenientes [1].

Existen varios aspectos negativos en iCloud en cuanto a la seguridad de la información, tales como; los datos almacenados en este servicio no se encuentran cifrados, es decir, hay riesgos de privacidad, además, cargar archivos en la nube puede resultar en gran consumo de datos, exigiendo la conexión a internet para su funcionamiento y algunas de sus tareas solo se encuentran disponibles si se cuenta con un equipo de Apple [2].

Se realizó una encuesta a usuarios que cuentan con dispositivos IOS que poseen el servicio de iCloud (Ver Anexo 1), determinando que, conocen varias clases de dispositivos con dicho servicio, la mayoría de ellos poseen Apple ID y cuentan con una capacidad de 5 gigas en la nube, así mismo, conocen varios de los servicios iCloud, sin embargo, manifiestan que, han presentado diversos inconvenientes, tales como: problemas para conectarse con iCloud, que el servicio no se sincronice con los datos entre dispositivos, la configuración de iCloud no deja de actualizarse, errores en la autenticación al iniciar sesión y quedarse sin almacenamiento.

A nivel mundial, en la Universidad de Alcalá se realizó el trabajo fin de máster titulado "Análisis de evidencias digitales en la nube", el cual es un estudio detallado para el análisis de evidencias digitales en la nube, empezando con la definición de una serie de conceptos que se asocian con la informática forense, teniendo en cuenta las normas, estándares y herramientas informáticas sobre computación en la nube que existen [3]. El trabajo tiene como objetivo realizar un estudio sobre las implicaciones legales y particularidades metodológicas dentro del proceso de análisis forense digital en la nube; contemplando la definición e implementación de un escenario simulado para un posible caso de ataque, generado a partir de intrusiones indebidas en un proveedor de servicios en la nube [3].

De la misma forma, en Latinoamérica, en la Universidad Nacional de Chimborazo, se presentó el trabajo de titulación "Creación de una guía de recuperación de datos utilizando

la técnica forense File Carving para ordenadores Windows", planteando que es muy importante establecer una guía o mecanismo que indique de forma clara al usuario, la metodología para realizar la recuperación de archivos perdidos, teniendo como problema principal, que actualmente los ordenadores tienen una capacidad alta de procesamiento y almacenamiento de los datos, por esto, se realiza el estudio de todas las actividades relacionadas a la recuperación de datos a través de técnicas forenses, teniendo como resultado, la creación de una guía de recuperación de datos mediante técnicas forenses File Carving, aplicándola positivamente a través de peritos informáticos [4].

Por otra parte, en la Universidad Estatal Península de Santa Elena, se elaboró el componente práctico "Diseño de una guía metodológica para el análisis forense digital tomando como base equipos con el sistema operativo Windows 8.1", conformado por el diseño de la guía en base al sistema operativo antes mencionado, estableciendo el uso de cinco fases principales de la metodología UNE, la cual se considera para el empleo de extracción de evidencias digitales, a través de la designación e implementación de programas de código abierto, mostrando las distintas herramientas que se pueden utilizar y cómo hacerlo, teniendo paso a paso el proceso de creación de una copia del disco duro, recibiendo el nombre de imagen forense, luego realizar el análisis y extracción de evidencia digital [5].

Luego de revisar los trabajos bibliográficos, se concluye que, existen diversos estudios realizados con relación al análisis forense de dispositivos, sin embargo, ninguno está destinado para el servicio de iCloud. Por esta razón, se plantea el presente proyecto, que analizará los servicios iCloud de dispositivos electrónicos con tecnología iPhone, a través de diversas técnicas forenses, con el fin de obtener la mayor cantidad de información.

1.2. Descripción del proyecto

El trabajo de investigación tiene como objetivo realizar un análisis de evidencias digitales iCloud mediante la implementación de laboratorios forenses usando máquinas virtuales y herramientas Open Source de investigación. Para lo cual, se desarrolla un marco conceptual relacionado con conceptos asociados con la computación forense, marco legislativo, y los tipos de servicios disponibles en la nube, tales como SaaS, PaaS y IaaS.

Este estudio se desarrolla utilizando la metodología descriptiva con aplicación de experimentos. Para lo cual, se diseñan e implementan 3 ciberataques en entornos controlados, a fin de realizar el análisis forense de las evidencias digitales. Para garantizar

la integridad de la evidencia y asegurar la veracidad de la investigación forense, este proceso se fundamenta en la aplicación de la norma ISO 27037:2012 para computación forense, y la guía de investigación DoJ 1. Finalmente, los resultados se presentan en un informe detallado incluyendo las particularidades metodológicas de la investigación, y las implicaciones legales de proceso forense digital en la nube.

Fase de identificación del entorno computacional de la nube

En esta fase se va a adherir todo el conocimiento acerca de los entornos cloud para definir conceptos, arquitecturas y modelos para el estudio en ambiente web, como un proceso de informática forense mediante la investigación, demostrando las actuales técnicas forenses, determinando y resolviendo las variedades de problemas a los que se enfrenta.

Se reportará el abuso o uso maligno de periféricos informáticos, procesando la identificación de evidencia, la cual puede ser una imagen de disco duro o archivos de tipo log (de registro) de alguna aplicación de sistema, por esto, la fase se divide en dos secciones, una para identificar el problema y otra para hallar las pruebas.

Fase de colección y preservación

Es la fase principal del proceso forense, teniendo en cuenta que, si ocurre algún error durante esta etapa podría afectar todo el proceso continuo a esta, como la evidencia que es extraída de los dispositivos utilizando un proceso denominado mirroring.

Fase de procesado y análisis

En esta fase, se emplearán las técnicas y herramientas forenses para detectar y extraer datos, sin dejar en evidencia la integridad del dispositivo. En este apartado, si no se logra llegar a una conclusión válida, se deberá regresar a la fase inicial, para esto, se necesitarán las siguientes herramientas:

Herramientas de análisis forense para dispositivos con S.O. Android	
Autopsy	Autopsy es una plataforma forense de código libre, la cual es rápida, fácil de usar y capaz de analizar distintos tipos de medio digitales y dispositivos móviles [6]. Su arquitectura de complementos le permite aumentarlo con módulos desarrollados o personalizados por la comunidad; Además, evoluciona para satisfacer las necesidades de muchos profesionales de la

	seguridad nacional, la fuerza del orden, litigios e investigaciones corporativas [6].
CAINE (Computer Aided Investigate Environment)	CAINE brinda un ambiente completo forense organizado para escanear varias herramientas de software que existen, tales como, módulos de aplicativos y proporcionar una interfaz gráfica amigable para el usuario [7].
DEFT (Digital Evidence & Forensic Toolkit)	DEFT es una de las distribuciones más avanzadas de análisis forense en los últimos años, no solo tiene una cantidad grande de herramientas forenses en su lista, sino que también se sabe adaptar al entorno y mimetizarse [8].

Tabla 1: Herramientas de análisis forense

Fase de diseminación de resultados

En esta fase se lleva a cabo todo el proceso, con el fin, de realizar un informe que describirá los datos obtenidos y el procedimiento mediante el cual se obtuvieron los mismos. Además, se redactará la documentación necesaria, brindando consejos de seguridad para no volver a ser víctima del mismo tipo de ataque.

Este proyecto contribuirá a la línea de investigación Tecnología y Sistemas de la Información (TSI), sub línea de Inteligencia Computacional.

1.3 Objetivos del proyecto

1.3.1 OBJETIVO GENERAL

Diseñar escenarios experimentales de ciberataques en ambientes iCloud utilizando herramientas de computación forense con el fin de reconstruir el ataque, y describir sus implicaciones legales.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar la legislación vigente respecto al desarrollo de un análisis forense en entornos iCloud mediante el ordenamiento de la protección de datos.

- Clasificar las amenazas cibernéticas más comunes que afectan a los servicios iCloud públicos y privados.

- Diseñar tres escenarios experimentales, que permitan describir las características del proceso de adquisición, preservación y análisis de las evidencias digitales en entornos iCloud.

- Elaborar un informe que describa los resultados metodológicos de la investigación forense, e incluya recomendaciones de ciberseguridad para los usuarios finales de estas tecnologías.

1.4 Justificación del proyecto

En la actualidad, el uso de espacio de memorias en las unidades computacionales pasó a ser segundo plano en lo que concierne al almacenamiento de información por el usuario, dando un giro y abriendo nuevas puertas a lo que ahora se conoce como computación en la nube, que permite guardar toda la información en una cloud, siendo indispensable para que grandes compañías formen imperios a base de ella, como Amazon, Google o Microsoft, llamando la atención de sus clientes con espacios gratuitos y limitados [9].

ICloud posee diversas características, tales como: música, videos, fotos, aplicaciones, documentos, notas, IBook y contactos; adicionalmente, sirve como una plataforma de correo electrónico de Apple y sus utilidades, sin embargo, para realizar la auditoria de esta nube se requiere de varios procesos dependiendo del dispositivo que se estará empleando, los cuales incluyen equipos computacionales, tabletas y dispositivos móviles iOS, de igual manera se requiere saber que para la transmisión de estos dispositivos es requerido tener la conectividad móvil activa y en caso de smartphone, el tipo de conexión que abarca desde 3G [10].

Las tecnologías iCloud a diferencia de otras nubes de almacenamiento masivo son mas exclusivas, y van vinculadas directamente con el dispositivo que se usa por medio de una ID de Apple, el cual utiliza un correo exclusivo con su correspondiente contraseña para el acceso, estos recursos van de la mano para sostener una seguridad fuerte al momento de que otra persona quiera realizar un acceso a su nube, pero al igual que cualquier almacenamiento cloud, presenta inconvenientes, los cuales serán los pilares fundamentales para lograr el objetivo de esta auditoría.

El fin de esta auditoria es demostrar las herramientas que se pueden utilizar para realizar el trabajo de investigación de iCloud, afrontando los procesos requeridos para la extracción de datos almacenados en la nube, diagnosticando las entradas y salidas de la información, orientando su entorno hacia el dispositivo que se está trabajando y sobrepasar barreras de seguridad que poseen en cada uno de los espacios con la información requerida.

Este proyecto concluirá con un informe en donde se mostrarán todos los datos obtenidos, los procesos realizados y los resultados que se obtuvieron, de igual forma los errores que se presentaron durante este diagnóstico; describiendo las herramientas con mayor importancia para la auditoria.

El presente trabajo se orienta al plan de oportunidades para cumplir con los requerimientos necesarios, mediante los objetivos del eje social [11]:

Objetivo 7. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos niveles.

Políticas:

7.2 Promover la modernización y eficiencia del modelo educativo por medio de la innovación y el uso de herramientas tecnológicas.

1.5. Alcance del proyecto

Con la problemática expuesta acerca de los dispositivos que manejan iCloud y de sus seguridades en este tipo de almacenamiento en la nube, se puede definir que el estudio ayudará a comprender acerca de la complejidad que conlleva la infiltración a la memoria virtual, con el fin de poder recuperar información perdida y aprender sobre las herramientas que se pueden utilizar para este proyecto forense.

De la misma manera, se determinará cómo trabajan y se vinculan estos dispositivos por medio de la contraseña y pin mediante su ID de registro asignado por la empresa, y a su vez, derivar los diversos equipos tecnológicos que cuentan con esta compañía, debido a su mayor costo de mercado, la información se determinó a través de una encuesta realizada a las personas universitarias que cuenten con teléfonos, tabletas o computadoras que se vinculen a una cuenta iCloud.

El proceso que se llevará en este trabajo, se divide en diversas fases, donde la fase de identificación del entorno computacional de la nube, permitirá adquirir todo el conocimiento acerca de la estructura de la iCloud para definir conceptos como arquitecturas y modelos para un proceso de informática forense mediante la indagación tecnológica, demostrando las actuales técnicas forenses y resolviendo las variedades de problemas que enfrentan. De la misma manera, la fase se divide en dos secciones, una para identificar el problema y otra para hallar las pruebas.

La fase de colección y preservación se denomina como la fase principal del proceso forense, determinando los errores que se presentan durante esta formulación, que podrían afectar todo el proceso continuo a esta, como los datos que se extraen de los dispositivos utilizando un proceso denominado mirroring.

En la fase de procesado y análisis, se emplearán las técnicas y herramientas forenses para detectar y extraer datos, se debe de realizar de una forma minuciosa para proteger la integridad del dispositivo, como dato principal, si no se logra llegar a una conclusión válida, se deberá regresar a la fase inicial. Además, se procurará utilizar las herramientas:

- Autopsy
- CAINE (Computer Aided Investigate Environment)
- DEFT (Digital Evidence & Forensic Toolkit)

En fase de diseminación de resultados se lleva a cabo todo el proceso documentado, con el fin, de realizar un informe que describirá los datos obtenidos y el procedimiento mediante el cual se obtuvieron los mismos. Además, se brindará consejos de seguridad para no volver a ser víctima del mismo tipo de ataque.

Variable

Se pretende encontrar la mayor cantidad de vulnerabilidades en las diferentes estructuras de cloud computing, utilizando la metodología para garantizar la integridad de la evidencia y asegurar la veracidad de la investigación forense, aplicando normas ISO.

1.6 Metodología del proyecto

1.6.1 Metodología de investigación

Se investigaron diversos trabajos bibliográficos similares al presente proyecto de auditoría en iCloud, el cual se centra en extraer información almacenada mediante herramientas Open Source, para indagar sobre los procesos que tienen en la actualidad. Por este motivo, se utiliza la metodología de investigación de tipo exploratoria [12]; dichas investigaciones se emplearán como guía para el desarrollo de esta propuesta.

En la recopilación de trabajos se pudo encontrar temas con orientación adecuada para esta investigación, teniendo en cuenta que, a nivel mundial, en la Universidad de Alcalá se realizó un trabajo titulado "Análisis de evidencias digitales en la nube", en el cual se utilizó herramientas informáticas sobre computación en la nube [3]; por otro lado, a nivel nacional en la Universidad Nacional de Chimborazo se presentó un proyecto de tesis titulado "Creación de una guía de recuperación de datos utilizando la técnica forense File Carving para ordenadores Windows" el cual se basó en guías o mecanismos para la recuperación de archivos perdidos [4], de igual manera de forma local, en la Universidad Estatal Península de Santa Elena se ejecutó un componente práctico denominado "Diseño de una guía metodológica para el análisis forense digital tomando como base equipos con el sistema operativo Windows 8.1", mediante una metodología UNE, se pudo extraer evidencias digitales implementando herramientas de código abierto [5].

Por otro lado, también se aplicó una metodología de tipo diagnóstica [13], para extraer información acerca de los problemas que se suscitan en la nube, tipos de soluciones, métodos de recolección de datos y tipos de dispositivos que usan iCloud.

1.6.2 Técnicas e instrumentos de recolección de datos

Para recolectar información sobre el conocimiento que poseen los usuarios que usan dispositivos con tecnología iCloud en la Universidad Estatal Península de Santa Elena, se empleó una encuesta con un tipo de muestra intencional a 20 estudiantes de la Facultad de Sistemas y Telecomunicaciones de la UPSE (Ver Anexo 1), determinando diversos aspectos que han suscitado los propietarios con respecto a la interacción que realizan en su almacenamiento virtual.

Por medio de las encuestas realizadas, se concluye qué es adecuado realizar una práctica para la extracción de información en la tecnología de almacenamiento en la nube,

orientada a dispositivos con iCloud, con el fin de medir la calidad de servicio y seguridad, siendo un punto esencial como indicador.

1.6.3 Metodología de desarrollo

Para realizar la auditoría en iCloud se estudió el uso de la metodología forense mediante el modelo de Kruse y Heiser, adaptándola para dispositivos IOS donde se enfocarán aspectos técnicos, para obtener los indicadores necesarios para este este proyecto de tesis basados en 4 etapas para preservar y documentar la evidencia que se mostrará como resultado [14].

- **Evaluar:** En donde se obtendrán las autorizaciones adecuadas, se identifica el equipo, se realiza evaluaciones y se adquieren las pruebas.
- **Adquirir:** Para recopilar la información adquirida de los datos como herramientas y sistemas operativos para la auditoría.
- **Analizar:** Se analizan los métodos de extracción de información, como también sus seguridades y el entorno dependiendo del dispositivo.
- **Informar:** Se recopila, organiza y se escribe el informe acerca de la evaluación que se ha obtenido durante todo el proceso.

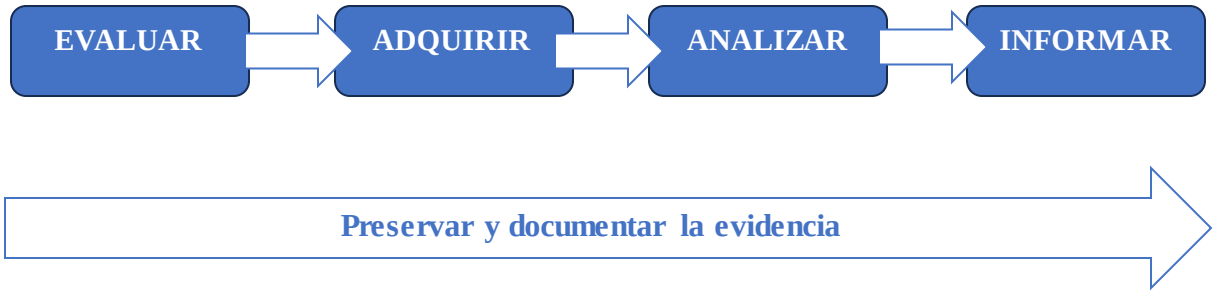


Figura 1: Metodología de desarrollo del proyecto

CAPÍTULO 2. PROPUESTA

2.1. Marco Contextual

2.1.1. CONTEXTO

El análisis forense en entornos ICloud contribuye con las firmas auditoras a detectar fraudes posibles por medio de la identificación de patrones o actividades irregulares en la información almacenada en la nube, permitiendo la verificación de transacciones, garantizando la autenticidad e integridad de los datos, siendo esencial para las mismas. Además, el análisis forense proporciona pruebas sólidas digitales que son admisibles en los tribunales, fundamental para las fiscalías en la construcción de casos legales que se relacionan con fraudes, delitos cibernéticos, acoso virtual u otros hechos delictivos que involucren la evidencia digital.

Por otro lado, facilita el análisis profundo de las evidencias digitales que se almacenan en la iCloud, ayudando a los peritos informáticos a comprender la cronología de los eventos y relaciones entre distintos datos digitales, permitiendo a su vez, la recuperación de datos borrados o perdidos, lo que es crucial para la reconstrucción de eventos, estableciendo la inocencia o culpabilidad en los casos legales.

2.1.2. ANÁLISIS FORENSE EN ICLOUD

Hoy en día, obtener un sistema en la nube o el llamado uso profesional de la computación en la nube es tan común como leer un periódico en línea o interactuar a través de las redes sociales; La nube existe desde hace años, como demuestra el hecho de que grandes empresas como Amazon, Google o Microsoft cuentan con sus propios entornos; términos como SaaS, PaaS, IaaS, local, nube pública, nube privada, híbrida. se han convertido en parte del lenguaje informático común incluso en entornos de usuarios que no son profesionales [15].

Aunque se está implementando a tal escala que a veces la funcionalidad se prioriza sobre todo lo demás, no podemos ignorar el hecho de que todas las nuevas tecnologías conllevan riesgos, y ser demasiado cauteloso significa convertirse en víctima de un incidente de seguridad; Nadie está inmune, y al tratarse de sistemas en la nube a los que se puede acceder directamente desde Internet, el nivel de exposición es mayor; por lo tanto, una mala configuración puede dejar nuestra nueva plataforma abierta a cualquier atacante [15].

Una vez que haya experimentado un ataque y haya logrado contenerlo, es hora de volver a la normalidad y examinar lo sucedido para poder aprender de ello y nunca volver a cometer el mismo error; Durante la respuesta a un incidente de seguridad, lo más importante es restablecer el funcionamiento normal y restaurar el sistema; por lo tanto, es difícil conservar datos para análisis forenses posteriores; La dificultad aumenta cuando consideramos la volatilidad de los datos y el inconveniente de analizar sistemas en la nube que no son exactamente los nuestros y no saber dónde están, fuera de la vista, fuera del contacto [15].

2.1.3. EVOLUCIÓN DEL ANÁLISIS FORENSE

La ciencia forense digital tradicional se considera ampliamente como una de las mejores herramientas para resolver los delitos cibernéticos; con estas tecnologías, se pueden recopilar pruebas y datos de software para ayudar a identificar a los ciberdelincuentes o establecer hechos relacionados con delitos; Mientras estemos en la misma jurisdicción, en el juicio se pueden utilizar pruebas de diferentes análisis. Esta es quizás la mayor diferencia entre la ciencia forense digital tradicional y la ciencia forense en la nube [16].

En el último caso, encontrar pruebas es más complicado porque puede resultar más difícil definir claramente quién es el propietario de las pruebas o qué tribunal puede permitirlas; Como es posible que esta información se almacene fuera de las instalaciones y que esta información se distribuya a diferentes ubicaciones o servidores propiedad de terceros, podemos enfrentar obstáculos legales que dificulten la investigación [16].

En resumen, la ciencia forense en la nube es una evolución de la ciencia forense informática tradicional que enfrenta nuevos desafíos, pero, en última instancia, es necesaria para mantener un mayor nivel de seguridad y herramientas de seguridad en la nube [16].

2.1.4. CLOUD COMPUTING: SITUACIÓN ACTUAL EN ECUADOR

El Índice de Desarrollo de Tecnologías de la Información de Ecuador es de 4,50, muy cercano al promedio mundial, pero aún existe una brecha entre este y los países desarrollados; Este indicador precede que el mercado de servicios TI en Ecuador se está desarrollando, especialmente el mercado de computación en la nube, que ha dejado de estar en pañales en la última década y ha comenzado a desarrollarse rápidamente en todo el territorio [17].

Hasta 2008 en Ecuador, la mayoría de los mercados grandes y medianos administraban su infraestructura de manera "on-premise", incluida la compra de equipos, la inversión en desarrollo de software e infraestructura interna o "on-premise", como aplicaciones y entre 2009 y 2012 surgió la llamada tercera generación de centros de datos: donde la mayoría de los proveedores de servicios de telecomunicaciones (TELCO) y proveedores de servicios de Internet (ISP) optaron por construir centros de datos globales en Ecuador [17].

Desde 2012, los servicios de hosting, virtualización avanzada y nube privada en el país son ofrecidos por el mismo nicho hasta el 2016 y nuevamente desde 2020, hyperscalori ha podido ingresar al mercado ecuatoriano a través de un creciente ecosistema de socios que hace más ágil y rápida la adopción de nuevas tecnologías, especialmente la computación en la nube [17].

Finalmente, analizando la madurez del mercado de computación en la nube en Ecuador, se puede decir que Ecuador sigue siendo un país seguidor, tanto el mercado como los jugadores siguen el camino que otras regiones o regiones ya han tomado; Por tanto, el foco del mercado sigue estando en IaaS, sin una transición exitosa hacia otros enfoques, a pesar de que hay algunos esfuerzos individuales que van más allá; se cree que a medida que los servicios de nube pública sean capaces de satisfacer las necesidades horizontales del mercado ecuatoriano, la madurez sin duda aumentará, pero el enfoque en la inversión y los centros de datos locales disminuirá [18].

2.2. Marco Teórico

2.2.1. INFORMATICA FORENSE Y SEGURIDAD EN LA NUBE

Se integró un desarrollo de consideraciones para la nube privada Own cloud donde utilizo informática forense utilizando técnicas de ingeniería inversa para abordar las vulnerabilidades de seguridad; se utilizaron tres (3) escenarios para cubrir estas consideraciones: DFIR en la nube sin acceso físico, DFIR en la nube con acceso físico, adquisición de imágenes en la nube, donde se utilizan diferentes métodos y herramientas para la adquisición e información de la nube, imagen. /o de la memoria, archivos de registro, etc.; Los medios físicos utilizados son servidores, clientes y teléfonos móviles. La topología de red utilizada es Wi-Fi [28].

Esto se hace creando una topología que simula el entorno real. Para este trabajo se eligió una situación de empresa a cliente (B2C); Por experiencia y conocimiento de

vulnerabilidades se decidió trabajar en servidores y clientes usando el sistema operativo Microsoft y teléfonos móviles usando el sistema operativo Android; Al examinar los resultados en el escenario mencionado anteriormente, se concluyó que la aplicación de estándares y buenas prácticas de seguridad fue efectiva y esencial para reducir las vulnerabilidades de seguridad; Para evitar futuros ataques y/o violaciones de seguridad, las organizaciones y/o usuarios que interactúan con sistemas en la nube requieren atención y capacitación [28].

Brindando como conclusión que los sistemas operativos de Microsoft se encontró vulnerabilidades; Por lo tanto, en términos de parámetros y seguridad del servidor, se recomienda utilizar sistemas operativos de distribución GNU/Linux (Debian, Ubuntu, Mint, etc.); También se recomienda instalar la nube privada usando la consola según la convención de línea de comandos; como alternativa, debido a la falta de conocimientos, también es adecuada una distribución con entorno gráfico [28].

2.2.2. LA NUEVA ERA DE LOS NEGOCIOS: COMPUTACIÓN EN LA NUBE

La computación en la nube no es más que un medio de comunicación, y las empresas, organizaciones y emprendimientos generalmente ven en esta tecnología una solución a sus problemas, tanto en términos de infraestructura técnica como de prestación de servicios, para lograr rentabilidad financiera [29].

A finales de junio de 2010, la consultora de servicios globales Gartner publicó un informe que confirma el asombroso crecimiento de la computación en la nube; Desde la perspectiva del proveedor de servicios informáticos (hardware y software), la mayoría de las grandes empresas como IBM, Microsoft, Oracle, HP, Cisco, etc. han desarrollado estrategias de gestión para proporcionar estos servicios [29].

En este sentido, los operadores de telecomunicaciones europeos (Telefónica, Vodafone, Telcel) y los operadores de telecomunicaciones americanos (ATT, Verizon) cooperan con empresas de Internet que juntas forman parte de la nube. Por ejemplo, Amazon, Google, Yahoo u otras redes sociales (Facebook o Twitter); Tanto las grandes empresas como las pequeñas y medianas empresas están migrando paulatinamente a la nube; No hay duda de que muchos de los que estamos en este grupo usamos la nube cuando enviamos correos electrónicos usando Gmail, Yahoo o Hotmail, podemos escuchar música en Spotify (un servicio de transmisión de audio), ver fotos en Flickr o ver fotos en Flickr; Google Maps tanto en nuestras computadoras de escritorio como en nuestros teléfonos inteligentes.

Todo esto y el uso masivo de almacenamiento en las redes de datos cada vez que utilizamos información de estos servicios [29].

El propósito de este artículo fue analizar descriptivamente de forma documental la transformación de la computación en la nube en un nuevo paradigma tecnológico que ha tenido un enorme impacto a escala global. Se basa en los aportes teóricos de Anderson (2010), Slama, J., Niculcea, A., Cancho, M., Jiménez, M. Ibarra, I., López, E. Corsini, J., Gregsamer, C. (2010), Siegel (2008), Rotaslietas (1997, 2009B, 2011C), etc.; Básicamente, este estudio es un estudio teórico documental, ya que conduce al estudio de la gestión de la nube, el almacenamiento y los servidores de información instalados en los centros de datos; Se centra en cómo almacenar millones de aplicaciones web y grandes cantidades de datos para que grandes organizaciones o empresas con cientos de miles de usuarios puedan descargar y ejecutar aplicaciones directamente y más; Servidores como Google Maps, Gmail, Facebook, etc.; Finalmente, cómo la nube o su procesamiento pueden facilitar una nueva revolución industrial que conduzca a cambios sociales, tecnológicos y económicos masivos [29].

2.2.3. RIESGOS Y AMENAZAS EN CLOUD COMPUTING

Una de las tendencias actuales en el mercado de sistemas de información es la proliferación de servicios basados en la nube, que permiten una distribución dinámica de recursos en función de la demanda de los clientes y reducen costes en infraestructuras críticas; Las "Pautas de seguridad y privacidad para la computación en la nube pública" del NIST (Instituto Nacional de Estándares y Tecnología) publicadas recientemente, además de la idoneidad de este nuevo modelo para la distribución de servicios y aplicaciones, también enfatiza la necesidad de distribución de buenas prácticas. Seguridad del modelo [30].

Este no es el único documento que refleja la creciente preocupación por la seguridad de estas plataformas, y documentos de autoridades de referencia también reflejan esta cuestión; El siguiente informe recopila algunos de estos artículos y tiene como objetivo proporcionar una descripción general de las amenazas, los riesgos y las consideraciones para la seguridad en la nube; Basado en el documento NIST anterior y los últimos informes de la organización, este informe primero describe los tipos de infraestructura y servicios en la nube y luego analiza los diversos elementos que deben considerarse al abordar su seguridad. Firma consultora Gartner [30].

Las preocupaciones expresadas en estos informes se centran principalmente en la gobernanza de datos, principalmente la propiedad de los datos, la forma en que los proveedores de servicios operan y procesan los datos, y la identificación y control del acceso a los recursos [30].

La seguridad y propiedad de los datos es uno de los aspectos clave. El informe plantea serias preocupaciones sobre la propiedad y el procesamiento de datos, ya que estas infraestructuras pueden manejar datos de múltiples países, lo que puede generar conflictos sobre el marco legal para el procesamiento de datos; También se señaló que estos entornos pueden estar expuestos a fugas de información, ya sea intencionalmente o no, porque manejan grandes cantidades de datos [30].

2.3. Marco Conceptual

2.3.1. FORENSE EN LA NUBE

La ciencia forense en la nube, o nube forense, se refiere a la investigación de delitos que tienen lugar principalmente en este entorno, incluye y cubre todos los tipos conocidos de ciberataques, como violaciones de datos o robo de identidad; El buen uso de estas técnicas forenses puede proteger a los propietarios de la información y garantizar mayores niveles de confianza y seguridad en el futuro [16].

Este es un concepto que se presta bien a la informática forense, que se refiere a un conjunto de procedimientos y técnicas que permiten la identificación, recolección, almacenamiento, interpretación y registro (entre otras tareas) de evidencia informática en el momento de un delito. un crimen [19].

2.3.2. NUBE SaaS

El Software como Servicio o Software como Servicio (SaaS) proporciona un producto completo proporcionado por un proveedor responsable de la gestión; En este modelo, no se tiene que preocupar por la infraestructura de la nube ni por saber cómo se mantiene el servicio, solo se tiene que utilizar el servicio, por lo que la única tarea es aprender a utilizarlo; Se puede acceder a estas aplicaciones a través de Internet y desde cualquier dispositivo utilizando un cliente (que puede ser un navegador web), se puede decir que son aplicaciones de usuario final [20].

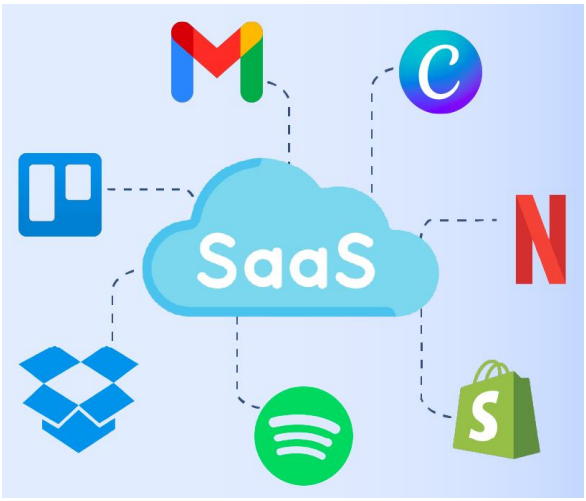


Figura 2: SaaS

2.3.3. NUBE IaaS

La infraestructura como servicio o infraestructura como servicio (IaaS) es utilizada principalmente por administradores de sistemas, proporciona recursos críticos, redes, servidores, almacenamiento y firewalls, todo como un servicio; en este modelo, como cliente, tiene más control sobre el mensaje porque puede implementar y ejecutar el software según sus preferencias; no puede controlar la infraestructura subyacente, pero a partir de la capa de virtualización, tiene control sobre el sistema operativo, el almacenamiento y las aplicaciones; Un ejemplo obvio es cuando se vuelve a implementar una aplicación en una máquina o instancia virtual, por supuesto, un mayor control conlleva una mayor responsabilidad; será responsable de administrar y proteger las máquinas virtuales, instalar parches de seguridad y establecer reglas de acceso [21].

Figura 3: IaaS

2.3.4. NUBE PaaS

La plataforma como servicio o plataforma como servicio (PaaS) es utilizada principalmente por desarrolladores de software; En principio, esto significa otro nivel de abstracción además de IaaS; En este modelo, el proveedor del servicio garantiza el sistema operativo, lenguaje de programación, bibliotecas y herramientas; Es una plataforma completa y extensible, y los desarrolladores sólo deben preocuparse por el código de la aplicación; se debe comprender que con PaaS no puede administrar ni controlar la infraestructura subyacente, incluidas las máquinas virtuales, el sistema operativo y las capas de almacenamiento; Sin embargo, usted tiene control total sobre la aplicación instalada y, en algunos casos, tendrá acceso a ciertos ajustes de configuración del entorno [22].

Figura 4: PaaS

2.3.5. HERRAMIENTA FORENSE

Las herramientas forenses digitales son relativamente nuevas, hasta principios de la década de 1990, la mayor parte de la investigación digital se realizaba mediante análisis en tiempo real, lo que implicaba examinar los medios digitales utilizando equipos adecuados como cualquier otro; A medida que los dispositivos se vuelven más complejos y contienen más información, el análisis sobre la marcha se vuelve engorroso e ineficiente; Con el tiempo, comenzaron a surgir tecnologías gratuitas especializadas en forma de hardware y software que podían filtrar, extraer u observar cuidadosamente datos en un dispositivo sin dañarlo ni modificarlo [23].

2.3.6. IMÁGENES DE DISCO (AUTOPSY)

Autopsy es un software para el análisis forense de imágenes de discos duros. Es una herramienta adecuada para diferentes sistemas operativos como: Linux, Windows, Mac OSx y BSD libre [24].

Fue creado en Perl y actualmente tiene una versión en código JAVA. La plataforma de análisis forense digital es utilizada por gobiernos, entidades públicas y privadas, fuerzas de seguridad como la policía y el ejército, profesionales y expertos en informática para investigar lo que sucedió en una computadora después de un incidente (como un ataque o falla) en un intento de recuperar. archivos o buscar por acciones del sistema [25].

2.3.7. KALI LINUX

Kali Linux es una distribución de Linux basada en Debian especialmente diseñada para diversos temas de seguridad como análisis de redes, ataques inalámbricos, análisis forense y otros temas que mencionaremos más adelante. Tiene las herramientas para realizar todas estas pruebas y análisis de seguridad [26].

Muchas personas en la industria de TI utilizan distribuciones de Linux para realizar su trabajo y tareas diarias. Otros perfiles como Crackers también juegan un papel importante; En las noticias y medios casi siempre usan la palabra "hacker" cuando en realidad solo se refiere a una persona con conocimientos de programación y "hackers" son aquellos que utilizan estos conocimientos con fines nefastos. Lo más importante es utilizar la información vendiéndolo en la Deep web o a terceros [27].

Figura 5: Kali Linux

CAPÍTULO 3. PROPUESTA

3.1. REQUERIMIENTOS

3.1.1. REQUERIMIENTOS FUNCIONALES

Código	Especificación de requerimientos
RQ01	Recolectar información, mediante una encuesta a los estudiantes, utilizando la escala de Likert en la elaboración de las opciones de respuesta.
RQ02	Obtener información acerca de las infraestructuras de cloud computer, para determinar un análisis de estudio.
RQ03	Identificar el grado de conocimiento de los estudiantes, con respecto a las seguridades que establecen las diferente nubes y características.
RQ04	Emplear la metodología de análisis forense adecuada, para estas arquitecturas propuesta en el proyecto.
RQ05	Seleccionar e identificar las plataformas que implementan cloud, para determinar técnicas adecuadas de análisis, aplicándolas en el presente estudio investigativo.
RQ06	Aplicar un laboratorio forense, mediante técnicas computacionales seleccionadas por cada tipo de cloud.
RQ07	Utilizar técnicas forenses, para capturar imágenes y extraer información en plataformas con infraestructura IaaS.
RQ08	Determinar mediante gráficos estadísticos los resultados de la encuesta, para tener información acerca la documentación que los usuarios poseen en estas infraestructuras.
RQ09	Crear un informe de las técnicas utilizadas por cada tipo de infraestructura, para constatar de qué manera se extrajo la información, abarcando un análisis completo de los datos obtenidos.
RQ10	Elaborar una guía sobre el uso seguro de cloud computing y buenas prácticas en entorno de seguridad.
RQ11	Instalar el sistema operativo Kali Linux en una máquina virtual y las herramientas adecuadas de los repositorios estudiados, para el laboratorio forense y así poder ejecutar las diferentes extracciones de información.
RQ12	Utilizar diversos dispositivos para el almacenamiento de la información obtenida.

RQ13	Realizar tablas de control que detalle la práctica realizada y los resultados obtenidos.
RQ14	Ejecutar las pruebas de manera adecuada para los diferentes entornos.
RQ15	Crear los ataques en base a reconocimiento de estudios realizados, dependiendo del ambiente de la infraestructura, sin alterar los archivos extraídos.

Tabla 2: Requerimientos

3.1. SIMULACIÓN DE ATAQUES EN SERVICIOS ICLOUD

En el presente proyecto de técnicas forense a servicios ICloud, se describirán los pasos a seguir para elaborar los diferentes laboratorios para los 3 casos de estudios. Se determina que estos procesos se ejecutarán de manera virtual en una computadora portátil, la cual cuenta con sistema operativo Windows 10, con disco duro de 2T y memoria Ram de 32 gigas, las cuales serán distribuidas por los diferentes SO de la máquina host, tomando en consideración que, con una PC con especificaciones inferiores, este trabajo también se desarrollaría, dependiendo de los recursos destinados para cada caso.

Al orientarse en un entorno virtual, uno de los recursos esenciales para un buen rendimiento es la capacidad de memoria RAM. En este proyecto que conlleva 3 casos, se ejecutarán 4 máquinas distintas, de la cuales se inicializarán de dos en dos al mismo tiempo; se recomienda como mínimo una PC que tenga 8 GB de RAM para su entorno.

En la siguiente esquematización, se determina de manera simple como estará estructurado este laboratorio para cada caso.

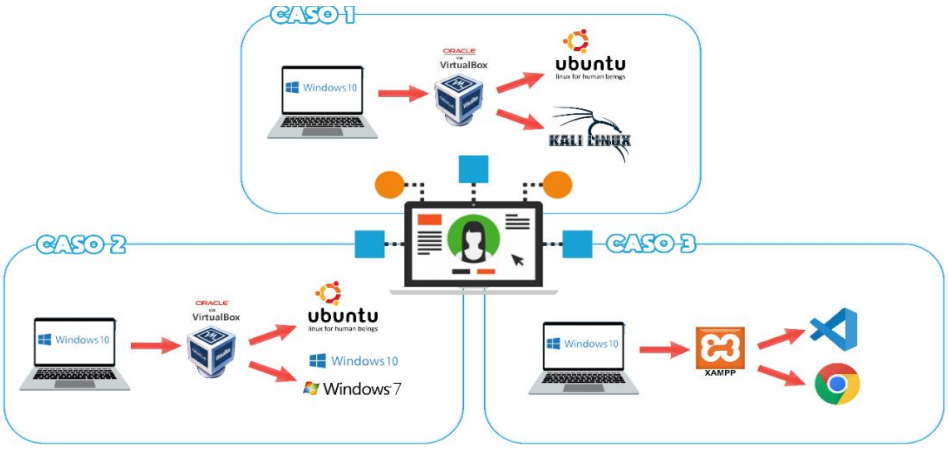


Figura 6: Esquematización

Para la conformación de estos laboratorios, se debe de tener en cuenta que es necesario la instalación de ciertos sistemas operativos, servidores y una máquina virtual para realizar estos casos:

Laboratorio		
Virtualización:	Oracle VM VirtualBox	Anexo 2
Caso	**Software**	**Nº de Anexo**
Caso 1 	Ubuntu	Anexo 4
	Kali Linux	Anexo 3
Caso 2 	Ubuntu	Anexo 4
	Windows 7	Anexo 5
Caso 3 	Xampp	Anexo 6
	Visual code	Anexo 7

Tabla 3: Laboratorio

3.2. IDENTIFICACIÓN DE INCIDENTES Y ANÁLISIS FORENSE

En este apartado se describe a detalle cómo se aplicó el método al caso descrito anteriormente, teniendo en cuenta cada uno de los pasos enumerados y descritos en el apartado previo.

3.2.1. CASO 1 – DENEGACIÓN DE SERVICIOS

Adquisición de evidencias

En este caso, al remitente del aplicativo web víctima se le envían varios paquetes de datos con IP en modo ramdom, en grandes cantidades y gran tamaño para colapsar la página web y produzca un volcado (Anexo 8).

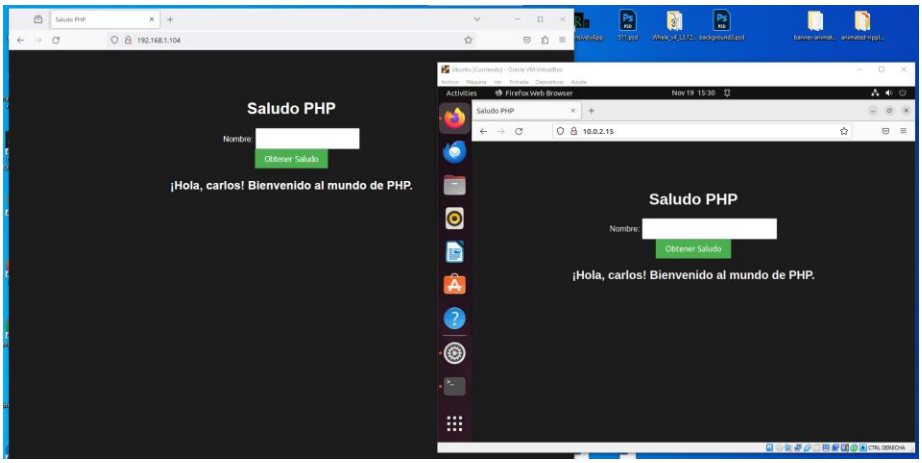


Figura 7: Página web creada

En la imagen anterior, se puede ver la aplicación web que se creó para la práctica, intentando un volcado de memoria y saturar la memoria de este servidor web donde se aloja, exponiéndose a que la página web se vuelva inestable, lenta o sin acceso en el momento de una actualización.

Figura 8: Prueba de volcado de memoria

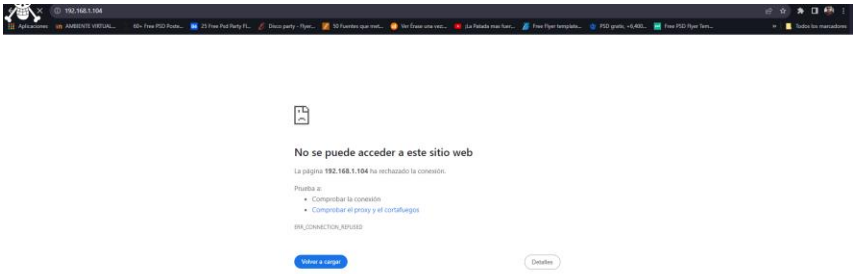


Figura 9: Prueba de saturación de la memoria

Del ataque anterior, se pueden ver los resultados mediante htop y Wireshark, mostrando la cantidad de ataque que se generan y las IP falsas de cada paquete.

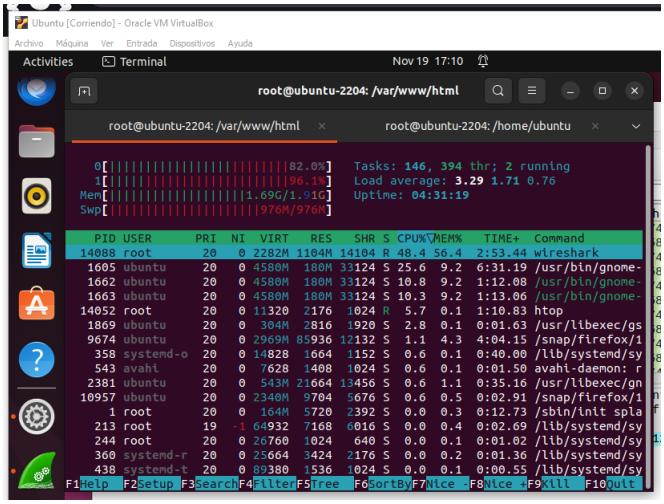


Figura 10: Resultados htop

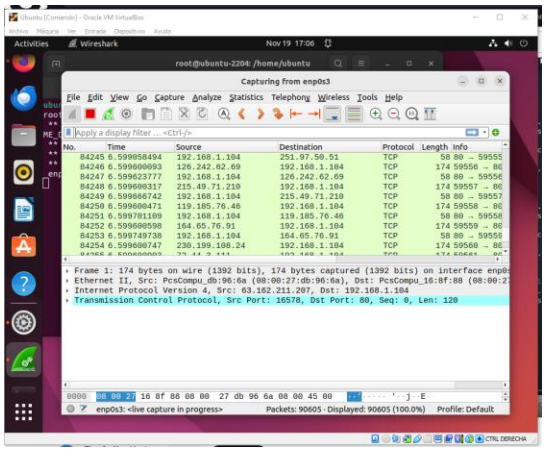


Figura 11: Resultados Wireshark

Preservación de evidencia

Generación de código Hash

En este punto se descargan los datos del análisis de los diferentes ataques, utilizados para generar su hash y así revisar su estructura. Con la ayuda de funciones hash, puede comprobar la exactitud de los documentos, por lo que es importante hacerlo también en estudios relacionados. Con el software QFileHasher, se debe ubicar el archivo que se descargó antes de poder continuar generando el código.

Una vez encontrado el archivo, se abre en el software correspondiente para generar un código que permita entender la autenticidad del archivo, obteniendo así un código hash para cada archivo procesado por el software. Para crear cada hash, se selecciona el archivo deseado y presiona el botón "Iniciar", el cual dará la información que se necesita para continuar con los pasos a continuación. Los procedimientos técnicos para la obtención de los valores hash se describen en las figuras adjuntas correspondientes a cada caso.

El propósito de este paso es usar QFileHasher para obtener el hash codificado SHA1 de este experimento para obtener los siguientes caracteres que pertenecen a este archivo:

Análisis de evidencias

Una vez obtenida la información y preservada la evidencia relevante, el siguiente paso es realizar un análisis para identificar las mismas que se obtuvieron del atacante. Durante este proceso, es importante utilizar el software presentado en la investigación para hallar adecuadamente: tipos, IP y otros datos que revelen la identidad del atacante. El siguiente proceso se utiliza para cargar un archivo TCP que se va a analizar. Es importante resaltar que este proceso es el mismo para todos los tipos maliciosos analizados.

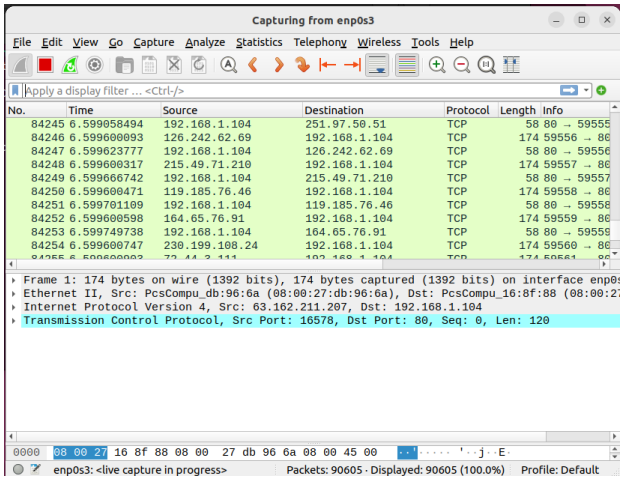


Figura 12: Análisis de evidencias

En donde se identifica el tipo de archivo y la IP atacante de los paquetes recibidos durante el proceso.

```
84245 6.599058494   192.168.1.104     251.97.50.51      TCP      58 80 → 59555
84246 6.599600093   126.242.62.69     192.168.1.104     TCP     174 59556 → 80
84247 6.599623777   192.168.1.104     126.242.62.69     TCP      58 80 → 59556
84248 6.599600317   215.49.71.210     192.168.1.104     TCP     174 59557 → 80
84249 6.599666742   192.168.1.104     215.49.71.210     TCP      58 80 → 59557
84250 6.599600471   119.185.76.46     192.168.1.104     TCP     174 59558 → 80
84251 6.599701109   192.168.1.104     119.185.76.46     TCP      58 80 → 59558
```

Figura 13: Identificación del tipo de archivo

Buscando la direccion de la IP de una TCP en páginas de ubicación, se determinó que no se encuentra la IP establecida.

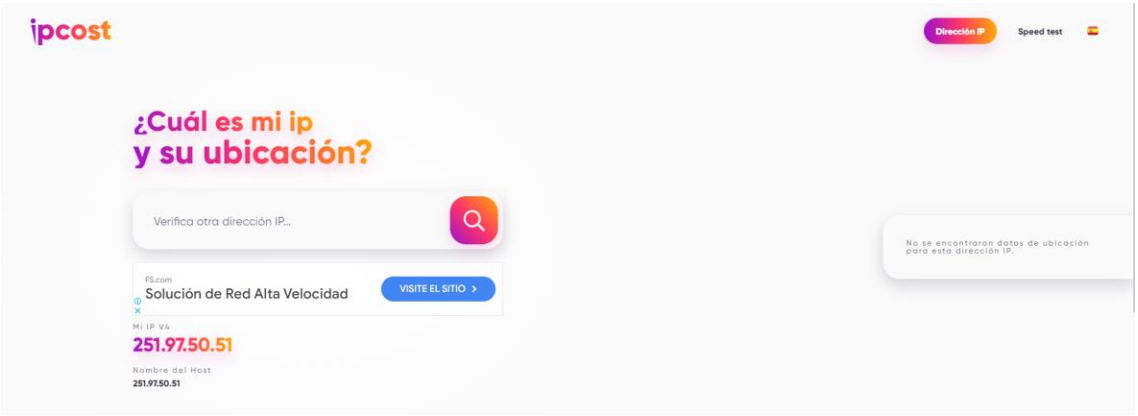


Figura 14: Dirección IP

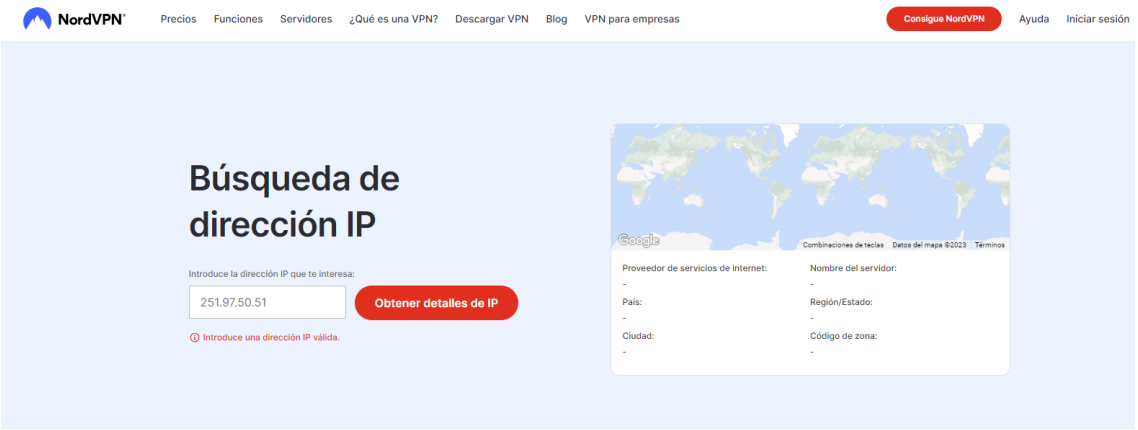


Figura 15: Búsqueda de dirección IP

Entre los otros análisis que se realizan al instante, se encuentra el htop, que muestra los paquetes de entrada en tiempo real.

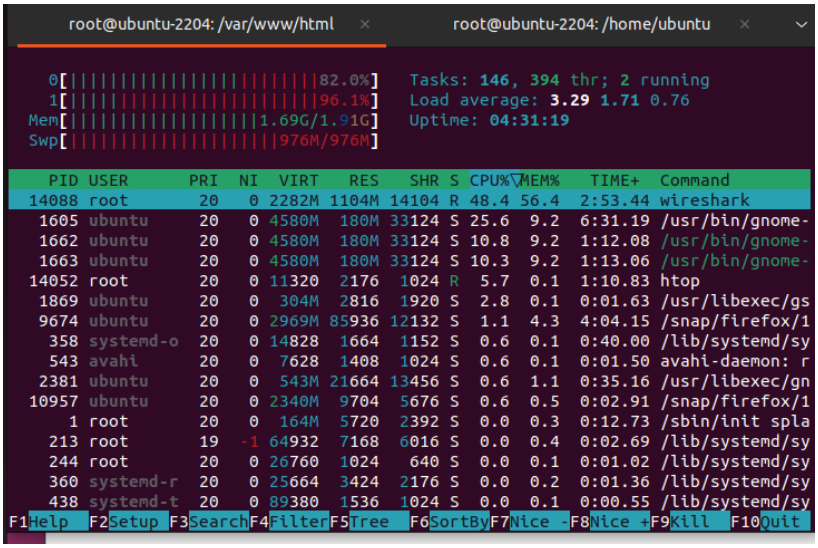


Figura 16: Análisis htop

Documentación y reportes

En esta etapa, se elabora un informe con opiniones y conclusiones sobre la evidencia obtenida para cada caso analizado; información relevante para esta sección, la cual estará seccionada en el (**Anexo 11)**.

3.2.2. CASO 2 – INFECCIÓN DE MALWARE

Adquisición de evidencias

En este segundo caso, se practicó un ataque de un rasonware hacia un sistema de archivos alojado en windows, y que como servidor está en red con otros equipos de linux, los cuales se encargarán de monitorear las acciones de este virus y poder hallar informacion acerca del mismo (**Anexo 9**).

Figura 17: Adquisición de evidencias

En la imagen de arriba, se puede ver el momento en que el virus ha atacado el sistema de archivos de windows, mientras tanto el sistema operativo linux se mantiene la detección de los datos infectados en esta práctica.

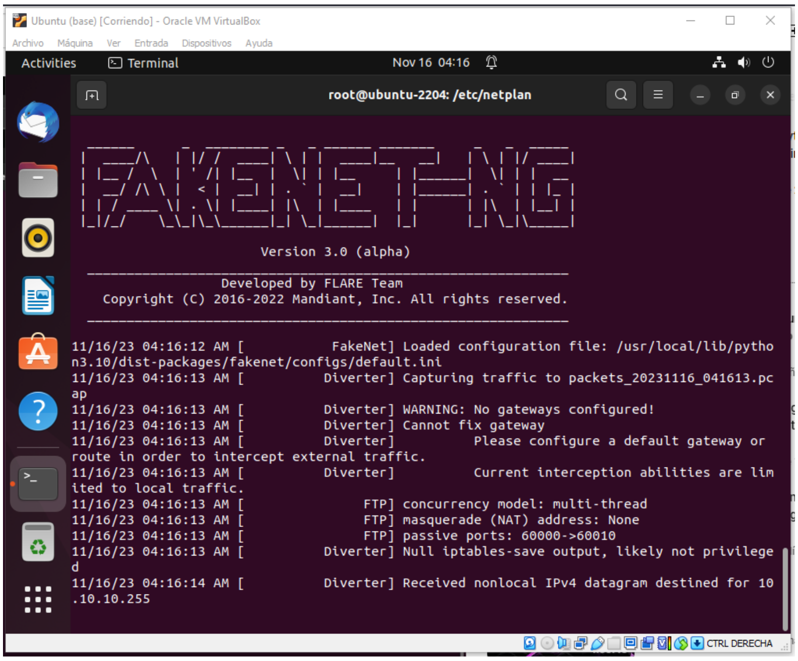


Figura 18: Extracción de datos

Del ataque realizado, se extrajeron datos pertinentes a los que enviaba este Malware para luego analizarlos, teniendo en cuenta que este tipo de datos están encriptados en base 64.

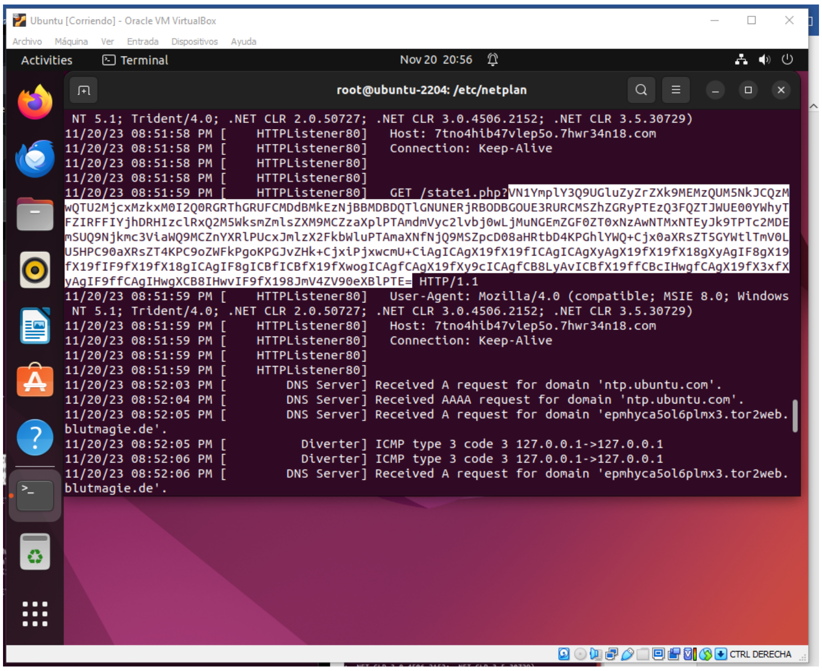


Figura 19: Análisis de datos extraídos

Preservación de evidencia

Generación de código Hash

En este punto, se copian los enlaces Get del análisis de los diferente ataques, los cuales se utilizan para desencriptar archivos de base 64 y se pueden comprobar la exactitud de las fuentes dadas, por lo que es importante que se debe copiar el nombre completo de los enlaces que se descargaron.

Una vez desencriptado el archivo, se busca mediante páginas correspondientes para identificar la dirección y su origen, permitiendo entender la autenticidad del link encontrado. Para analizar esta base 64, escribiendo la dirección deseada y presionando el botón "Iniciar", el cual dará la información necesaria para continuar con los pasos a continuación.

El propósito de este paso es usar QFileHasher para obtener el cifrado de el link que se obtuvo y poder comprender como actúa este tipo de ataque.

Análisis de evidencias

Una vez obtenida esta informacion del enlace extraido, el siguiente paso es realizar un análisis para identificar las evidencia, su origen y hacia donde dirige si se realiza el proceso que se está solicitando. Durante estos indicios de decodificación, se utilizaron varias páginas de internet, es importante tener en cuenta que este tipo de sitios de internet ayudan a verificar hacia donde te redirigue el enlace que se crea internamente para investigar e identificar adecuadamente las intenciones del atacante.

Figura 20: Análisis para identificación de evidencias

Al reconocer el estado de cuenta del Big coin encontrado se puede percatar que la función de este virus es crear una cuenta en Big Coin nueva para que el pago por el rescate de archivo sea único, haciendo irrastreable el origen.

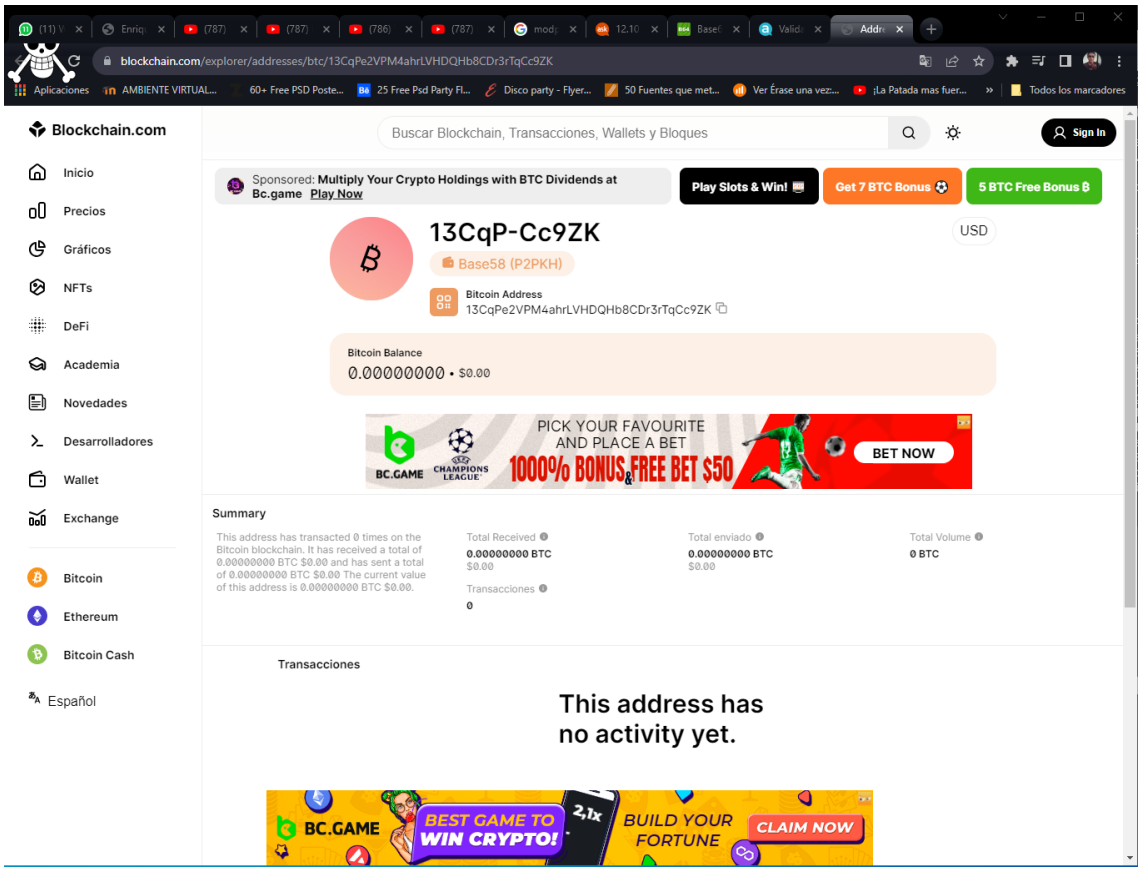


Figura 21: Big Coin

Documentación y reportes

En esta etapa se elabora un informe con opiniones y conclusiones sobre la evidencia obtenida para cada caso analizado; información relevante para esta sección, la cual estará seccionada en el (**Anexo 11**).

3.2.3. CASO 3 – DEFACEMENT

Adquisición de evidencias

En este último caso se utilizará la tecnica defacement para realizar una clonación de página, en este ejemplo el Index.php y cambiarle la apaciencia para luego volverla a arrancar como un ataque al sitio (**Anexo 10**).

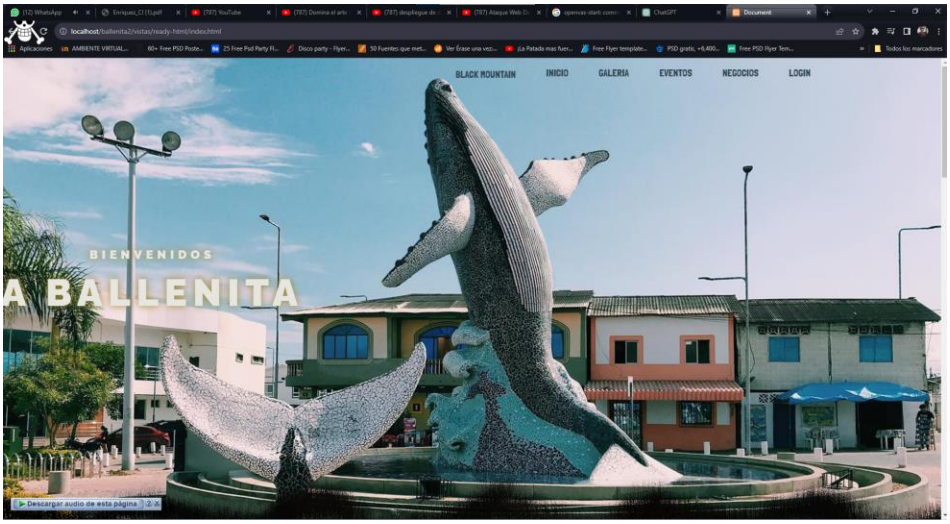


Figura 22: Clonación de página web

En la imagen anterior, se puede ver la aplicación web que será la víctima para el ataque y que mediante codificación en visual code studio se le cambiará de entorno a esta página web.

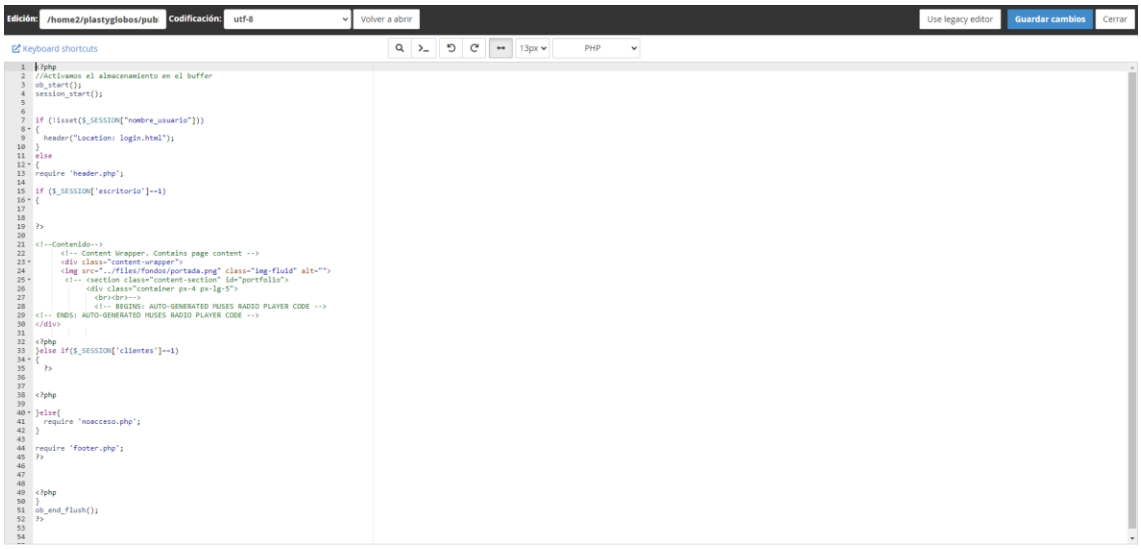


Figura 23: Arranque de la página

Una vez realizados estos cambios, se envía a arrancar esta página mediante el servidor Xampp, apreciando la nueva apariencia de la página, mostrando que ya están siendo atacados.

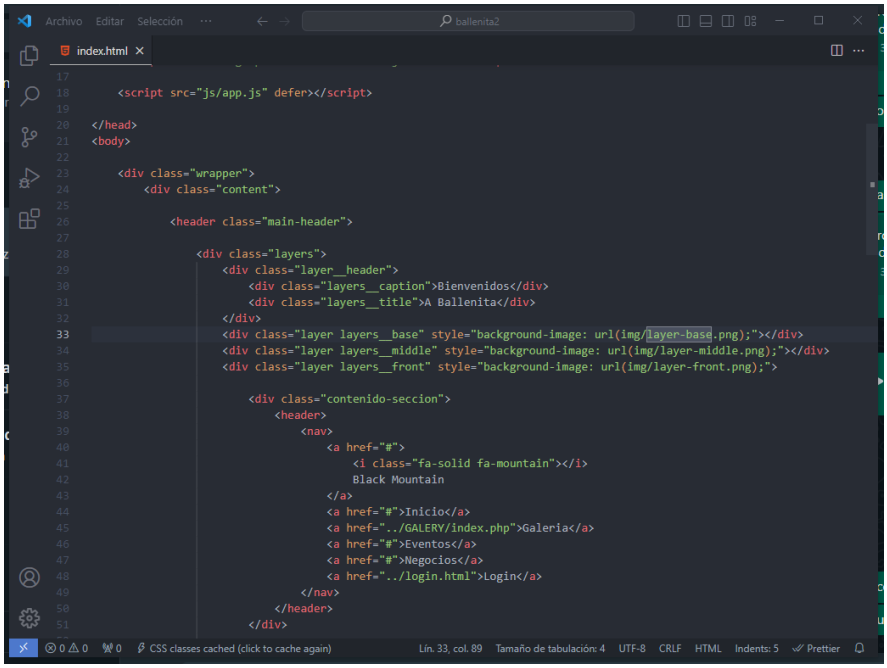


Figura 24: Codificación

Figura 25: Resultado del ataque

Documentación y reportes

En esta etapa, se elabora un informe con opiniones y conclusiones sobre la evidencia obtenida para cada caso analizado; información relevante para esta sección, la cual estará seccionada en el (**Anexo 11)**.

CAPÍTULO 4. RESULTADOS

4.1. Población

Teniendo en cuenta que la población es un conjunto de individuos que reúnen las características necesarias que se pretenden estudiar, se establece que este trabajo se conforma por una población infinita, ya que, se desconoce la cantidad de personas. Es decir, es imposible determinar el número de usuarios que utilizan dispositivos con iCloud.

4.2. Muestra

El muestreo que se va a aplicar en este proyecto es de tipo intencional, siendo una técnica en la cual la persona investigadora se basa en su propio juicio para escoger los integrantes que conformarán el trabajo. Tomando en consideración esto, se elige a 20 personas para aplicar la encuesta diseñada con el fin de conocer sobre los dispositivos con tecnología iCloud.

4.3. Resultados de la encuesta realizada a usuarios que utilizan dispositivos con iCloud

El objetivo de esta encuesta es analizar el conocimiento que poseen los usuarios que usan dispositivos con tecnología iCloud; para esto se realizó esta técnica de recolección a 20 individuos.

1. **¿Cuántas clases de dispositivos con iCloud conoce?**

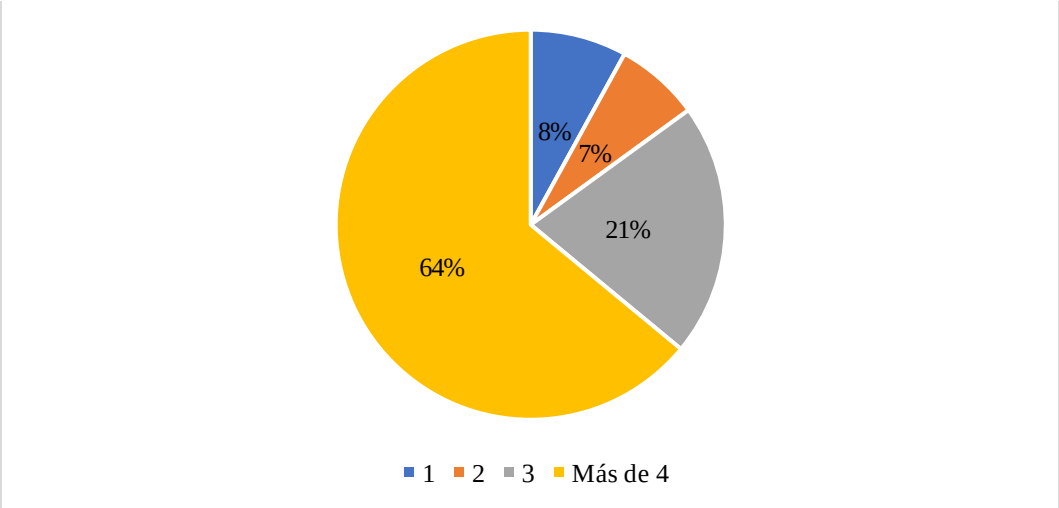


Figura 26: Clases de dispositivos iCloud

El 64% de la población encuestada conoce más de 4 dispositivos que poseen iCloud, el 21% sabe de 3 dispositivos, el 8% está al tanto de 1 clase de dispositivo y el 7% conoce dos tipos.

2. ¿Cuenta con Apple ID en su dispositivo?

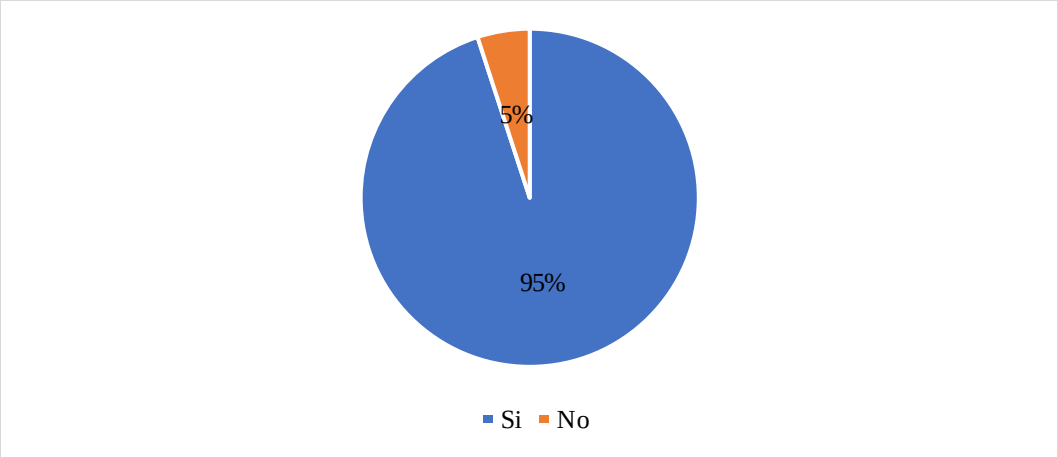


Figura 27: Apple ID

El 95% de la población encuestada cuenta con Apple ID en su dispositivo, mientras que, el 5% no poseen esta cuenta.

3. ¿Con cuánta capacidad de la nube cuenta?

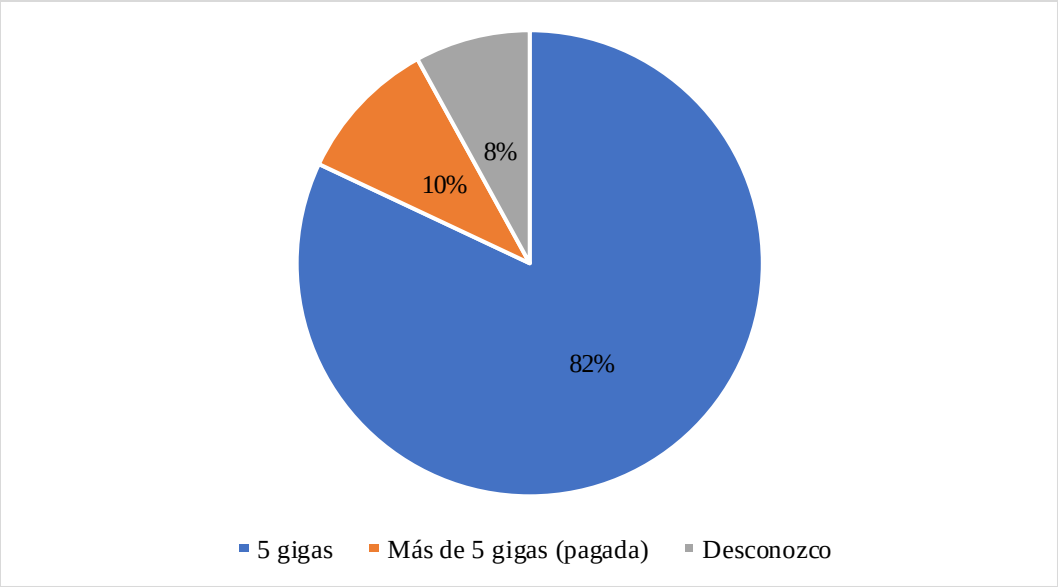


Figura 28: Capacidad de la nube

El 82% de los encuestados tienen una capacidad de 5 gigas en la nube, mientras que, el 10% posee más de 5 gigas pagadas y el 8% desconoce la capacidad.

4. **¿Cuántos servicios de los que brinda iCloud conoce?**

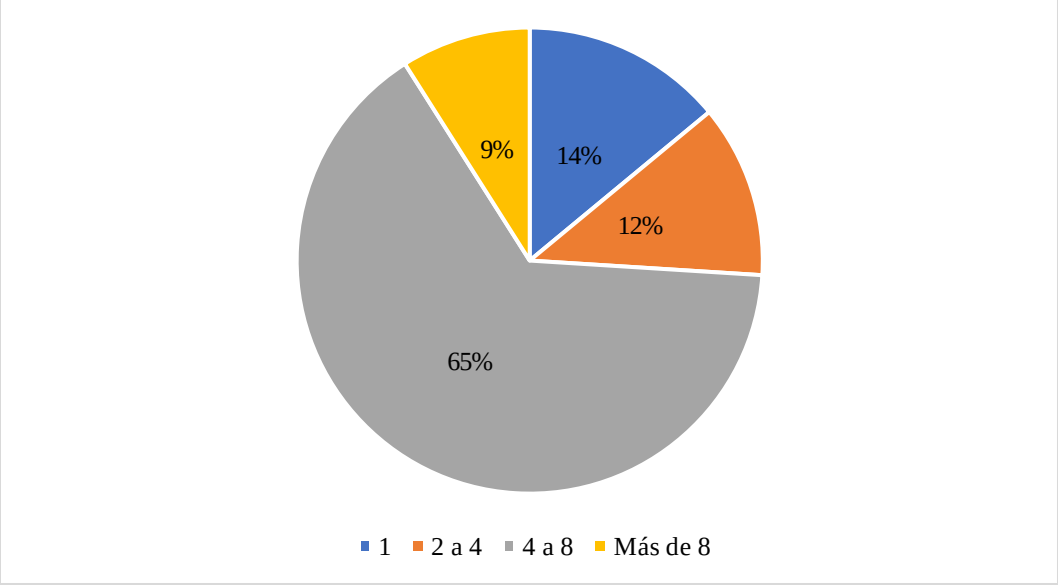


Figura 29: Servicios que brinda iCloud

El 65% de la población encuestada conocen entre 4 a 8 servicios que brinda iCloud, mientras que, el 14% sabe de un solo servicio, el 12% conoce de 2 a 4 y el % sabe más de 8 servicios que ofrece la nube.

5. **¿Ha tenido algún problema con el inicio de sesión en su dispositivo?**

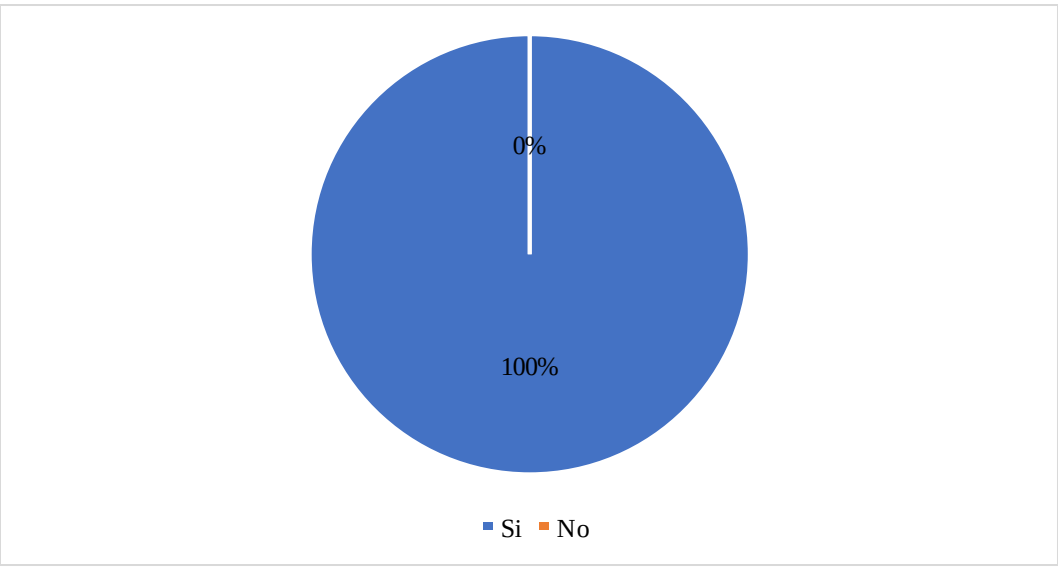


Figura 30: Problemas con el inicio de sesión

El 100% de los encuestados manifiestan que si han tenido problemas con respecto al inicio de sesión en su dispositivo.

6. ¿Con qué frecuencia ha tenido este tipo de errores?

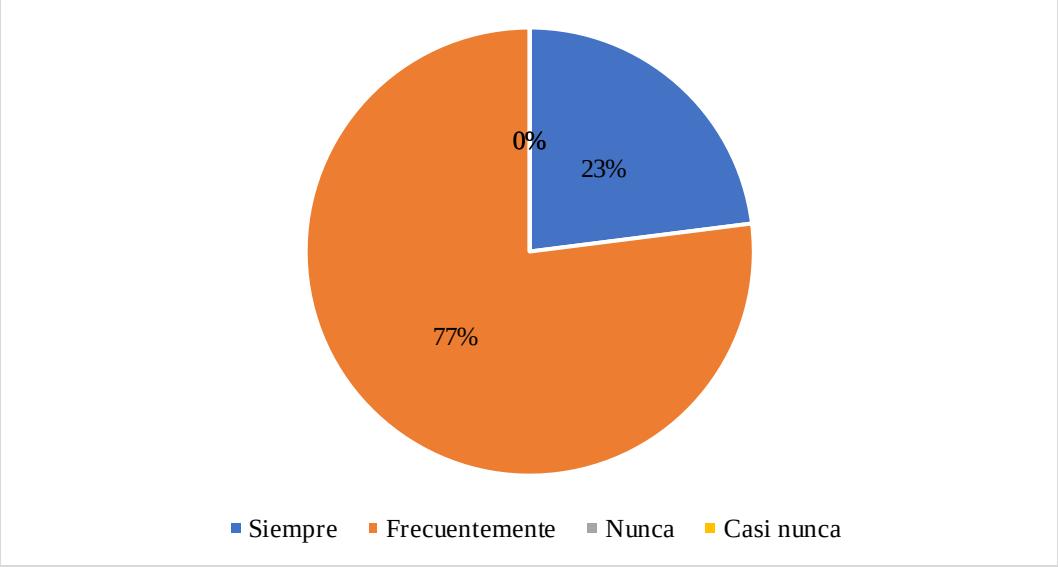


Figura 31: Frecuencia de errores

El 77% de la población encuestada frecuentemente ha tenido este tipo de inconvenientes en el inicio de sesión en su dispositivo, mientras que, el 23% presenta siempre esta clase de errores.

7. ¿Ha pagado alguna vez por un servicio de Apple?

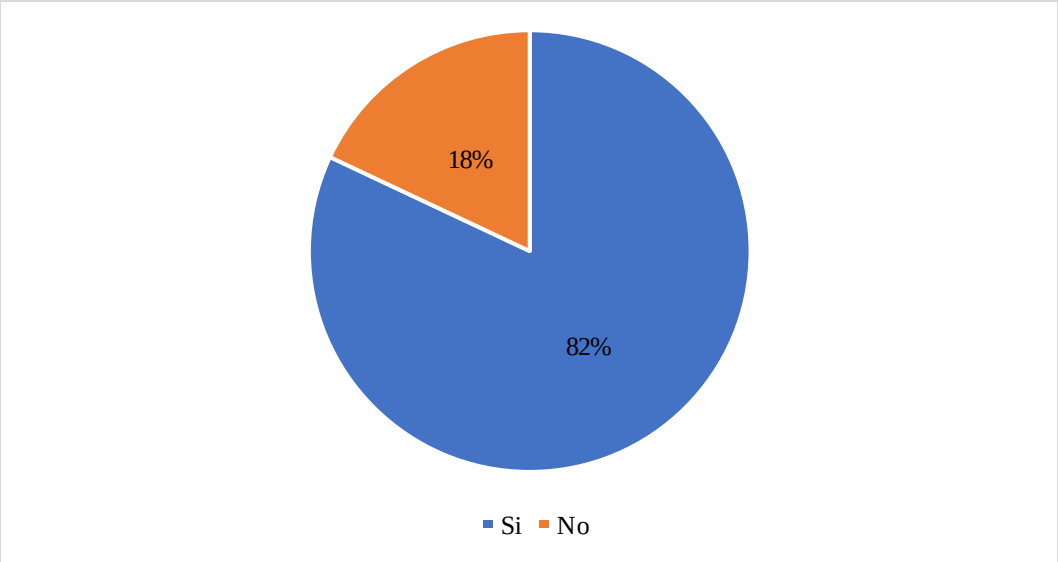


Figura 32: Servicios de Apple

El 82% de los encuestados si han pagado en alguna ocasión por un servicio de Apple, sin embargo, el 18% no lo han hecho.

8. Aproximadamente, ¿Cuánto tiempo de uso ha tenido con estos dispositivos?

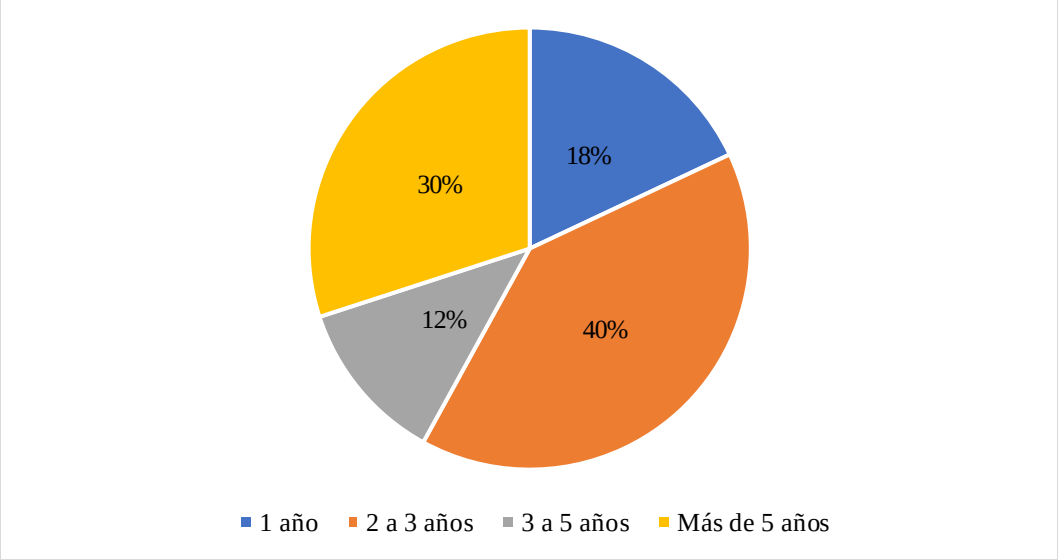


Figura 33: Tiempo de uso de dispositivos

El 40% de la población encuestada ha utilizado de 2 a 3 años estos dispositivos, mientras que, el 30% los ha usado por más de 5 años, el 18% ha manejado por un año esta clase de dispositivos y el 12% ha empleado los mismos de 3 a 5 años.

4.1. Estándares para gestionar la seguridad del servicio cloud

A continuación, se muestra una tabla de comparación de los estándares ISO en donde se encontrarán términos y contenido que los proveedores de servicios Cloud deben cumplir:

ISO 27001

El objetivo de la norma ISO 27001 es garantizar que las organizaciones comprendan los riesgos asociados con la gestión de la información y emprendan, reduzcan y gestionen los riesgos a través de procesos documentados, sistemáticos, estructurados, eficaces, repetibles y adaptables, para hacer frente a las posibles modificaciones que puedan derivarse de los riesgos de medio ambiente y tecnología.

ISO 27701

Se propone introducir un Sistema de Gestión de Privacidad de la Información (SGPI) para aplicar políticas y controles que protejan los datos personales de la empresa tanto desde

el punto de vista del responsable del tratamiento (Data Controller) como del encargado del tratamiento.

Cuando se habla de responsable del tratamiento, se refiere a una persona física o jurídica, pública o privada, que determina diversos aspectos del tratamiento de datos personales, como su finalidad y uso o duración.

ISO 27017

ISO 27017 es un estándar de seguridad que brinda control a los clientes y proveedores de servicios en la nube, su importancia radica en la precisión con la que define la relación entre el cliente y el proveedor de servicios en la nube, determinando qué puede pedir el cliente y qué información debe proporcionar el proveedor de servicios.

El cumplimiento de estas pautas permite mejorar la seguridad de la red y la gestión de servicios en términos de arquitectura, medidas de seguridad, funcionalidad disponible, tecnologías de cifrado y geolocalización de datos.

ISO 27018

La norma ISO 27018 describe buenas prácticas para los servicios en la nube (en relación con los controles de protección de datos), especialmente para los proveedores de servicios.

Su objetivo principal es establecer estándares, procedimientos y controles que los proveedores de servicios (como "procesadores de datos") deben aplicar. Además, garantiza el cumplimiento de las disposiciones reglamentarias sobre el tratamiento de datos personales.

ISO 27032

La ISO 27032, que se considera un nuevo estándar que se centra en la ciberseguridad, ya que es uno de los mayores riesgos que enfrentan las empresas en todo el mundo.

En este sentido, si bien existe una norma ISO 27001 que se enfoca en la seguridad de la información, la Organización Internacional de Normalización decidió formular principios específicos para la seguridad de la red para brindar a las empresas una mayor protección y soporte.

"El ciberespacio es un entorno complejo que consiste en interacciones entre personas, software y servicios destinados a difundir información y comunicación en todo el

mundo". Al presentar la norma, el organismo ISO afirmó que se trata de un contexto muy amplio: "La cooperación es importante para garantizar un entorno seguro". En resumen, el objetivo principal de esta ISO es proporcionar orientación para garantizar interacciones seguras en el complejo entorno del ciberespacio.

4.1. Buenas prácticas para la implementación de la arquitectura Cloud Computing

Gestionar y administrar la arquitectura de la computación en la nube puede ser una tarea bastante desafiante porque la arquitectura de la computación en la nube es compleja y detallada. Sin embargo, para asegurar su eficacia y eficiencia, su ejecución debe realizarse correctamente.

Es importante definir claramente los requisitos a cumplir, cuáles son los objetivos marcados por la organización, los recursos necesarios para realizar la tarea sin errores y la funcionalidad requerida.

Otro aspecto importante de la implementación de la arquitectura en la nube es elegir la plataforma adecuada. Un servicio que cuenta con las mejores y necesarias características para el trabajo empresarial y una variedad de servicios de hosting para simplificar la gestión del tiempo y la carga de trabajo.

La arquitectura debe ser escalable para que pueda adaptarse fácilmente a los cambios en el negocio y el entorno general. El rendimiento de la nube también debe monitorearse para identificar problemas de rendimiento que puedan resolverse, mejorar continuamente la eficiencia de los recursos y garantizar la seguridad de los datos almacenados y las conexiones de los usuarios en todo momento.

CONCLUSIONES

- El análisis de la legislación vigente fue primordial para garantizar la legalidad y ética en la presente investigación forense de los entornos Cloud estudiados; comprendiendo dichas leyes de protección de datos, se proporcionó una base sólida para el manejo de la evidencia digital, asegurando que el proceso cumpla con las normativas y estándares pertinentes.

- Se clasificaron las ciber amenazas más comunes en los entornos Cloud públicos y privados, siendo crucial para identificar los riesgos posibles y desarrollar estrategias efectivas de seguridad, comprendiendo las amenazas más comunes, con el fin de implementar medidas preventivas y adecuadas para proteger la integridad de la información almacenada en la nube.

- Se diseñaron escenarios experimentales, simulando condiciones del entorno real en la nube, logrando una comprensión profunda de los procesos de adquisición, preservación y análisis de las evidencias digitales, ajustándolas según sus debidas complejidades.

- La elaboración del informe detallado describiendo los resultados metodológicos de la investigación forense, proporcionó información precisa y clara acerca de los ataques empleados, así como recomendaciones que fortalezcan la seguridad, fomentando las prácticas correctas en el uso de dichos servicios.

RECOMENDACIONES

- Se debe establecer un equipo multidisciplinario, incluyendo expertos en las leyes de protección de datos y tecnologías de la información, garantizando la aplicación efectiva de medidas de seguridad con requisitos legales para análisis digital forense en los entornos Cloud.

- Es recomendable mantener un sistema de monitoreo constante de vulnerabilidades y amenazas específicas en los entornos Cloud, implementando herramientas avanzadas de detección, además de estar al día con las nuevas amenazas, permitiendo una adaptación rápida de estrategias seguras.

- Incorporar más casos experimentales de entornos Cloud, abordando distintas configuraciones y ataques, asegurando que las metodologías desarrolladas sean adaptables y robustas a diferentes contextos.

- Ampliar la guía de recomendaciones de ciber seguridad, adaptadas al público objetivo, implementando nuevas medidas seguras frente a posibles ataques en los entornos Cloud.

REFERENCIAS

[1] Apple, «Introducción a iCloud,» 2023. [En línea]. Available: https://support.apple.com/es-es/guide/icloud/mm74e822f6de/icloud.

[2] Apple, «Resolver problemas entre iCloud para Windows o iTunes y el software de seguridad de terceros,» 2023. [En línea]. Available: https://support.apple.com/es-co/HT201413.

[3] J. L. Narbona Moreno, «Análisis de Evidencias Digitales en la Nube,» Alcalá, 2021.

[4] L. F. Borja Brito, «Creación de una guía de recuperación de datos utilizando la técnica forense File Carving para ordenadores Windows,» Riobamba, 2021.

[5] F. J. Mirabá Quimí, «Diseño de una guía metodológica para el análisis forense digital tomando como base equipos con el sistema operativo Windows 8.1,» La Libertad, 2021.

[6] B. LLC, «Autopsy,» Autopsy, 2023. [En línea]. Available: https://www.autopsy.com/. [Último acceso: 11 04 2023].

[7] CAÍN.E., «CAINE Computer forensic linux live distro,» Linux, 2023. [En línea]. Available: https://www.caine-live.net/. [Último acceso: 11 04 2023].

[8] Dragonjar, «DEFT (Digital Evidence & Forensic Toolkit),» Dragonjar, 2023. [En línea]. Available: https://www.dragonjar.org/deft-digital-evidence-forensic-toolkit.xhtml. [Último acceso: 11 04 2023].

[9] Ó. Perez y I. Mora López, «Introducción al análisis forense en entornos 'cloud',» red seguridad, 28 10 2020. [En línea]. Available: https://www.redseguridad.com/especialidades-tic/cloud-y-virtualizacion/introduccion-al-analisis-forense-en-entornos-cloud_20201028.html. [Último acceso: 18 06 2023].

[10] K. K. Rada Jimenez, «HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL ORIENTADAS A INFRAESTRUCTURAS TI COMO MEDIO DE

INVESTIGACIÓN EN DELITOS INFORMÁTICOS,» UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD, Barrancabermeja, 2022.

[11] Ecuador, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf.

[12] N. Morales, «Investigación Exploratoria: Tipos, Metodología y Ejemplos,» 2023.

[13] M. L. H., «Diplomado en Metodología de la Investigación - Investigación diagnóstica descriptiva y explicativa».

[14] W. Kruse II y J. Heiser, «Computer Forensics,» Lucent Technologies, Indianapolis, 2002.

[15] Ó. P. Pérez y I. Mora Lopez, «Introducción al análisis forense en entornos 'cloud',» red Seguridad, 28 10 2020. [En línea]. Available: https://www.redseguridad.com/especialidades-tic/cloud-y-virtualizacion/introduccion-al-analisis-forense-en-entornos-cloud_20201028.html. [Último acceso: 25 09 2023].

[16] F. Fuentes, «Análisis forense en cloud: ¿qué es y en qué consiste?,» Arsys, 07 11 2022. [En línea]. Available: https://www.arsys.es/blog/analisis-forense-cloud#:~:text=El%20an%C3%A1lisis%20forense%20en%20cloud,o%20los%20robos%20de%20identidad. [Último acceso: 25 09 2023].

[17] D. Zambonino, «Cloud Computing: Situación Actual en Ecuador,» 2022.

[18] D. Zambonino, «Cloud Computing: Situación Actual en Ecuador — Nube Pública en Ecuador — Análisis,» 09 03 2022. [En línea]. Available: https://davidzambonino.medium.com/cloud-computing-situaci%C3%B3n-actual-en-ecuador-nube-p%C3%BAblica-en-ecuador-an%C3%A1lisis-100ec762aac. [Último acceso: 29 09 2023].

[19] DigitoForense, «Cómo la nube complica la escena del crimen digital,» 08 09 2020. [En línea]. Available: https://www.digitoforense.cl/noticias/cloud-computing/como-la-nube-complica-la-escena-del-crimen-digital/.

[20] F. Flores, «Cloud Computing: Tipos de nubes, servicios y proveedores,» OpenWebinars, 22 03 2021. [En línea]. Available: https://openwebinars.net/blog/tipos-de-cloud-computing/. [Último acceso: 25 09 2023].

[21] Google Cloud, «Qué es IaaS,» 2023. [En línea]. Available: https://cloud.google.com/learn/what-is-iaas?hl=es.

[22] RedHat, «Qué es una PaaS,» 26 08 2022. [En línea]. Available: https://www.redhat.com/es/topics/cloud-computing/what-is-paas.

[23] ciberseguridad, «HERRAMIENTAS Y SOFTWARE PARA ANÁLISIS FORENSE DE SEGURIDAD INFORMÁTICA,» ciberseguridad, 24 09 2022. [En línea]. Available: https://ciberseguridad.com/servicios/analisis-forense/software/. [Último acceso: 25 09 2023].

[24] J. Guzman, «Plataforma de análisis forense para imágenes de discos duros (Autopsy),» backtrackacademy, 27 11 2022. [En línea]. Available: https://backtrackacademy.com/articulo/plataforma-de-analisis-forense-para-imagenes-de-discos-duros-autopsy. [Último acceso: 25 09 2023].

[25] Sleuth Kit, «Autopsy,» 2023. [En línea]. Available: https://www.sleuthkit.org/autopsy/.

[26] R. Altube, «Kali Linux: Qué es y características principales,» openwebinars, 05 11 2021. [En línea]. Available: https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/#:~:text=Kali%20Linux%20es%20una%20distribuci%C3%B3n,pruebas%20de%20seguridad%20y%20an%C3%A1lisis.. [Último acceso: 29 09 2023].

[27] Kali, «Kali Linux,» 2023. [En línea]. Available: https://www.kali.org/.

[28] P. Croci, «INFORMATICA FORENSE Y,» Universidad Fasta, Buenos Aires, 2022.

[29] I. Orozco y J. Odina, «LA NUEVA ERA DE LOS NEGOCIOS: COMPUTACIÓN EN LA NUBE,» Telematique, Venezuela, 2019.

[30] INTECO-CERT, «RIESGOS Y AMENAZAS EN CLOUD COMPUTING,» 2019.

[31] E. Nuñez Soto, «Investigación forense de dispositivos móviles: metodologías y herramientas,» red seguridad, 21 10 2020. [En línea]. Available: https://www.redseguridad.com/especialidades-tic/activos-de-informacion/investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html. [Último acceso: 18 06 2023].

[32] C. Ramos Galarza, Los alcances de una investigacion, Quito: CiencIAmerica, 2020.

[33] D. Ortiz Negrin, EL MODELO INCREMENTAL PARA EL DESARROLLO DE UN SISTEMA INFORMÁTICO DE GESTIÓN DE INFORMACIÓN, Granma-Cuba: Centro Universitario Municipal de Media Luna de la Universidad, 2020.

ANEXOS

Anexo 1. Encuesta realizada a usuarios que utilizan dispositivos con iCloud

	Universidad Estatal Península de Santa Elena **Facultad de Sistemas y Telecomunicaciones** **Carrera de Tecnologías de la Información**
Encuesta dirigida a los usuarios que utilizan dispositivos con iCloud	
Objetivos: Analizar el conocimiento que mantiene los usuarios que usan dispositivos con tecnología iCloud.	
1.	**¿Cuántas clases de dispositivos con iCloud conoce?** **1___ 2____ 3____ más de 4_____**
2.	**¿Cuenta con Apple ID en su dispositivo?** **Sí____ No_____**
3.	**¿Con cuanta capacidad de la nube cuenta?** **5 gigas___ +5 Gigas(pagada)____ Desconozco_____**
4.	**¿Cuántos servicios de los que brinda iCloud conoce?** **1___ 2 a 4___ 4 a 8___ más de 8_____**
5.	**¿Ha tenido algún problema con el inicio de sesión en su dispositivo?** **Sí____ No____**
6.	**¿Con qué frecuencia ha tenido este tipo de errores?** **Siempre____ Frecuentemente_____ Nunca_____ Casi nunca____**
7.	**¿Ha pagado alguna vez por un servicio de Apple?** **Sí____ No_____**
8.	**Aproximadamente, ¿Cuánto tiempo de uso ha tenido con estos dispositivos?** **1 año___ 2 a 3 años___ 3 a 5 años___ Más de 5 años_____**
Resumen:	Recolección de información para determinar el uso de dispositivos con tecnología iCloud en diversos usuarios.
Responsable:	Pita Vera Carlos Adrián.

Anexo 2. Instalación de VirtualBox

Para descargar VirtualBox, visita su sitio web oficial y haz clic en el botón grande "Descargar VirtualBox", que te llevará a la sección de descargas. Una vez allí, haga clic en "Hosting de Windows" para descargar el instalador, luego haga clic en "Todas las plataformas compatibles" para descargar el paquete de expansión (VirtualBox Expansion Pack).

Figura 34: Página oficial de VirtualBox

Abra el archivo de instalación .exe de la carpeta de descarga y haga clic en Siguiente para iniciar la instalación.

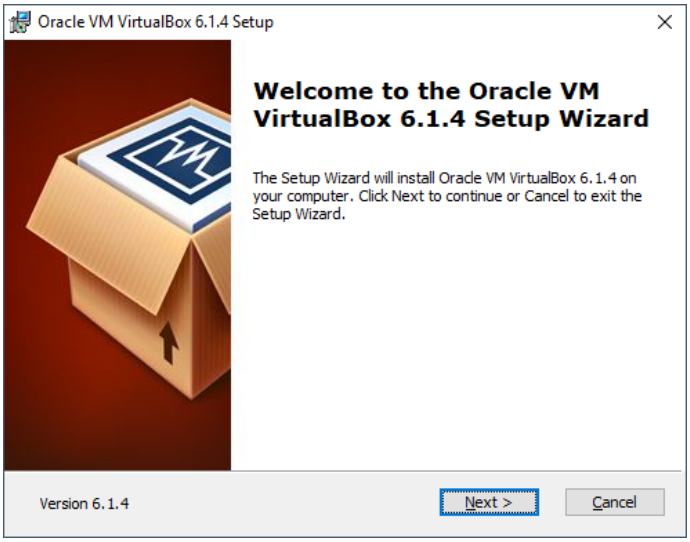


Figura 35: Instalación de VirtualBox

Seleccione los componentes que desea instalar y haga clic en Siguiente para instalar el software en la ubicación predeterminada. También puede cambiar la carpeta de destino.

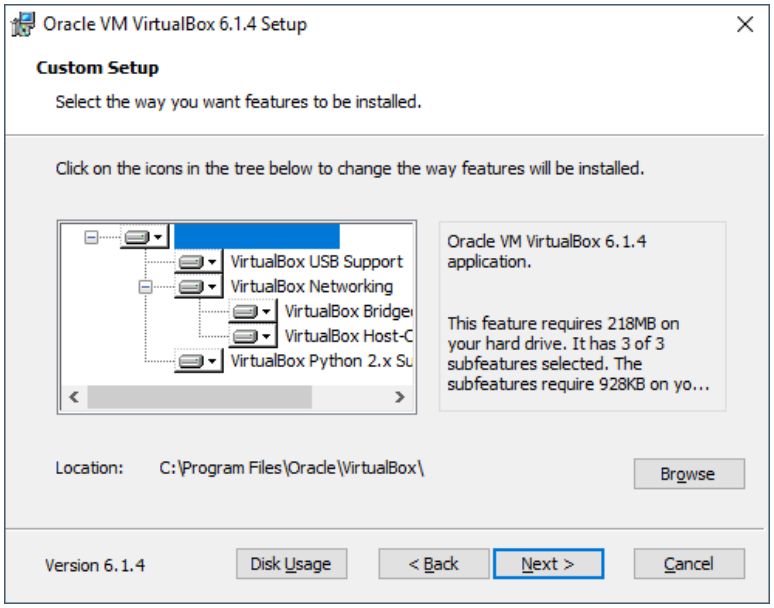


Figura 36: Componentes a instalar

Seleccione el acceso directo que desea crear y haga clic en Siguiente. Haga clic en "Sí" para continuar.

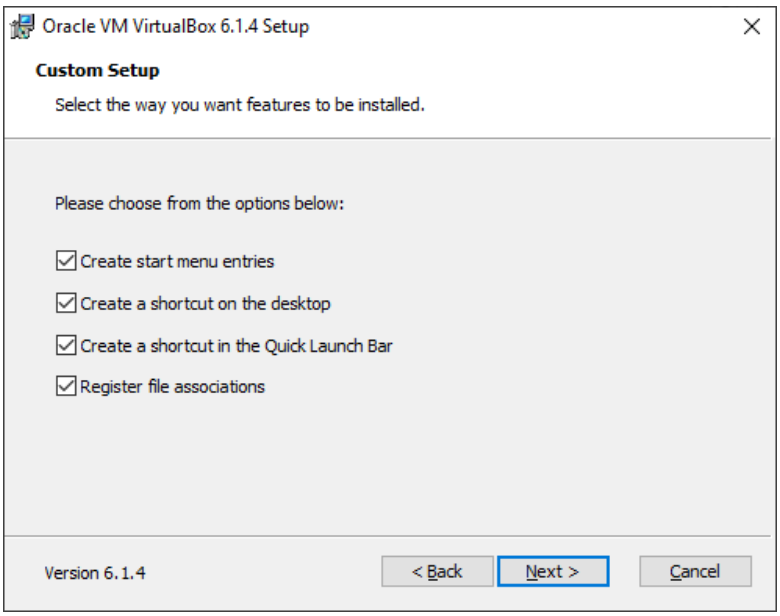


Figura 37: Selección del acceso directo

Haga clic en "Instalar" para iniciar la instalación.

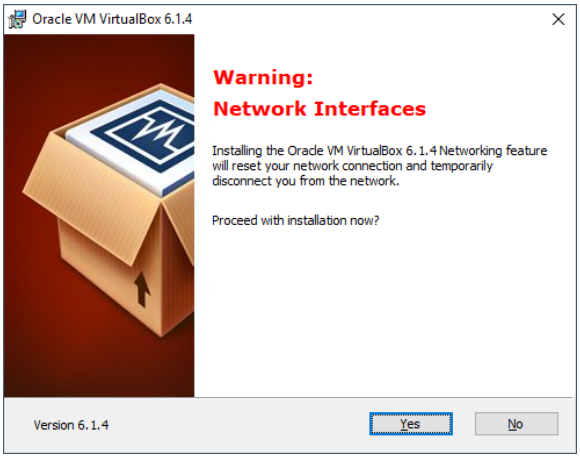


Figura 38: Instalar

Haga clic en Instalar cuando se le solicite.

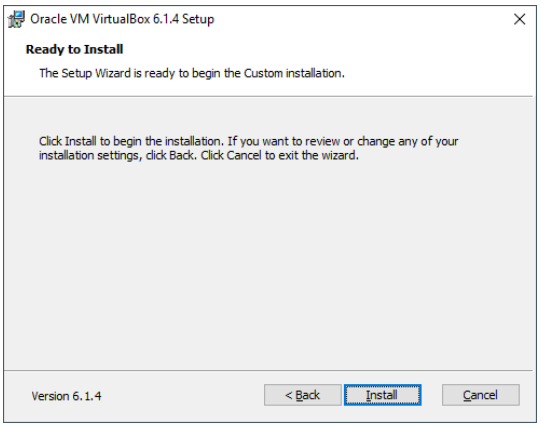


Figura 39: Aceptar la instalación

Esto comenzará a instalar VirtualBox en su computadora.

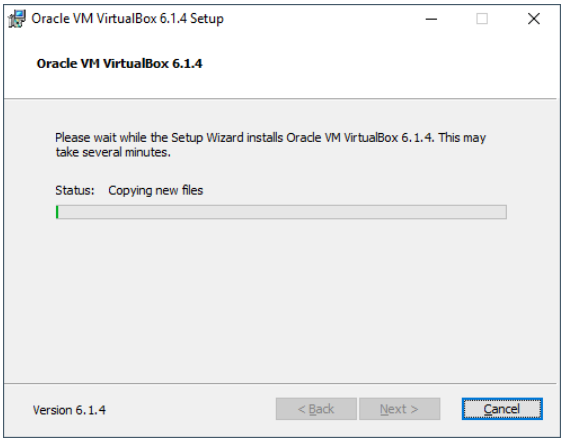


Figura 40: Culminación de la instalación

Cuando se complete la instalación, marque la casilla para ejecutar el programa y haga clic en Finalizar.

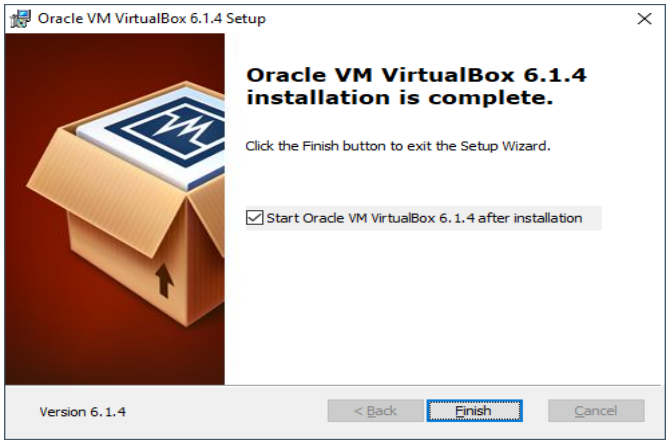


Figura 41: Ejecutar el programa

El programa está instalado y listo para usar.

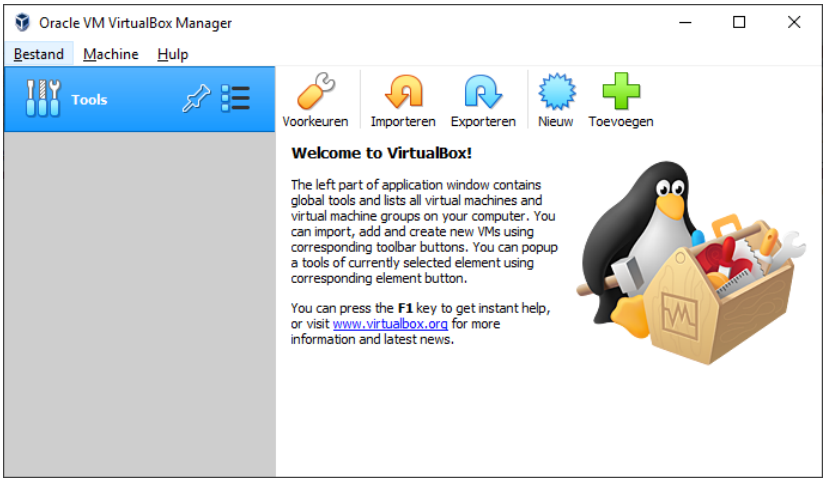


Figura 42: VirtualBox instalado

Anexo 3. Instalación de Kali Linux

Se requieren dos cosas para iniciar el proceso, primero el hipervisor, en este caso será VirtualBox y la imagen ISO de Kali Linux para continuar con la instalación.

- Usaremos VirtualBox versión 7.0 que se puede descargar desde este enlace.
- También usaremos la última versión de Kali Linux de 64 bits versión 2022.2.

Cuando esté todo listo, abrimos VirtualBox y hacemos clic en "Máquina -> Nueva" en la pantalla de inicio para comenzar a crear esta máquina virtual, se recomienda hacer clic en el botón "Modo Experto" a continuación para acceder a todas las opciones de configuración de la máquina virtual.

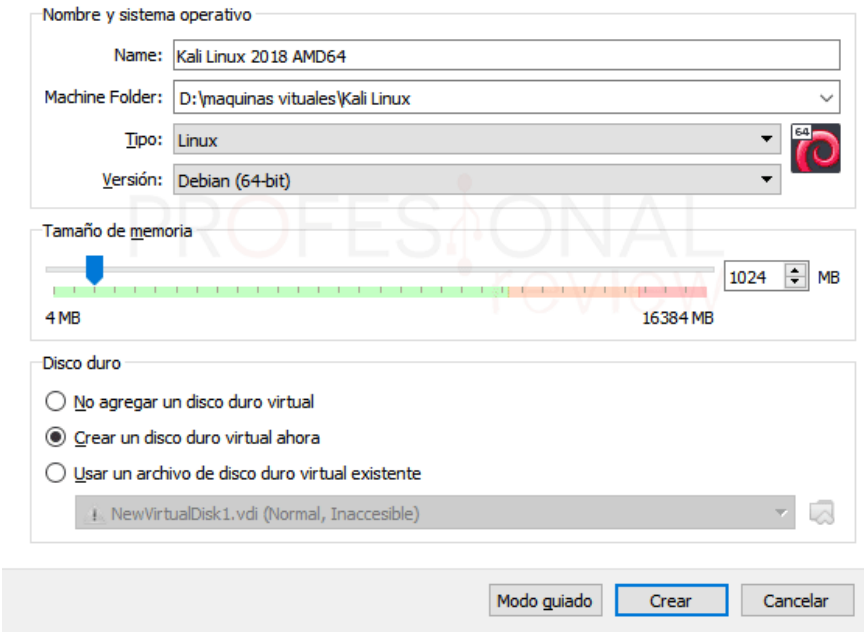


Figura 43: Nueva máquina

Se da un nombre y seleccionamos Linux como tipo de sistema y Debian (64 bits) como versión, ya que nuestro sistema está basado en Debian. También colocaremos la cantidad de RAM, usaremos la memoria mínima requerida que es 1024 MB, pero si hay más memoria insertar al menos 2 GB.

Finalmente seleccionamos "Crear un disco duro virtual ahora" porque la máquina virtual se creará desde cero. Cuando hayamos terminado y todo esté como queremos, haga clic en "Crear".

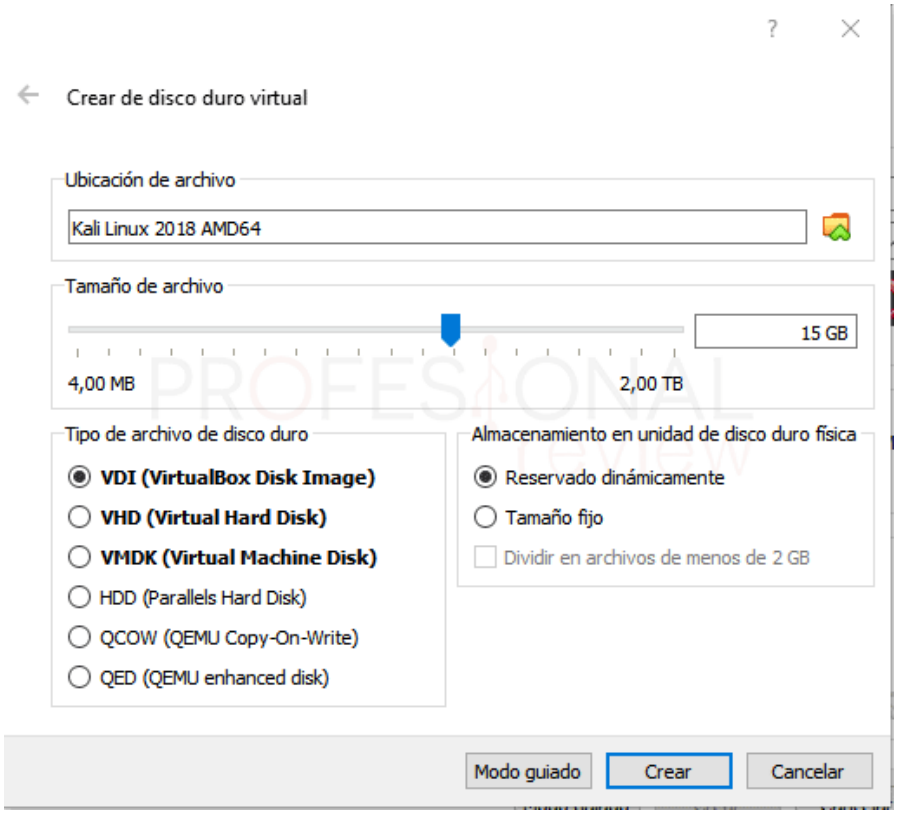


Figura 44: Creación de disco duro virtual

En la siguiente pantalla, debemos seleccionar la ubicación de almacenamiento del disco duro virtual usando un espacio mínimo de 15 GB, se recomienda que, si tienes pensado utilizar el sistema de forma activa, elijas más espacio para no quedarte corto, al menos 25 GB.

En cuanto al formato del disco duro virtual, lo reservaremos como VDI por defecto y elegiremos "Reserva dinámica", así el espacio real de nuestro disco duro se asignará dinámicamente según el número de veces que se utilice. Cuando haya terminado, haga clic en Crear.

Configuración de Kali Linux

Antes de instalar el sistema operativo, debemos seleccionar nuestra imagen ISO y colocarla en una unidad virtual para que se pueda instalar el sistema, haciendo clic en la máquina virtual creada y seleccionamos la opción "Configuración".

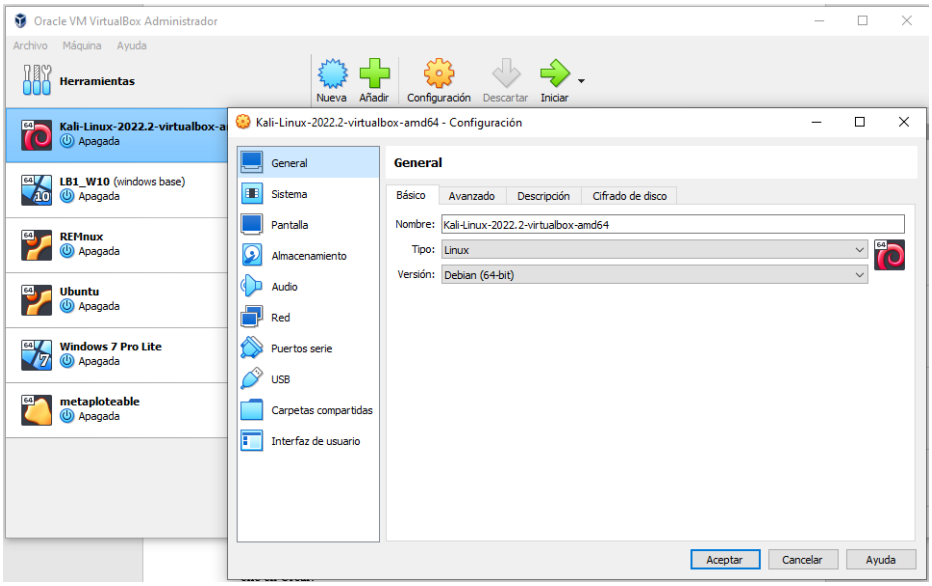


Figura 45: Seleccionar imagen ISO

El primer cambio que se hizo es eliminar el disquete de la lista de inicio en "General", ya que no se utilizará en absoluto y en principio no necesitamos habilitar la opción EFI en la BIOS, porque sólo traerá problemas.

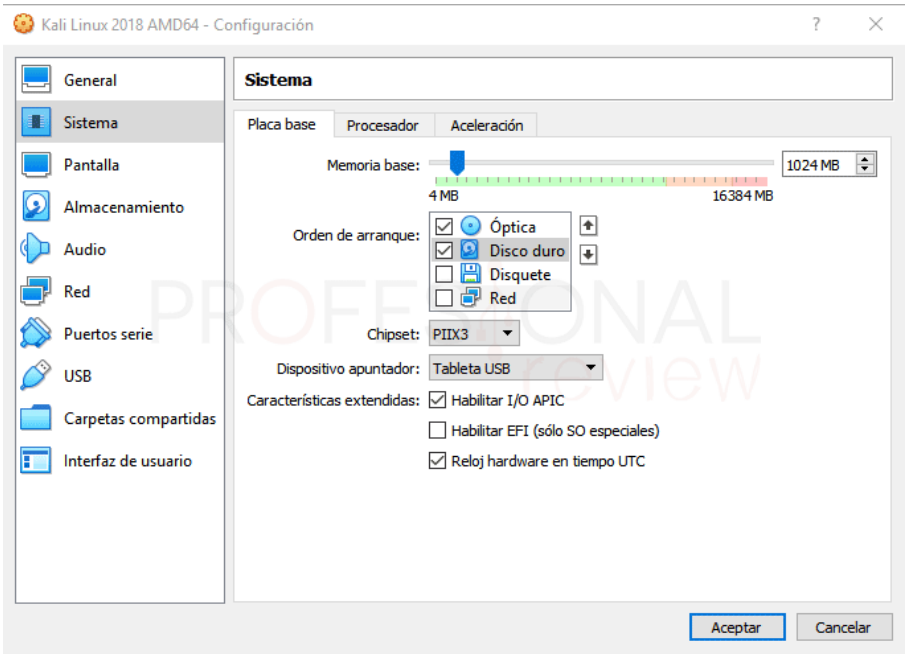


Figura 46: Eliminar disquete

En el apartado “Sistema” elegiremos usar dos núcleos de procesador, si tenemos más núcleos o queremos destinarlos todos, adelante. Si nos centráramos en esta distribución, conseguiríamos velocidades mucho más rápidas.

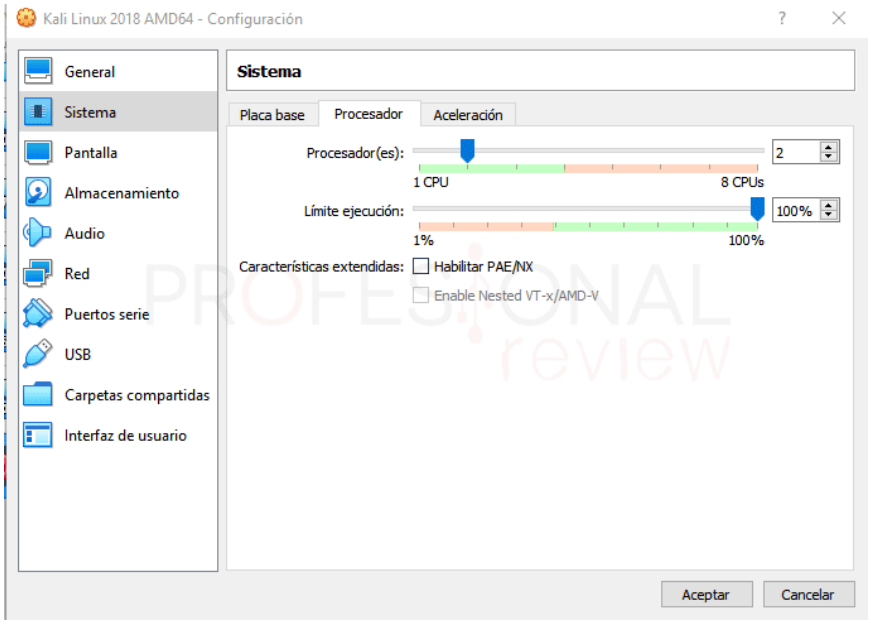


Figura 47: Elección de dos núcleos de procesador

Ahora vamos directamente al apartado de Almacenamiento y seleccionamos nuestro lector de CD virtual, luego pulsamos en el icono del disco de la derecha. Seleccionamos la imagen ISO de Kali Linux que se guardó durante el proceso de descarga.

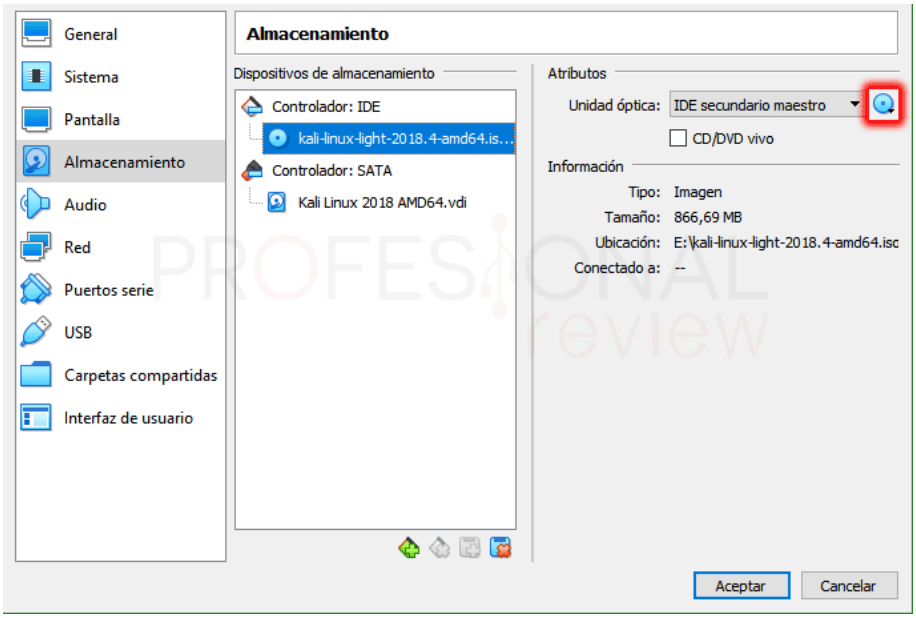


Figura 48: Apartado de almacenamiento

En cuanto a la parte de red, la dejamos como está por ahora, accediendo a internet a través de nuestros dispositivos físicos en modo NAT.

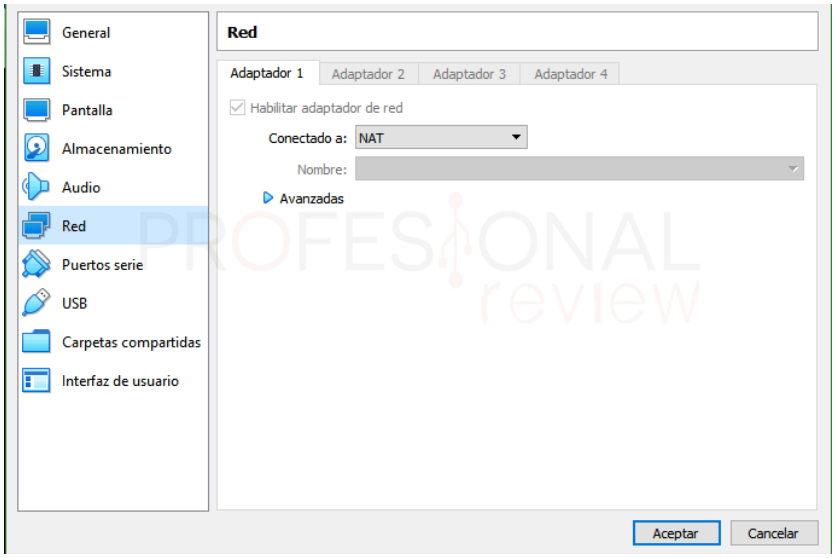


Figura 49: Red

Instalación de Kali Linux

La instalación es muy similar de instalar a las distribuciones basadas en Debian, pero si queremos utilizar la GUI, primero debemos seleccionar la opción "Instalación gráfica".

Figura 50: Instalación de Kali Linux

Seleccionamos el idioma de instalación y aceptamos el mensaje de que la traducción está incompleta.

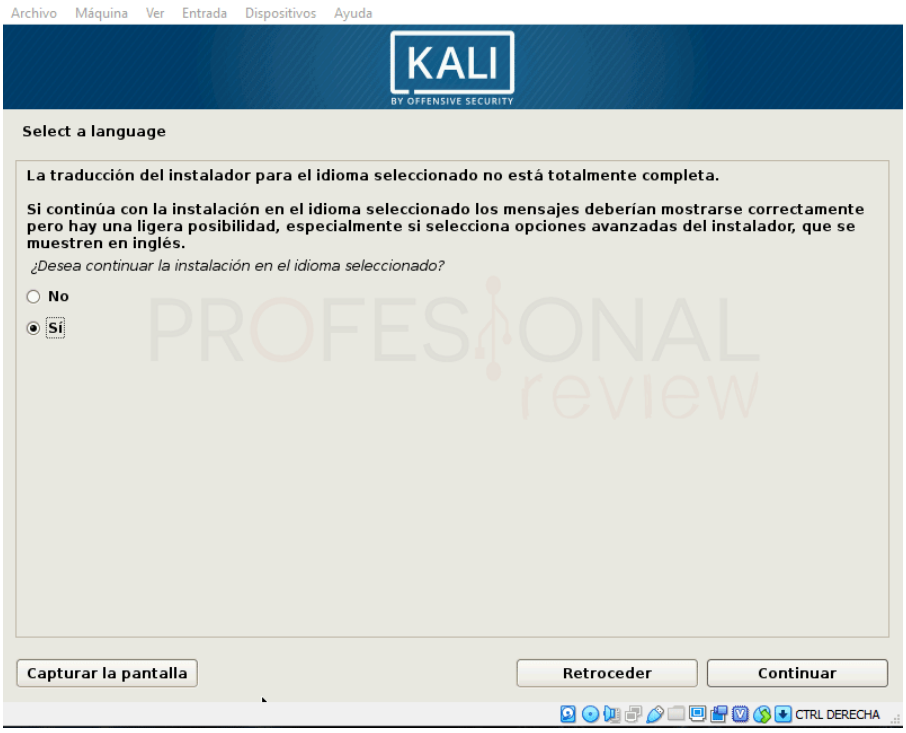


Figura 51: Idioma de instalación

Ahora necesitamos ingresar el nombre de la máquina, es muy importante identificar esta máquina en la red, por eso ingresamos un nombre al que podamos referirnos si es necesario.

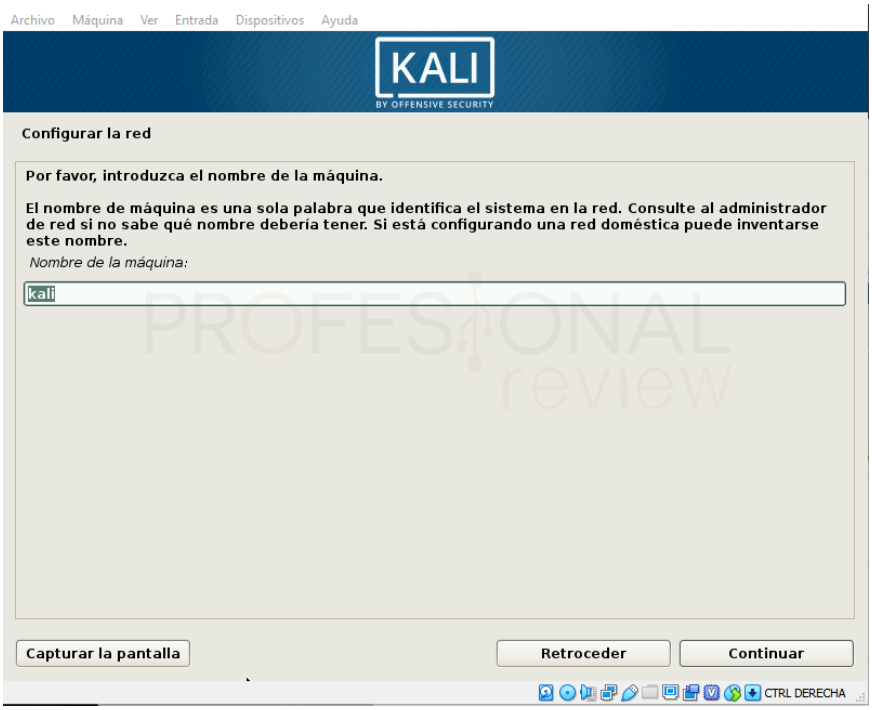


Figura 52: Nombre de la máquina

El sistema preguntará si el ordenador está en la red bajo un dominio, por ejemplo, con Directorios de red o simplemente porque tenemos un dominio activo local. Como estamos en un entorno doméstico solo se prosigue los pasos.

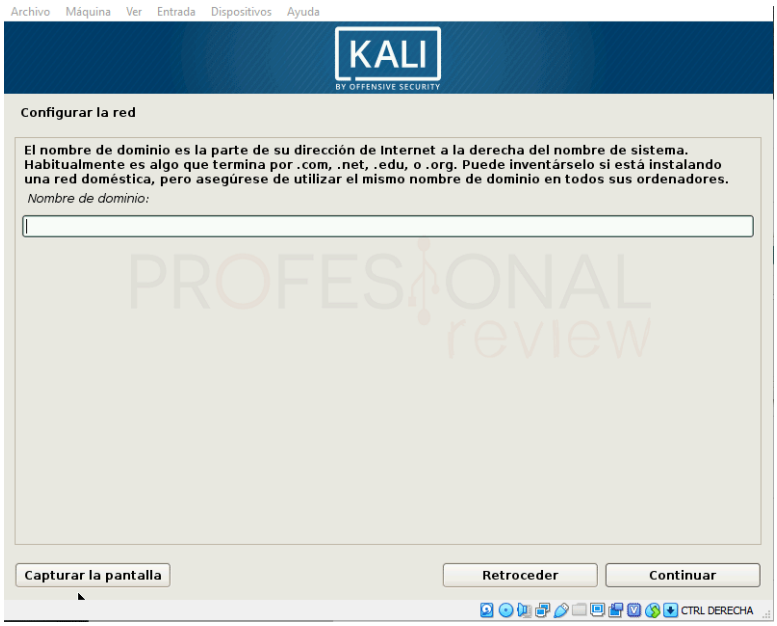


Figura 53: Ordenador en red

En la nueva ventana ingresamos la contraseña del usuario Root, Este usuario será el usuario activo original en el sistema, es decir, siempre seremos Root, por lo que necesitamos crear una buena contraseña para estar seguros en este caso será Kali.

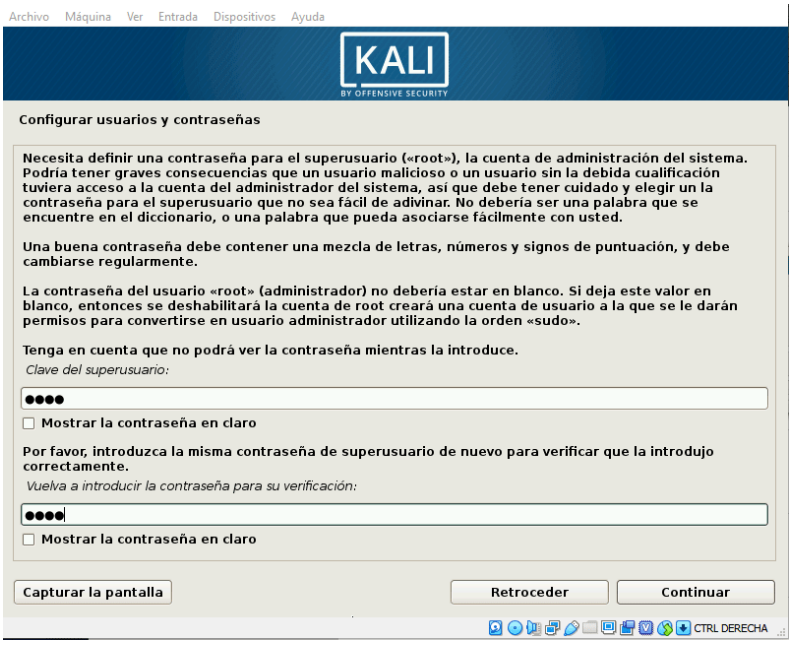


Figura 54: Contraseña del usuario Root

Ahora entramos en la configuración del modo de instalación que haremos, elegiremos un modo de arranque donde queramos utilizar todo el disco duro, ya que es una máquina virtual.

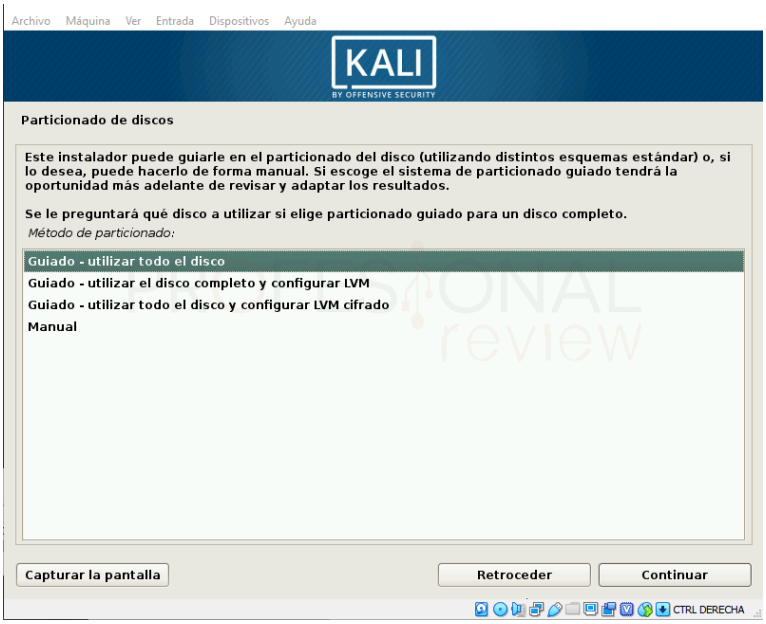


Figura 55: Configuración del modo de instalación

También elegiremos tener todos los archivos en una partición, aunque podemos elegir que el sistema cree tres particiones para agregar /home, /var y /tmp para separar particiones si queremos.

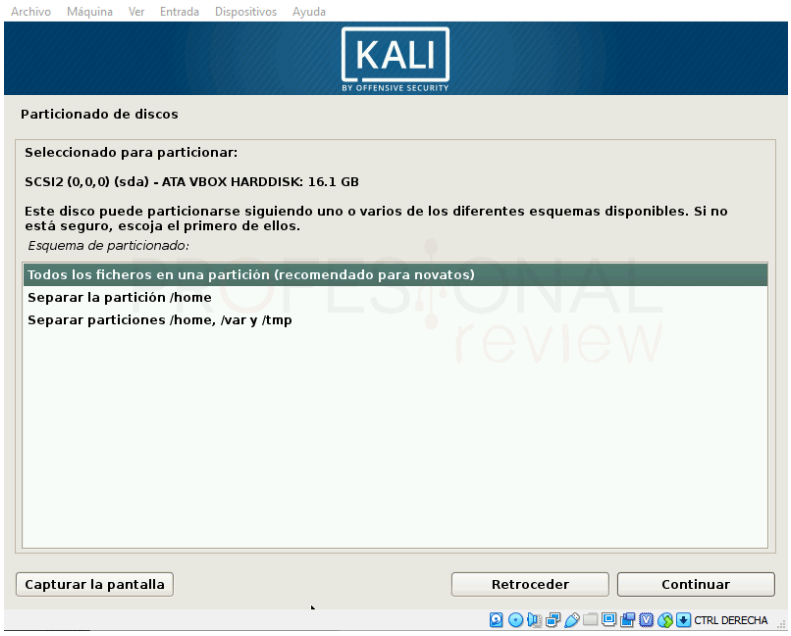


Figura 56: Elección de los archivos en una partición

Veremos un resumen de lo que se hará, de forma predeterminada, Linux siempre asigna 1 GB de espacio para memoria virtual o memoria de intercambio que serán inquebrantable.

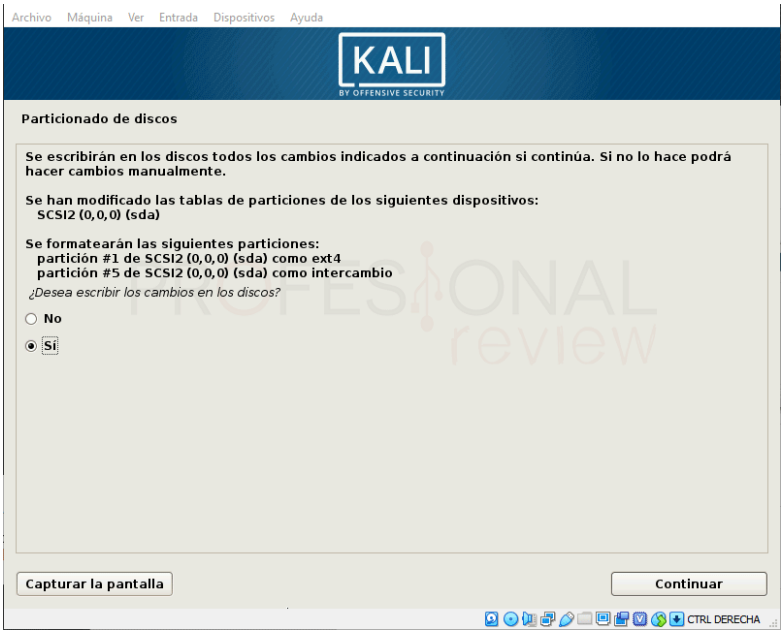


Figura 57: Asignación de espacio para memoria virtual

Antes de iniciar el proceso de instalación del archivo, se nos pregunta si queremos crear una copia de red, normalmente para actualizaciones del programa. Elegimos que realmente queremos hacerlo.

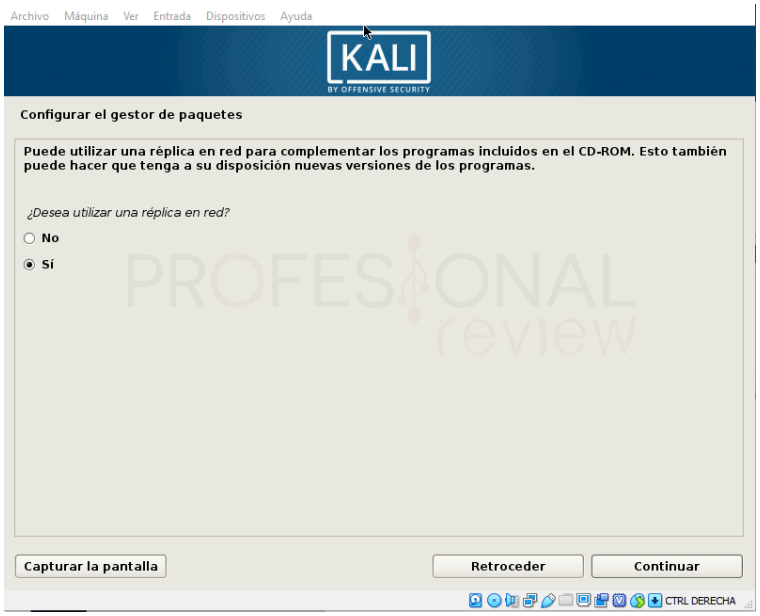


Figura 58: Crear copia de red

Finalmente, se nos preguntará si queremos instalar **GRUB** para controlar el inicio de la máquina virtual, se recomienda que lo instale si se tiene problemas en el futuro o desea cambiar este orden usando un sistema diferente.

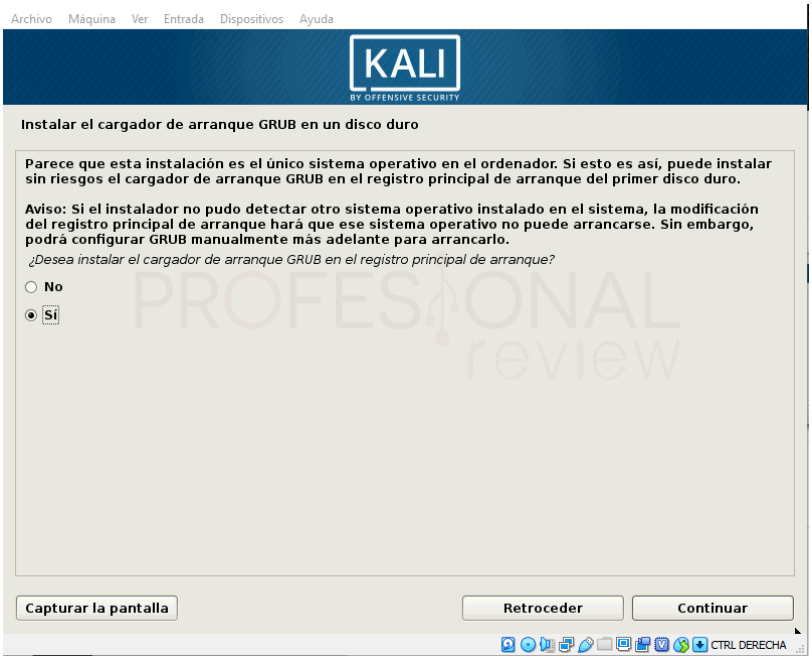


Figura 59: Instalación de GRUB

Por supuesto, elegimos la partición activa del sistema donde instalamos Kali Linux.

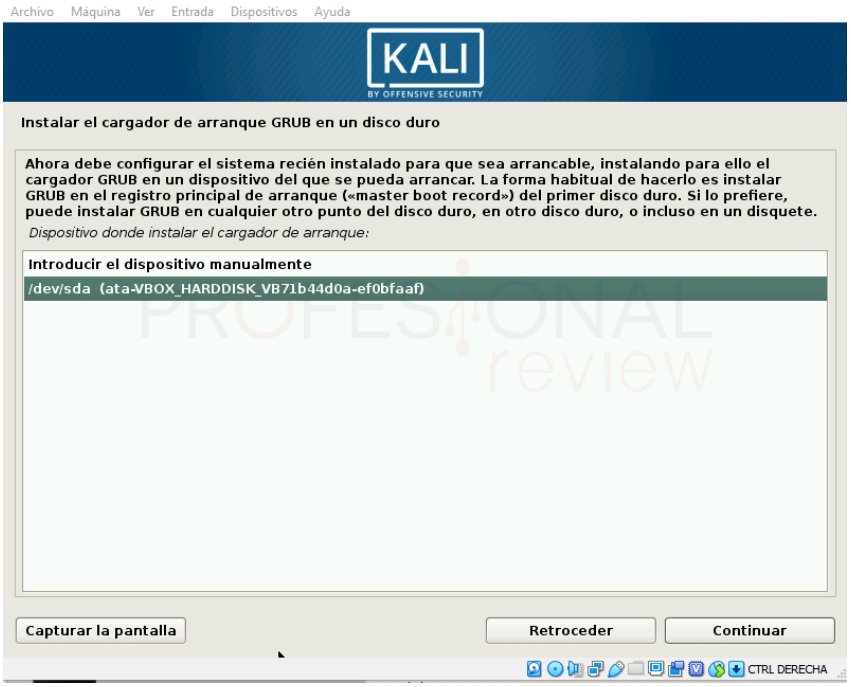


Figura 60: Partición activa del sistema

Finalmente, el proceso se ejecutará y nuestra máquina virtual comenzará a funcionar. Debemos recordar que el usuario predeterminado es Kali y la contraseña que ingresamos anteriormente en el asistente.

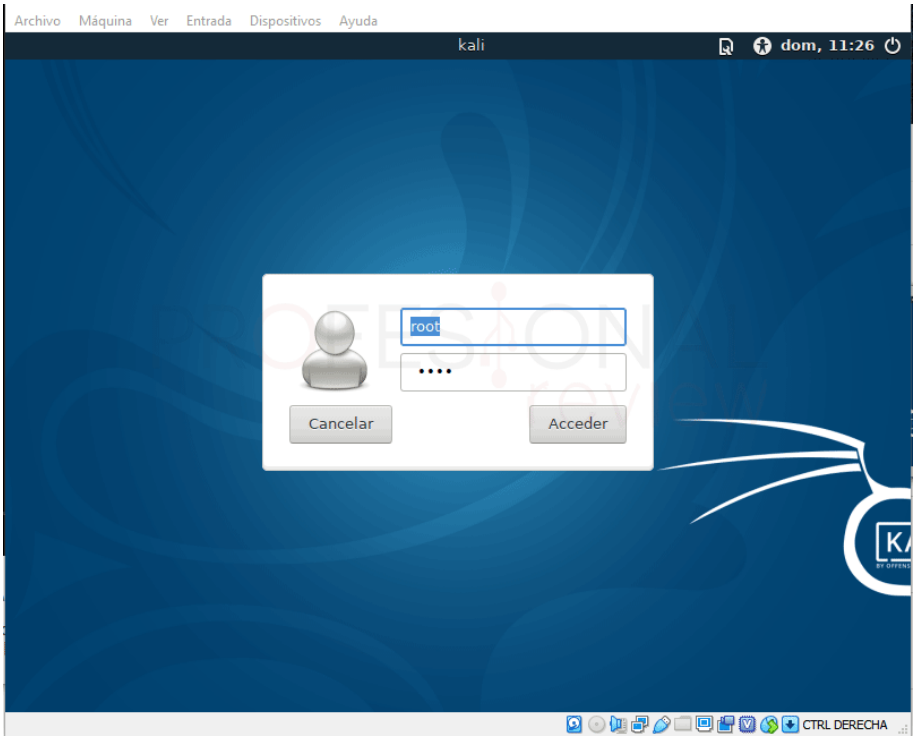


Figura 61: Proceso ejecutado

Anexo 4. Instalación de Ubuntu

El primer paso para instalar Ubuntu es descargar la imagen ISO oficial del sistema operativo Ubuntu 22.04 LTS la configuración del Virtual Box es similar a la de Kali Linux.

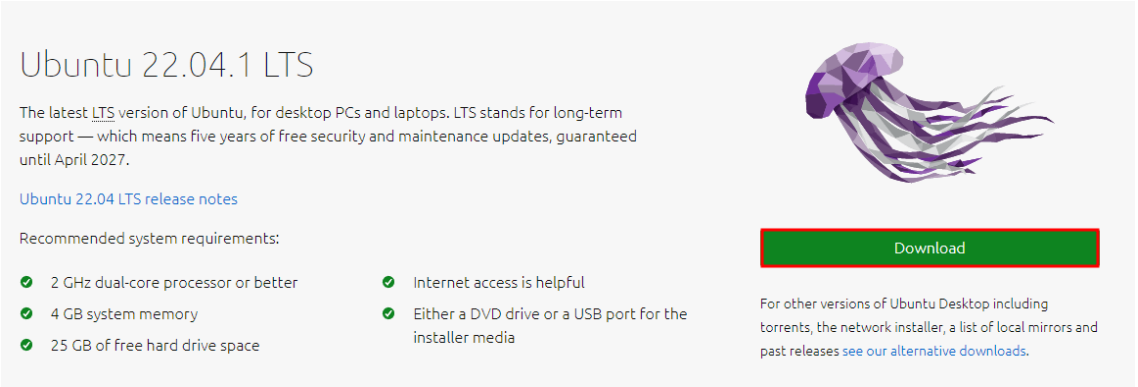


Figura 62: Descarga de la imagen ISO de Ubuntu

Cuando el sistema arranque en la nueva pantalla de instalación de Ubuntu, seleccione la opción Probar o instalar Ubuntu.

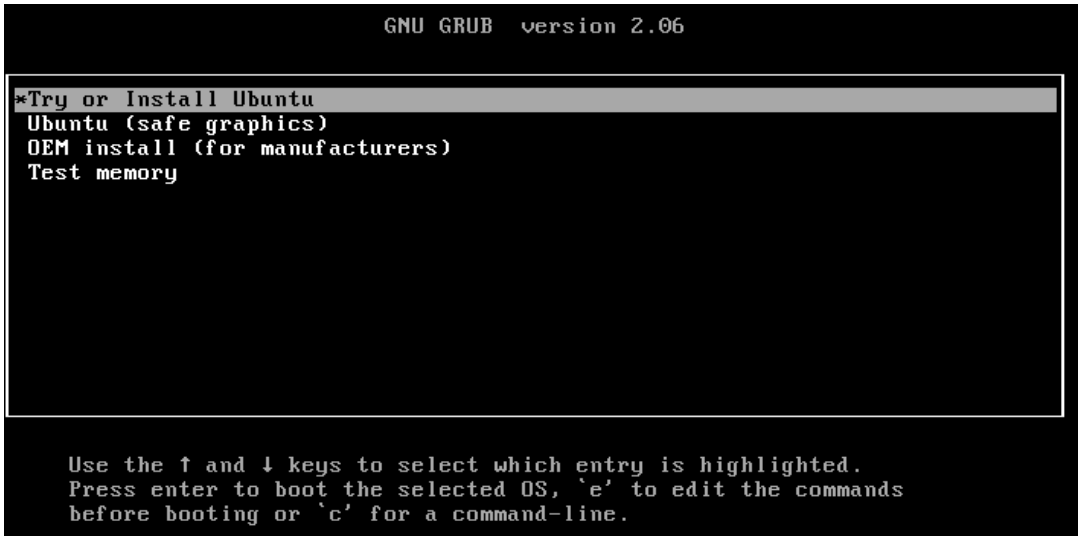


Figura 63: Pantalla de instalación

Seleccione el idioma de instalación y seleccione la opción Instalar Ubuntu en el siguiente paso. También existe la opción de probar Ubuntu. En este caso, los archivos del disco duro no se eliminarán. Sin embargo, pasemos a la instalación completa.

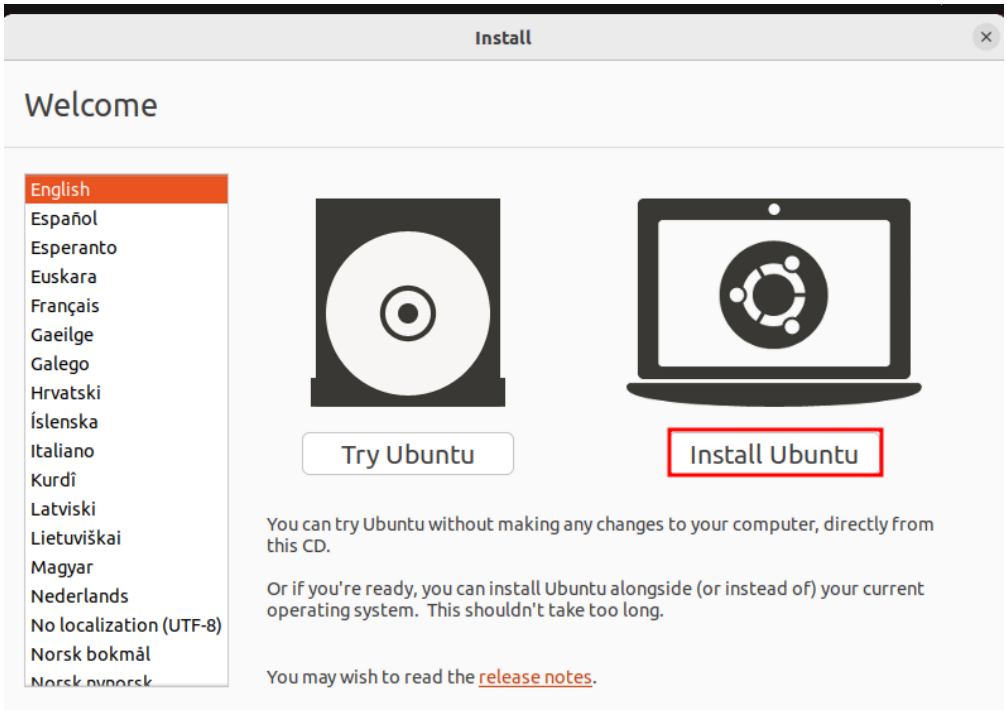


Figura 64: Idioma de instalación

Elija su distribución de teclado preferida y continúe.

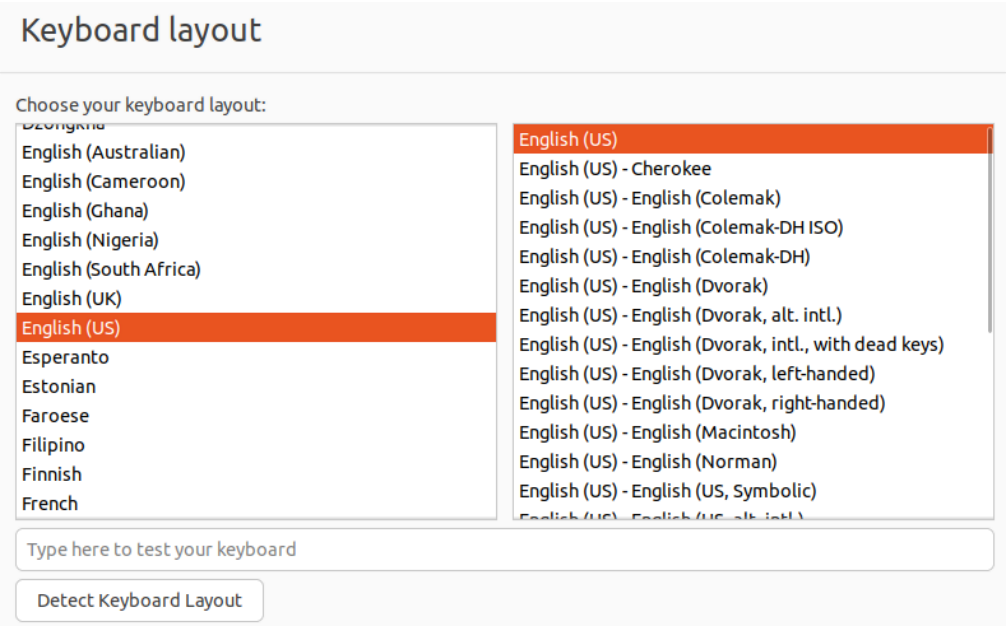


Figura 65: Distribución de teclado

Ahora puedes elegir entre instalación normal y mínima. Recomendamos seguir con la instalación normal, ya que proporciona más utilidades y paquetes de software. Seleccione también la opción de descargar actualizaciones para obtener la última versión.

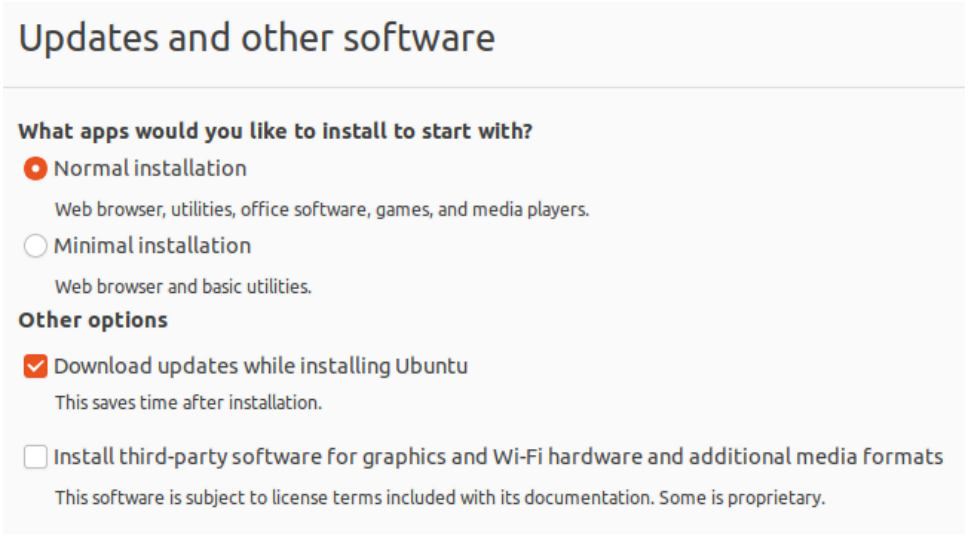


Figura 66: Instalación normal

Para Tipo de instalación, seleccione Borrar disco e instale Ubuntu.

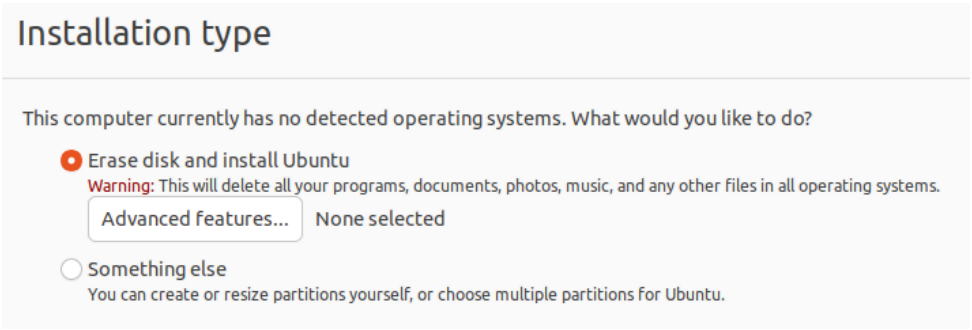


Figura 67: Tipo de instalación

Cuando se le solicite particionar, haga clic en Continuar.

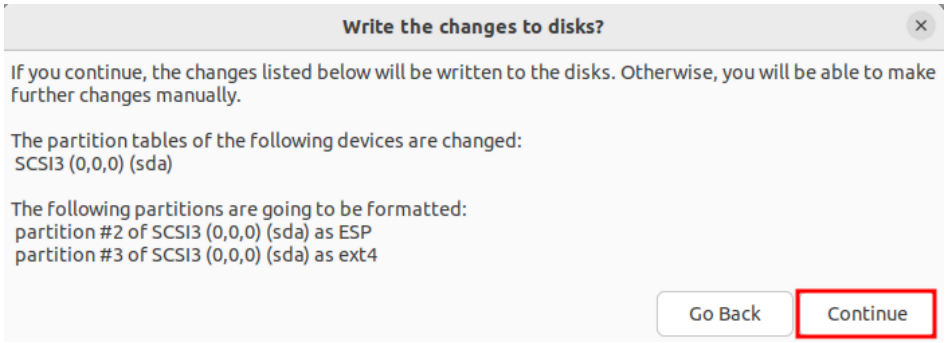


Figura 68: Particionar

Luego seleccione su zona horaria.

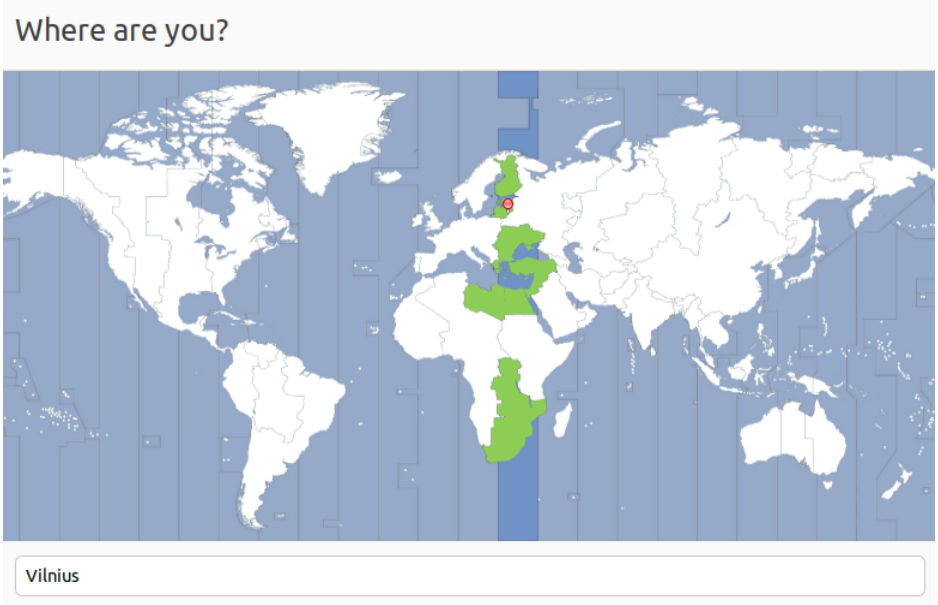


Figura 69: Zona horaria

Finalmente, ingresa tu nombre, usuario y contraseña.

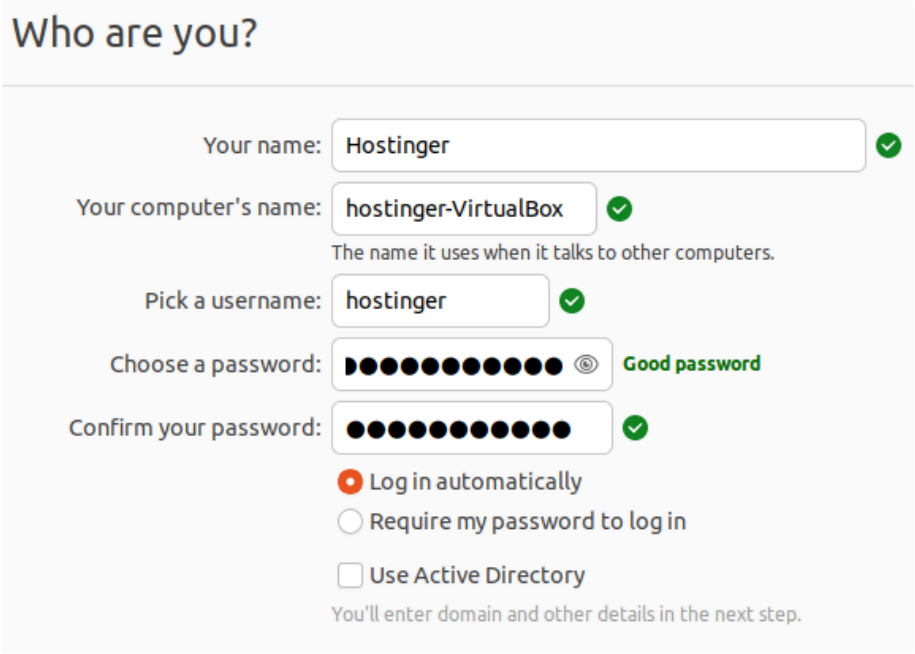


Figura 70: Ingreso de nombre, usuario y contraseña

Después de hacer clic en Continuar, comenzará la instalación de Ubuntu. Espere unos 20 minutos para que se complete la instalación y luego reinicie su computadora. Cuando su computadora se inicie, debería ver la pantalla de bienvenida estándar.

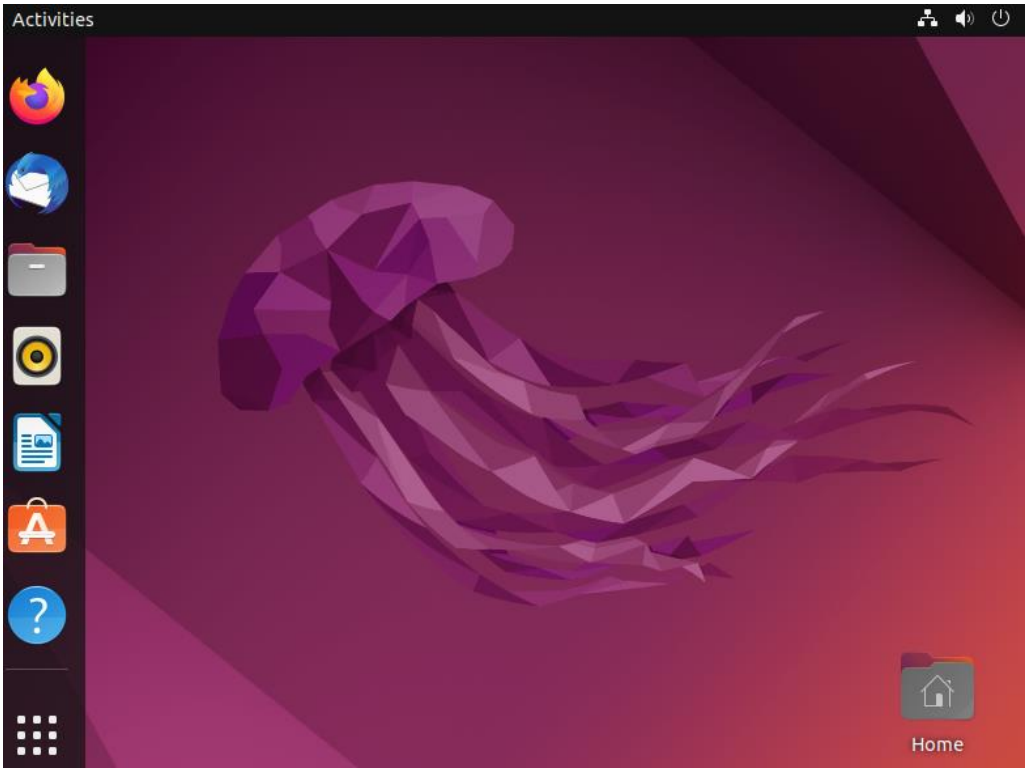


Figura 71: Comenzar la instalación de Ubuntu

Anexo 5. Instalación de Windows 7

La instalación mostrará unas pantallas entre las que encontraremos:

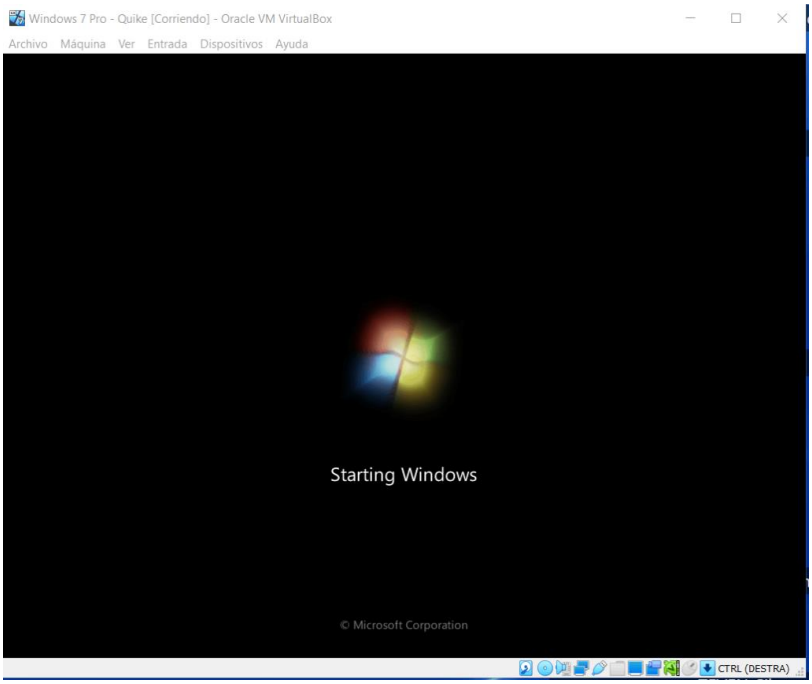


Figura 72: Pantalla de Windows

Cuando el programa nos muestre este apartado es el momento de elegir el idioma de instalación.

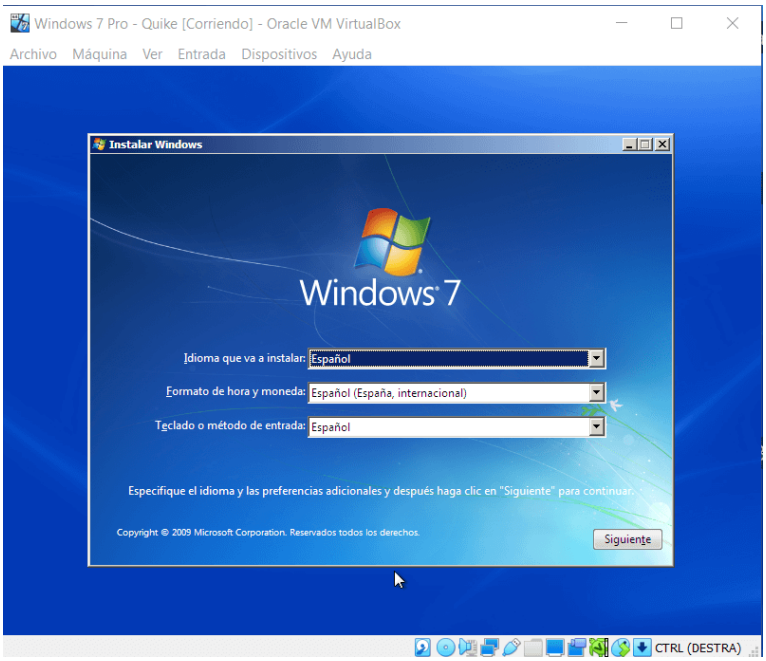


Figura 73: Elegir idioma de instalación

Seleccionamos español y pulsamos el botón Siguiente, luego veremos otro apartado donde presionaremos el botón “Instalar ahora”.

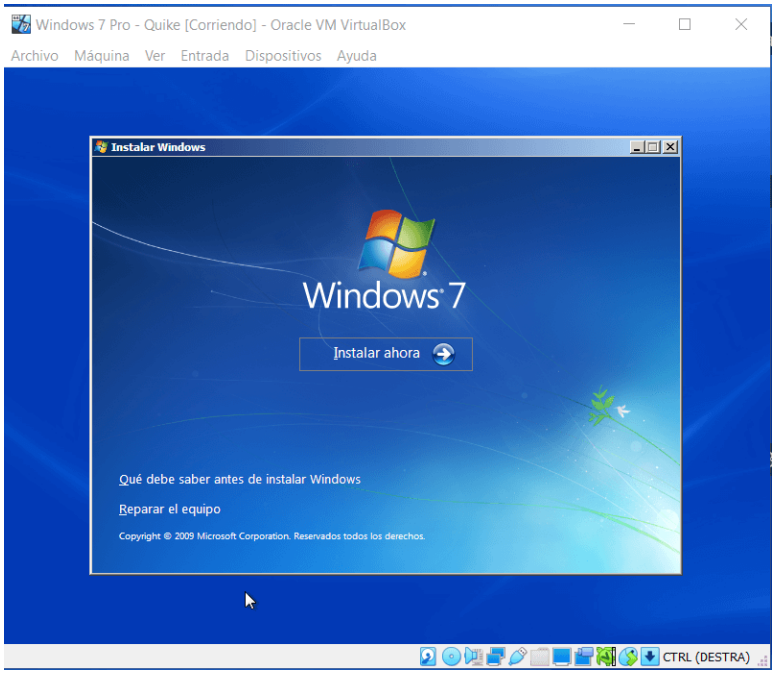


Figura 74: Instalar ahora

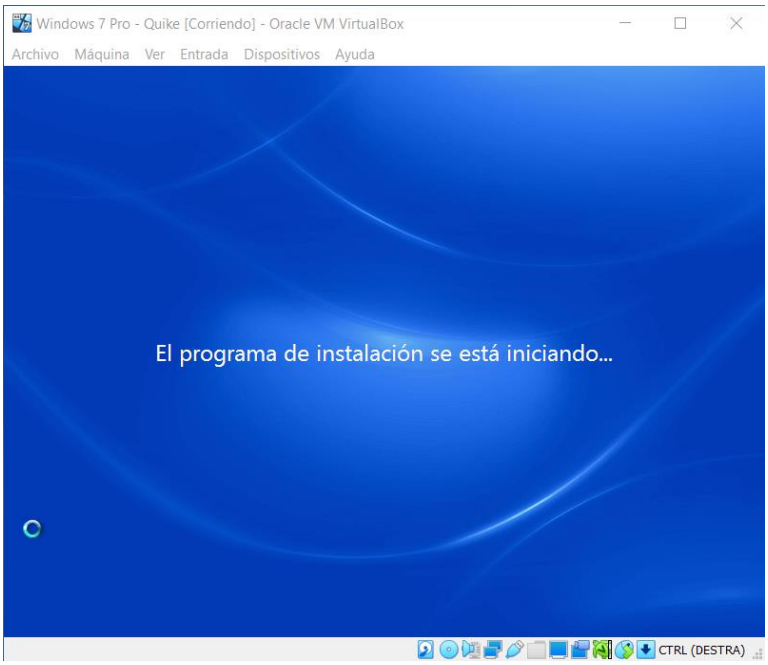


Figura 75: Inicio de programa de instalación

Hacemos clic en "Acepto los términos de la licencia" y luego hacemos clic en el botón "Siguiente".

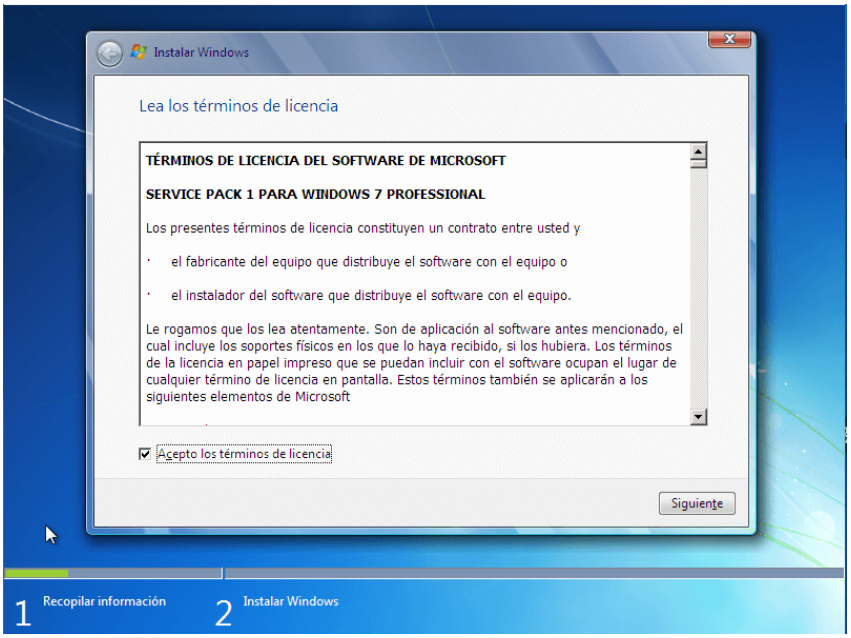


Figura 76: Aceptar términos de la licencia

Luego aparece un apartado donde tenemos que elegir el tipo de instalación que queremos hacer.

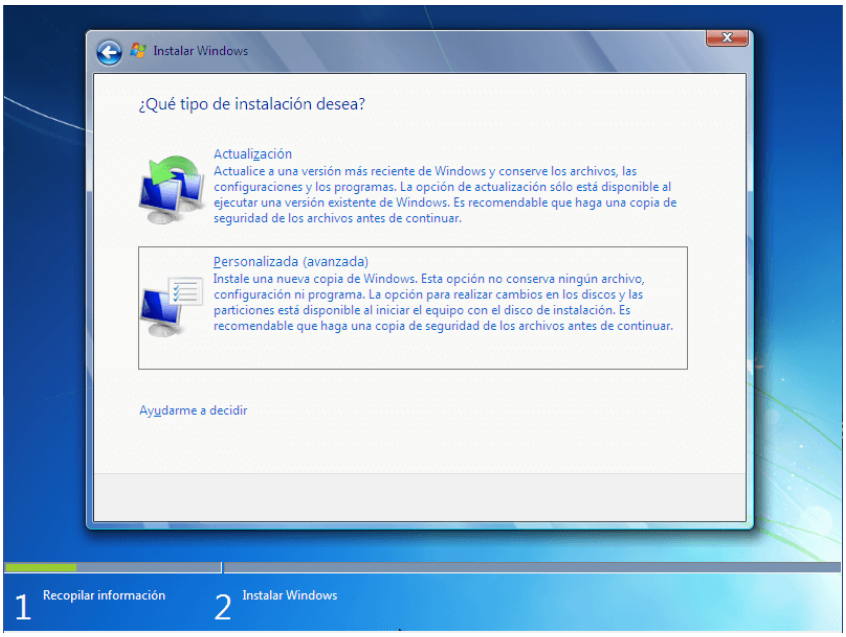


Figura 77: Tipo de instalación

Seleccionamos Personalizado (Avanzado).

Se nos pregunta dónde queremos instalar Windows 7 y pulsamos el botón "Siguiente" para continuar.

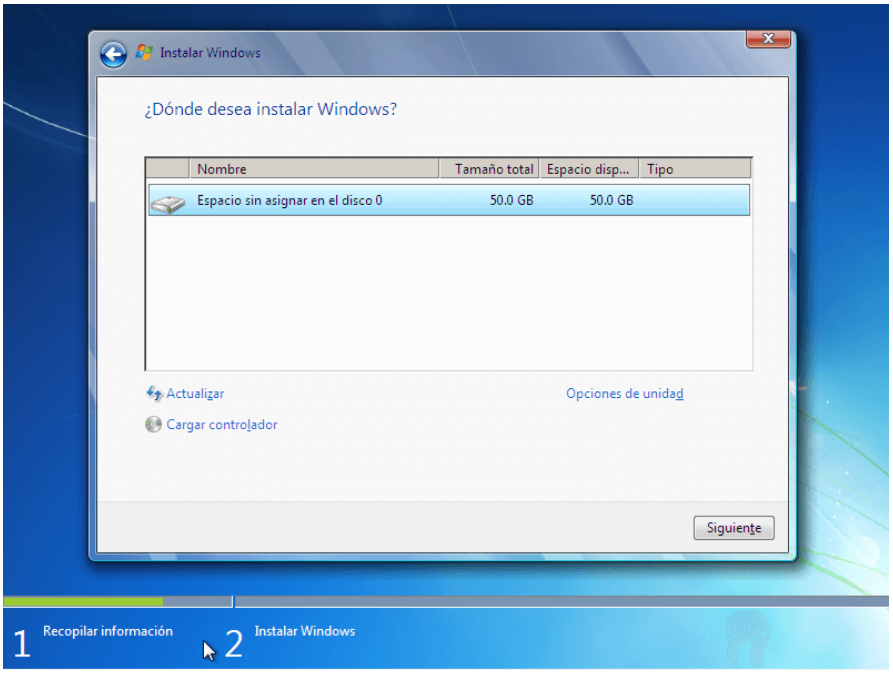


Figura 78: Continuación de la instalación

Cuando se complete el proceso de instalación, su computadora se reiniciará.

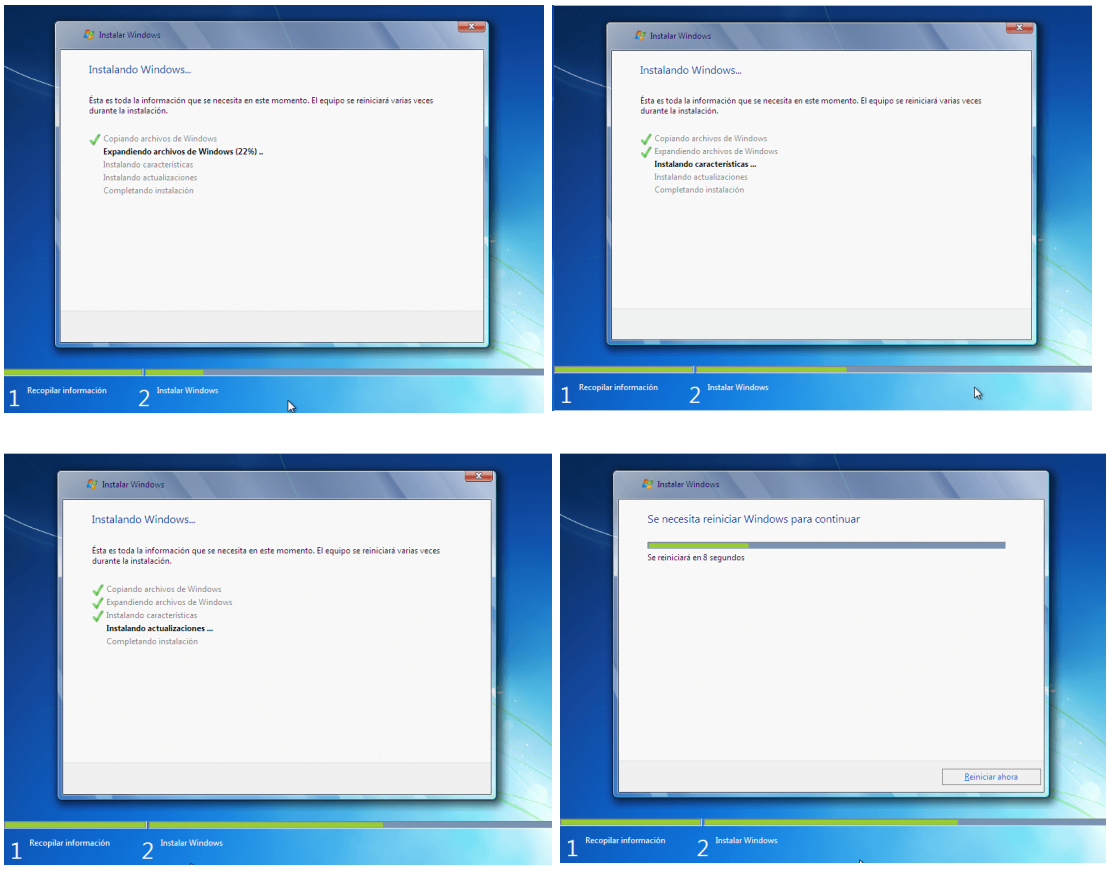


Figura 79: Reinicio de la computadora

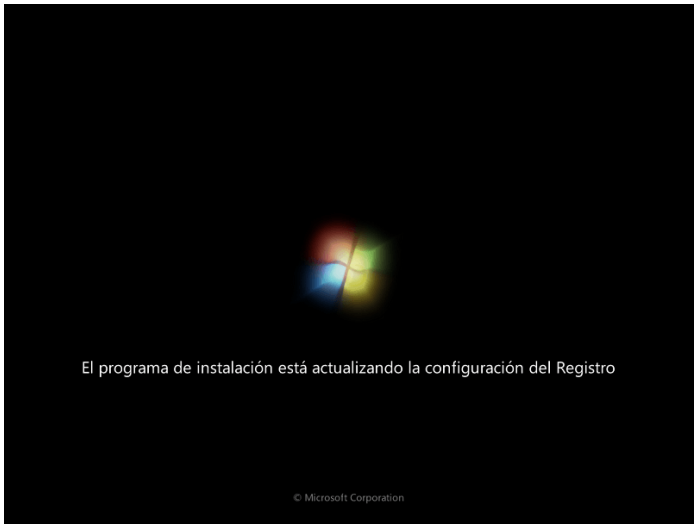


Figura 80: Instalación completada

Cuando el sistema operativo se inicia por primera vez, el primer paso que debemos hacer es ingresar la información básica de instalación.

Figura 81: Inicio de Windows 7

Especificamos el nombre de usuario y el nombre del ordenador que se asignará al ordenador. Pulsamos el botón "Siguiente" para continuar.

Si es necesario especificar la contraseña, personalmente la dejo en blanco. Si decidimos ingresar una contraseña, además de proporcionar una pista en caso de que la olvidemos en el futuro, también debemos escribirla dos veces.

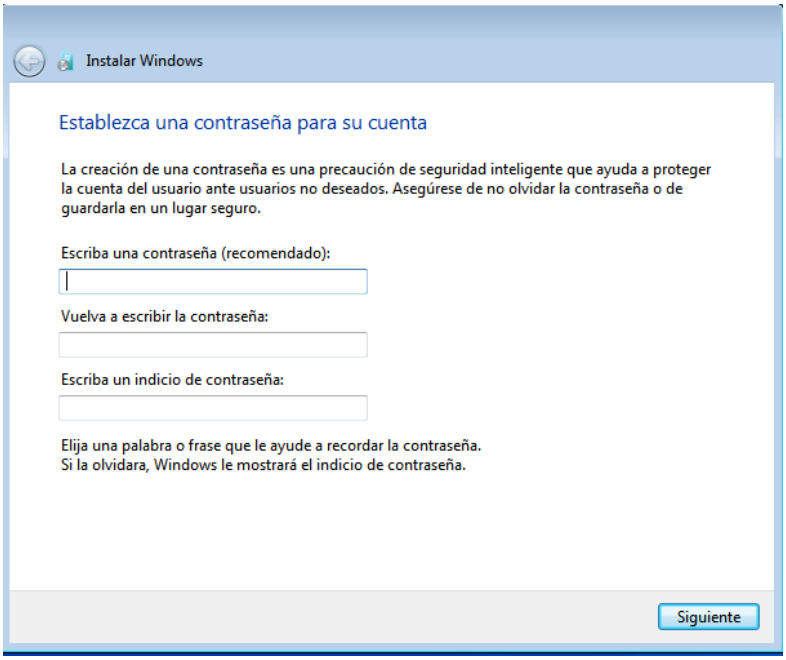


Figura 82: Especificar la contraseña

Ahora debemos decidir qué configuración usar para instalar la actualización. En nuestro caso seleccionaremos Preguntarme más tarde para que podamos descargar el paquete de actualización completo de inmediato.

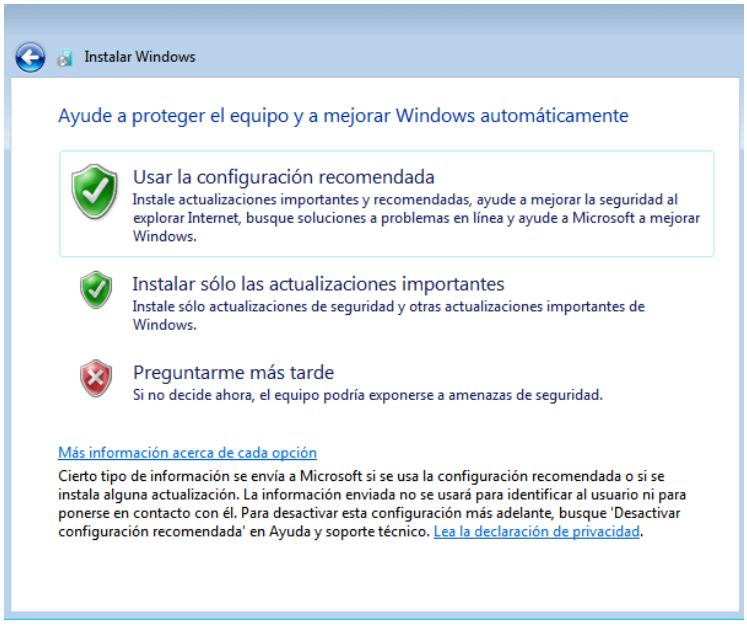


Figura 83: Configuración para instalar la actualización

Luego se nos pedirá que confirmemos la zona horaria. En la siguiente sección, especificamos el tipo de red utilizada por la máquina virtual.

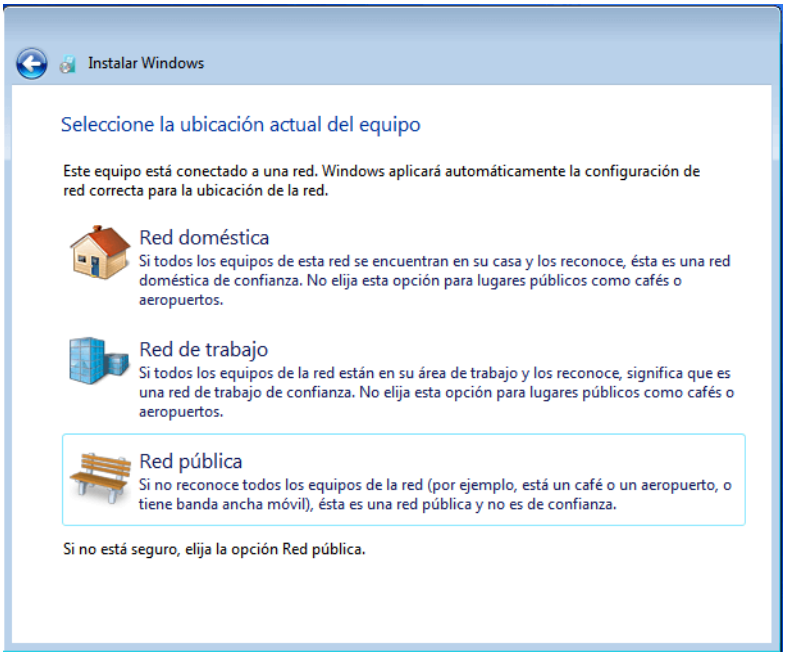


Figura 84: Confirmar zona horaria

Seleccionamos la opción de red doméstica. Esperamos hasta que se complete toda la configuración inicial hasta que aparezca la siguiente pantalla.

Figura 85: Opción de red doméstica

Figura 86: Preparación del escritorio

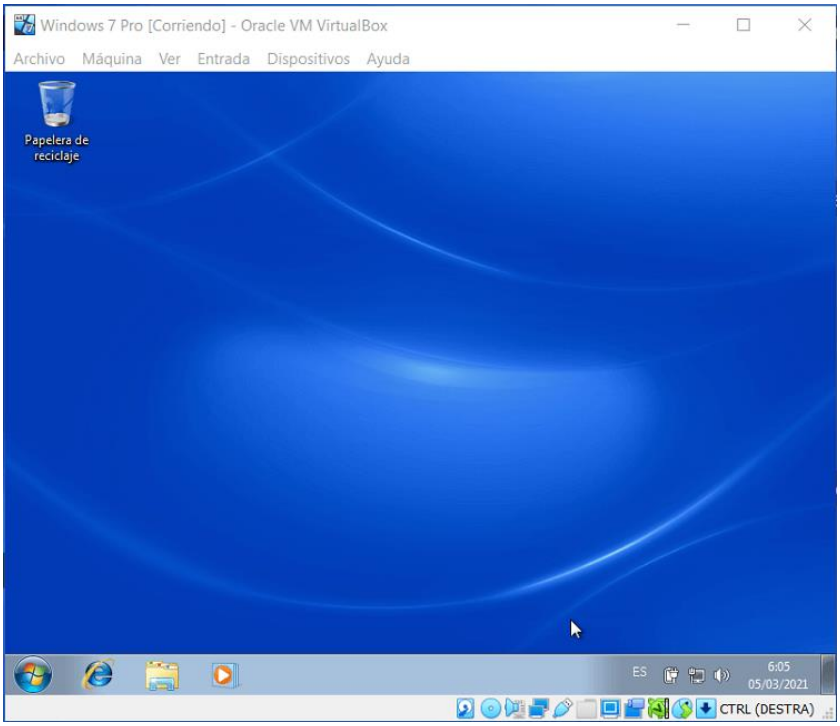


Figura 87: Pantalla principal de Windows 7

Anexo 6. Instalación de Servidor Xampp

Visite Apache Friends en su navegador web y descargue el instalador de XAMPP.

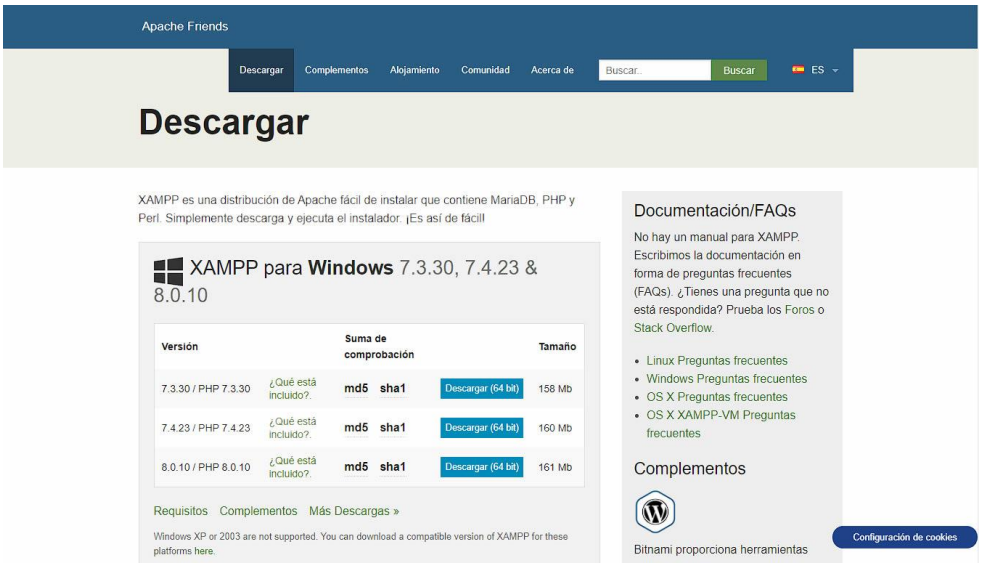


Figura 88: Página de Apache

Después de descargar el paquete, puede ejecutar el archivo .exe haciendo doble clic en él, se muestra la pantalla inicial del asistente de instalación de XAMPP. Haga clic en Siguiente para personalizar la configuración de instalación.

Figura 89: Descarga del paquete

En la sección Seleccionar componentes, puede excluir componentes individuales del paquete XAMPP de la instalación, se recomienda utilizar la configuración

predeterminada del servidor de prueba local e instalar todos los componentes disponibles. Haga clic en "Siguiente" para confirmar su selección.

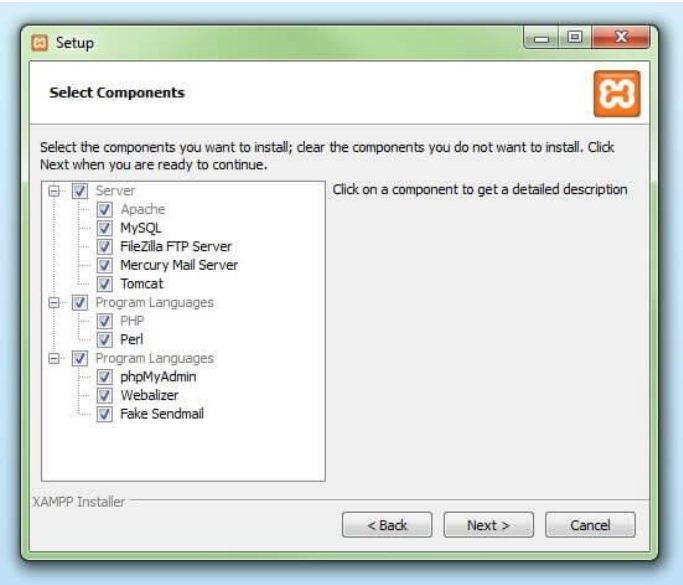


Figura 90: Comienzo de la instalación

En este paso, seleccione la carpeta donde se instalará el paquete. Si elige la configuración predeterminada, se crea una carpeta llamada Xampp en C:\.

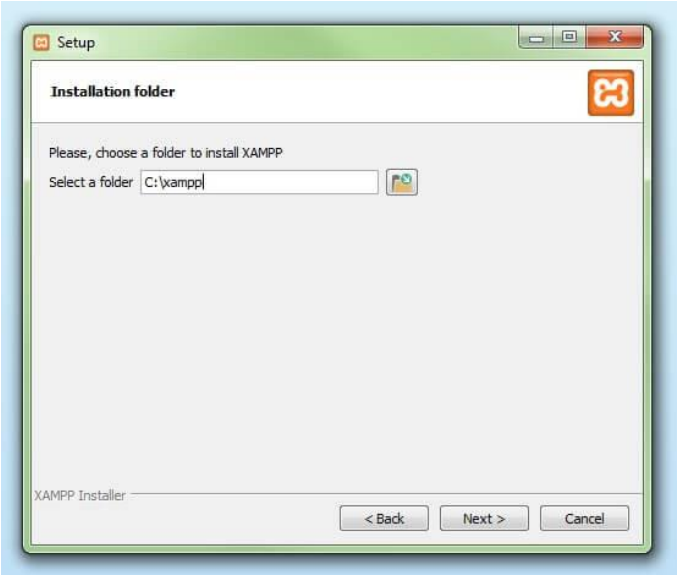


Figura 91: Selección de la carpeta

El asistente extraerá los símbolos seleccionados y los guardará en la carpeta seleccionada, lo que puede tardar unos minutos. El progreso de la instalación se muestra como una barra de carga verde.

Figura 92: Extracción de símbolos seleccionados

Durante el proceso de instalación, el asistente suele advertir sobre el bloqueo del firewall, En este cuadro de diálogo, puede seleccionar las casillas para permitir que el servidor Apache se comunique en su red privada o en su red de trabajo. Recuerda que no es recomendable utilizarlo en redes públicas.

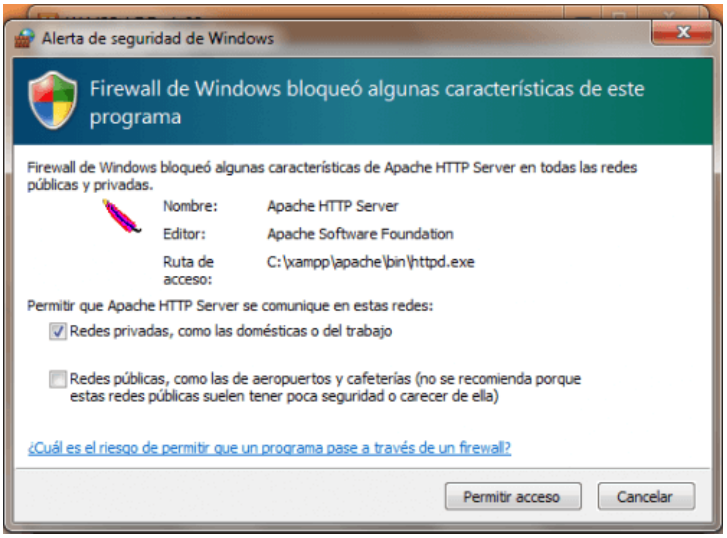


Figura 93: Proceso de instalación

Una vez que se hayan extraído e instalado todos los componentes, puede utilizar el botón "Listo" para cerrar el asistente. Para acceder inmediatamente al panel de control basta con marcar la casilla que pregunta si queremos hacer esto.

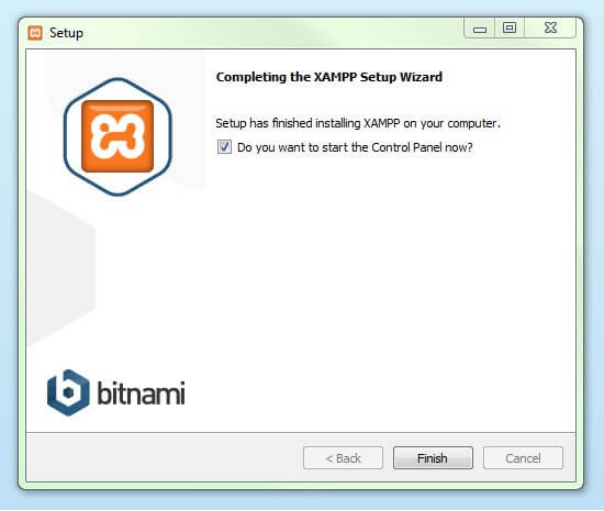


Figura 94: Botón de listo

Todas las acciones se registran en la interfaz de usuario del panel de control y los módulos se pueden activar o desactivar individualmente con un solo clic. Además, se encuentran disponibles varias utilidades, tales como:

- **Configuración:** configure XAMPP y otros componentes de aislamiento.
- **Netstat:** muestra todos los procesos que se ejecutan en esta máquina
- **Shell:** iniciar una ventana de comandos de UNIX
- **Explorador**: abra la carpeta XAMPP en el Explorador de Windows
- **Servicios:** muestra todos los servicios en ejecución.
- **Ayuda:** Contiene enlaces a foros de usuarios.
- **Salir:** Se utiliza para salir de la consola

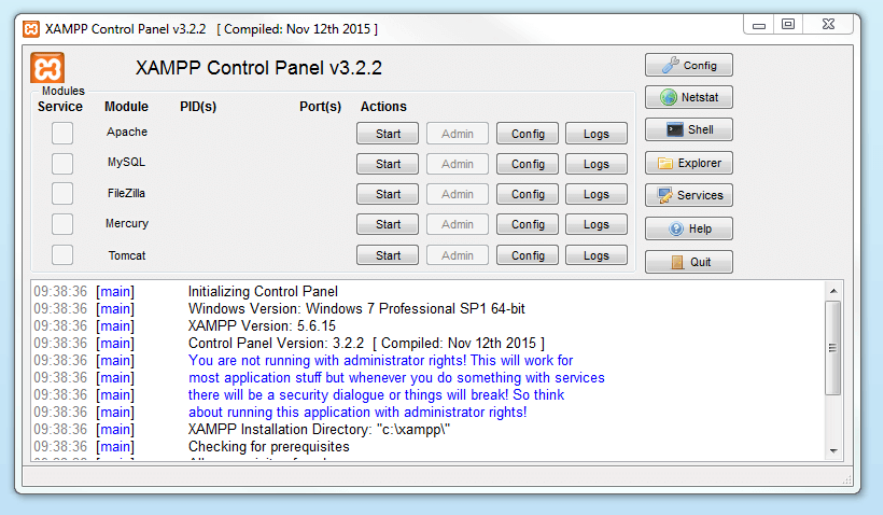


Figura 95: Pantalla de Xampp

Anexo 7. Instalación de Visual Studio Code

En la página de Microsoft Visual Studio Code en Academic Software y haga clic en el botón Descargar Visual Studio Code para descargar el archivo de instalación.

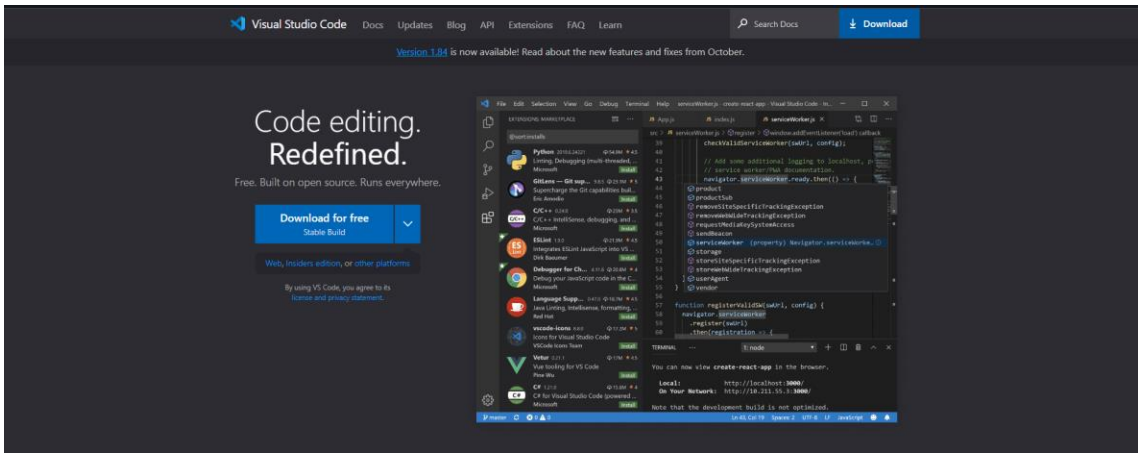
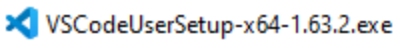


Figura 96: Instalación de Visual Studio Code

Para iniciar la instalación, abra el archivo de instalación .exe en la carpeta de descarga.



Lea y acepte el acuerdo de licencia. Haga clic en Siguiente para continuar.

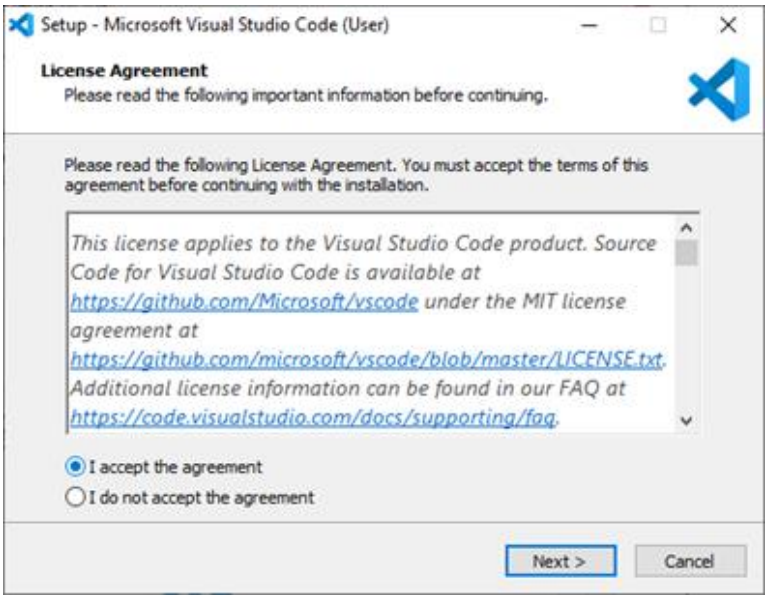


Figura 97: Aceptación de la licencia

Puede cambiar la ubicación de la carpeta de instalación o mantener la configuración predeterminada. Haga clic en Siguiente para continuar.

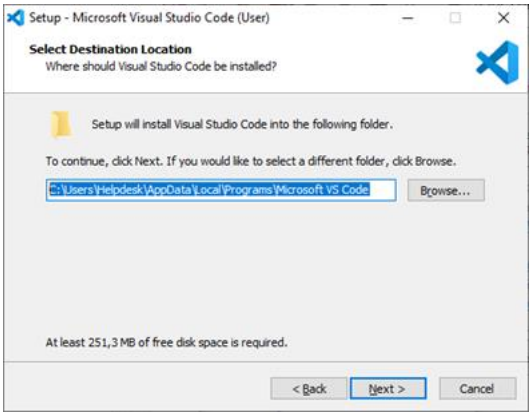


Figura 98: Ubicación de carpeta

Elija si desea cambiar el nombre de la carpeta de accesos directos en el menú Inicio o no instalar ningún acceso directo y haga clic en Siguiente.

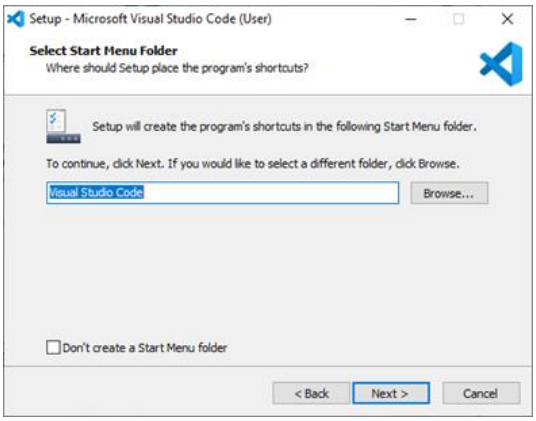


Figura 99: Cambio del nombre de carpeta

Seleccione otras tareas, como crear un icono en el escritorio o agregar opciones al menú contextual del Explorador de Windows. Haga clic en Siguiente.

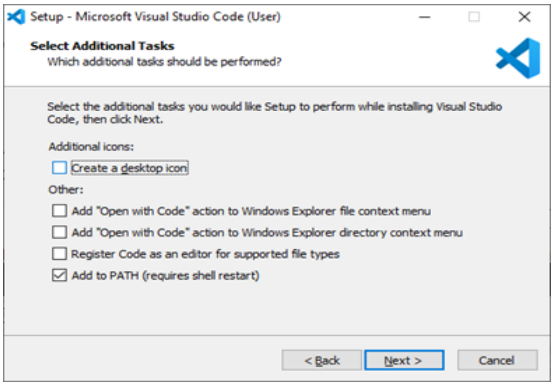


Figura 100: Selección de otras tareas

Haga clic en "Instalar" para iniciar la instalación.

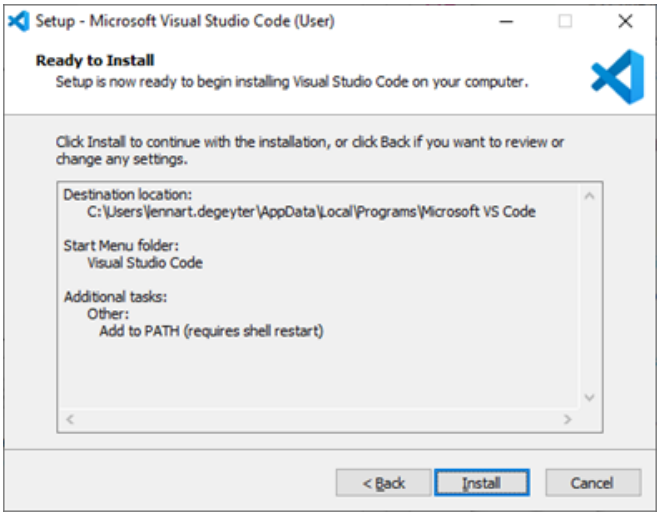


Figura 101: Instalar

El programa está instalado y listo para usar. Haga clic en "Finalizar" para completar la instalación e iniciar el programa.

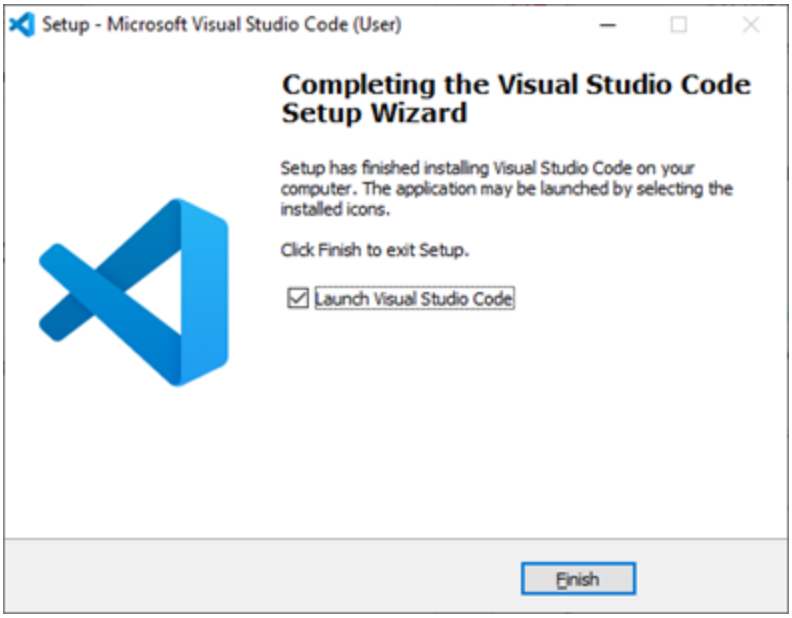


Figura 102: Finalizar instalación

Anexo 8. Caso 1 – Denegación de servicios

Para este caso forense de denegación de servicio, se utilizará el S.O. Windows 10 del equipo, además se empleará de forma virtualizada los sistemas operativos Ubuntu y Kali Linux, los cuales son de la familia de Linux y que previamente se instalarán en la máquina virtual, para luego proceder a instalar las siguientes herramientas para cada uno de las máquinas virtuales.

Se debe tomar en cuenta que la máquina Ubuntu será la encargada de ser el servidor de la página web creada y el atacante será la maquina con sistema Linux.

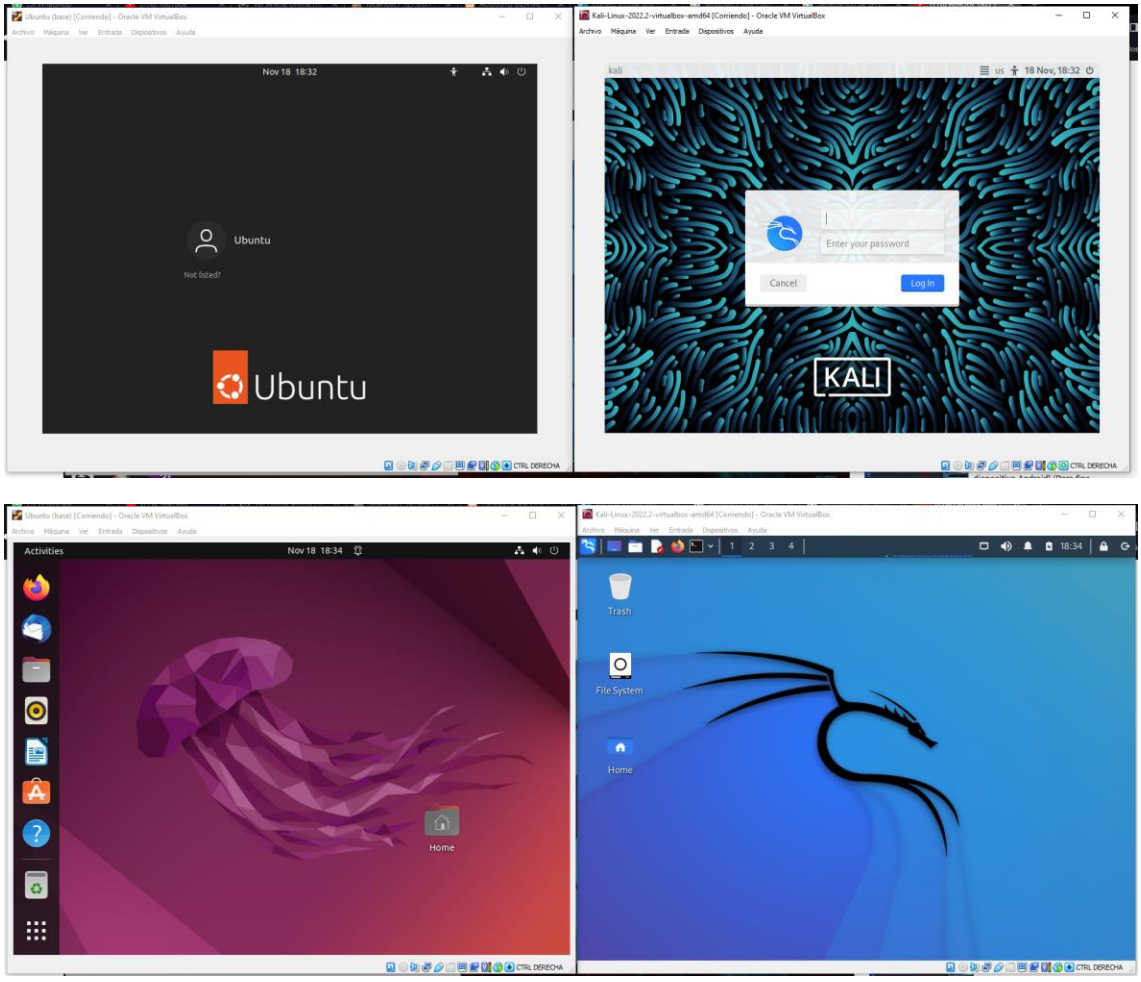


Figura 103: Ubuntu

Personalización para servidor Ubuntu

Para la máquina servidor, lo primero que se debe de ejecutar es una actualización del sistema utilizando desde el terminal el comando **apt update**, en modo superusuario con el comando **sudo -s**.

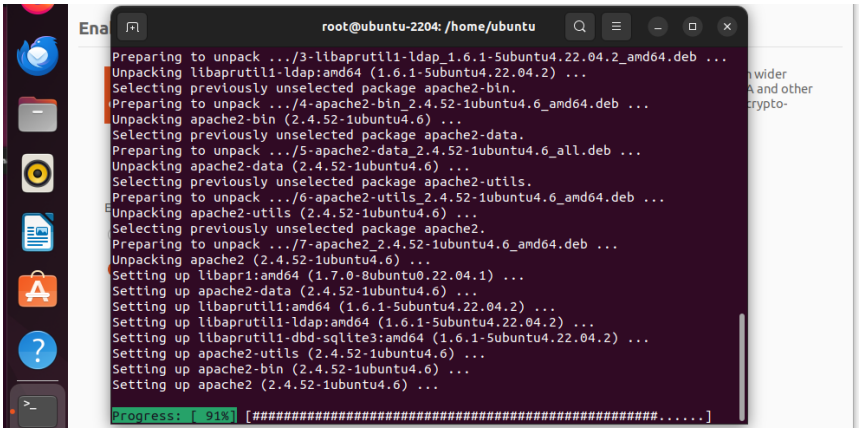


Figura 104: Personalización para servidor Ubuntu

Una vez actualizado el sistema, se procede a la instalación del servidor en Ubuntu mediante la línea de código **apt install apache2**, el cual empezará la instalación de este servidor.

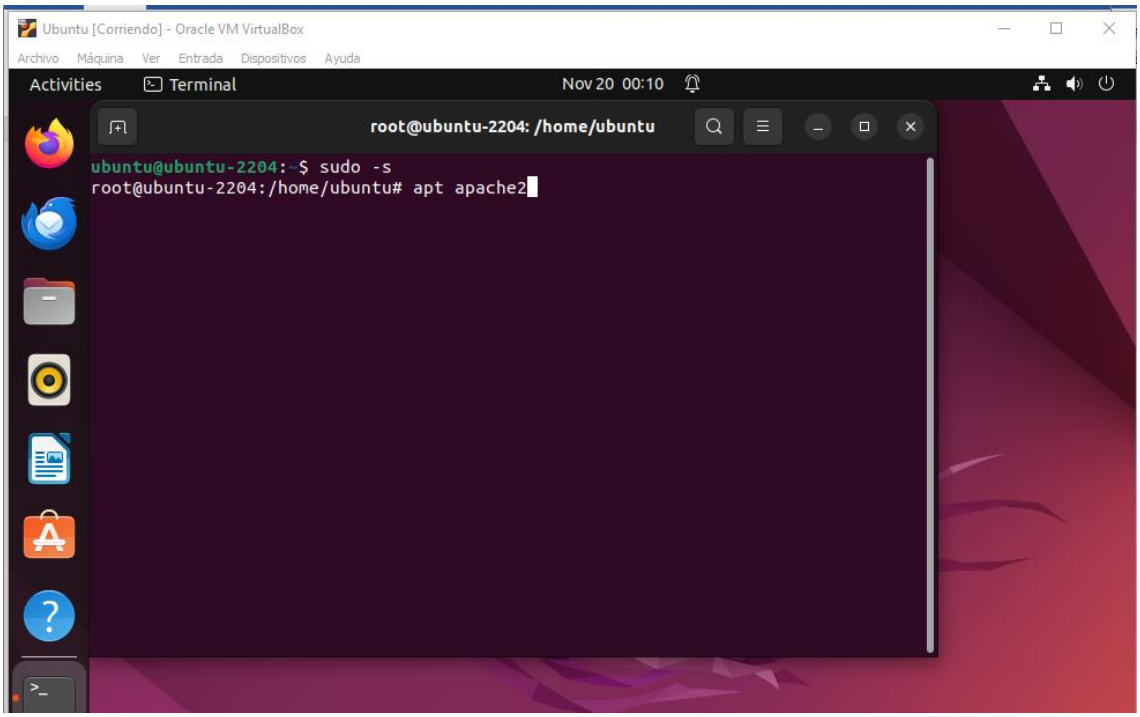


Figura 105: Actualizar el sistema

Una vez instalado, se puede verificar la versión del servidor apache usando el comando **apache2 -v.**

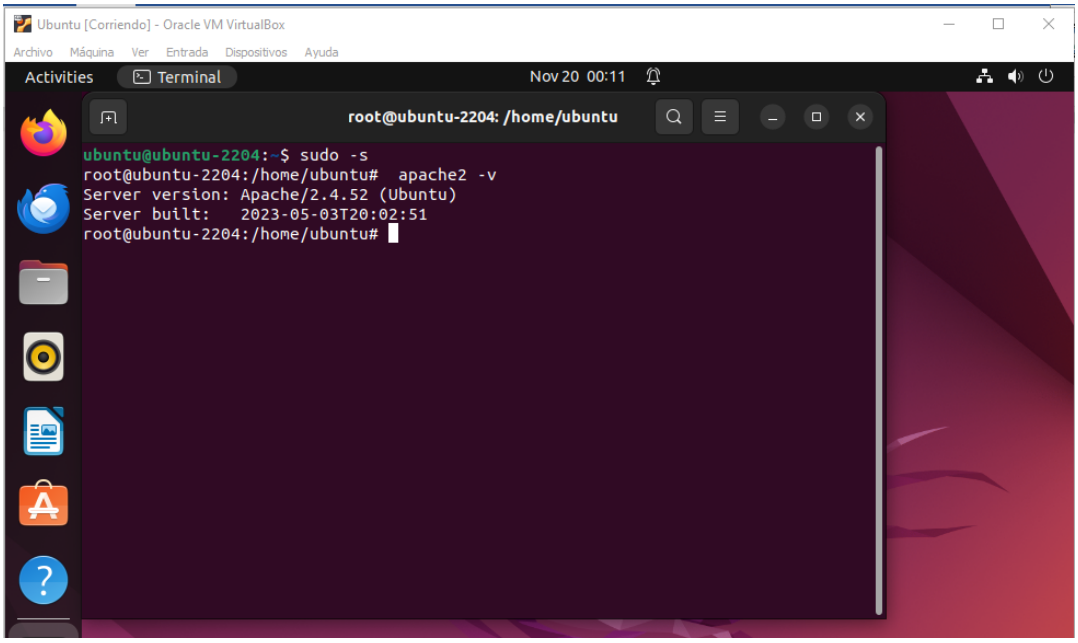


Figura 106: Verificar la versión

Verificando esto, se puede ver el estado del apache2 utilizando el comando **service apache2 status** para corroborar que está arrancando la máquina del servidor en el Ubuntu.

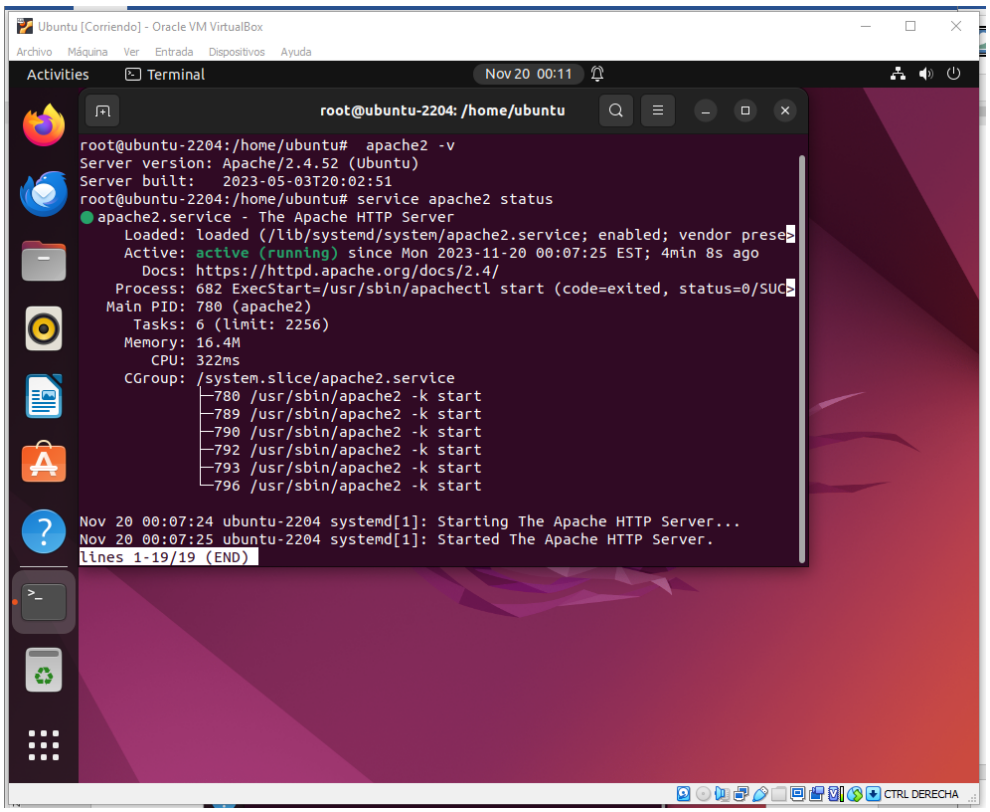


Figura 107: Arranque de la máquina

Luego de esta instalación, se procederá a instalar el Php para que arranque el servidor con una página web personalizada, utilizando el comando **apt install phplibapache2-mod-php.**

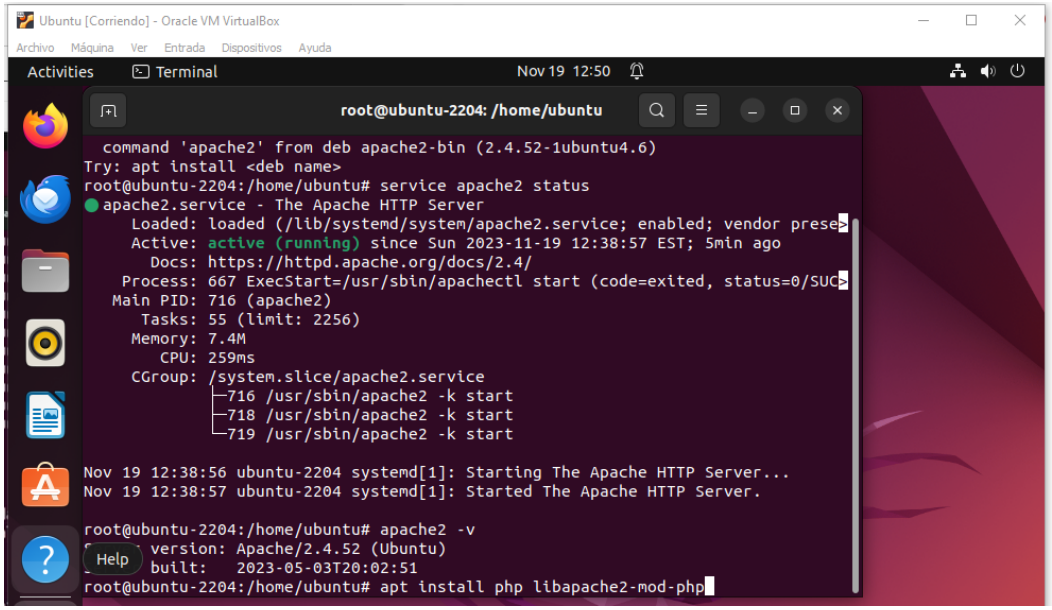


Figura 108: Instalar PHP

Para confirmar que la instalación fue exitosa se utilizará el comando **php -v** para verificar la versión que se está empleando.

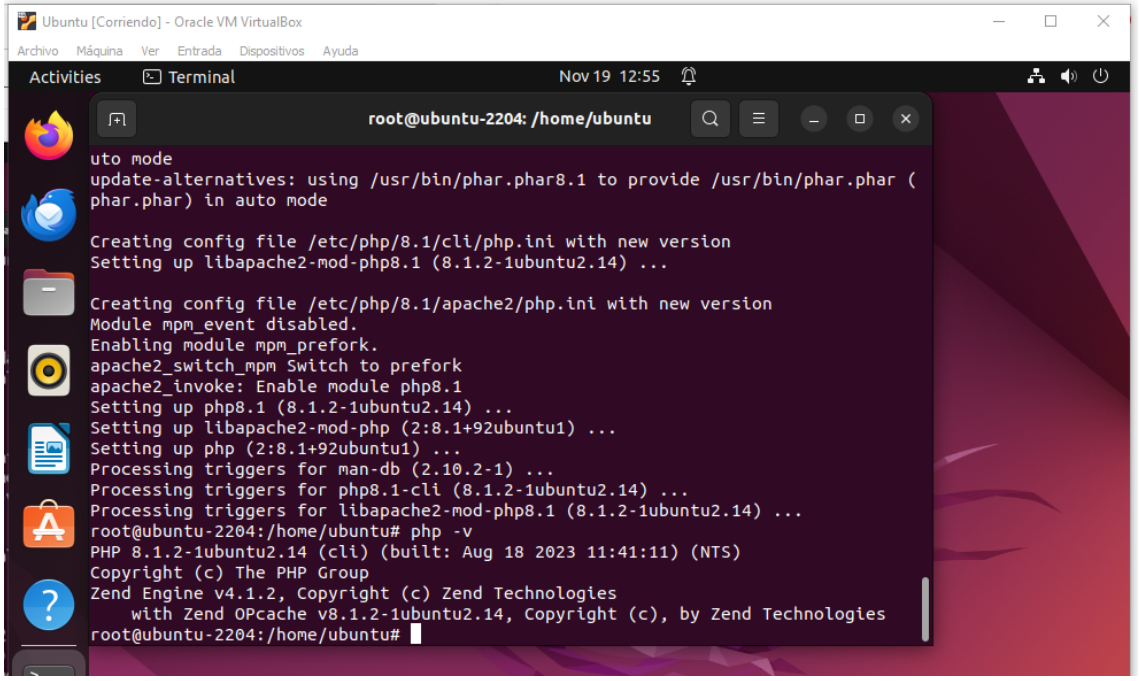


Figura 109: Confirmación de la instalación

Una vez completada esta instalación y verificada se accede a la carpeta de origen de esta instalación nueva, abriendo el directorio mediante el código **cd /var/www/html** y se ejecuta el comando **ls** para que me muestre el contenido de la carpeta y poder encontrar el archivo **index.html**.

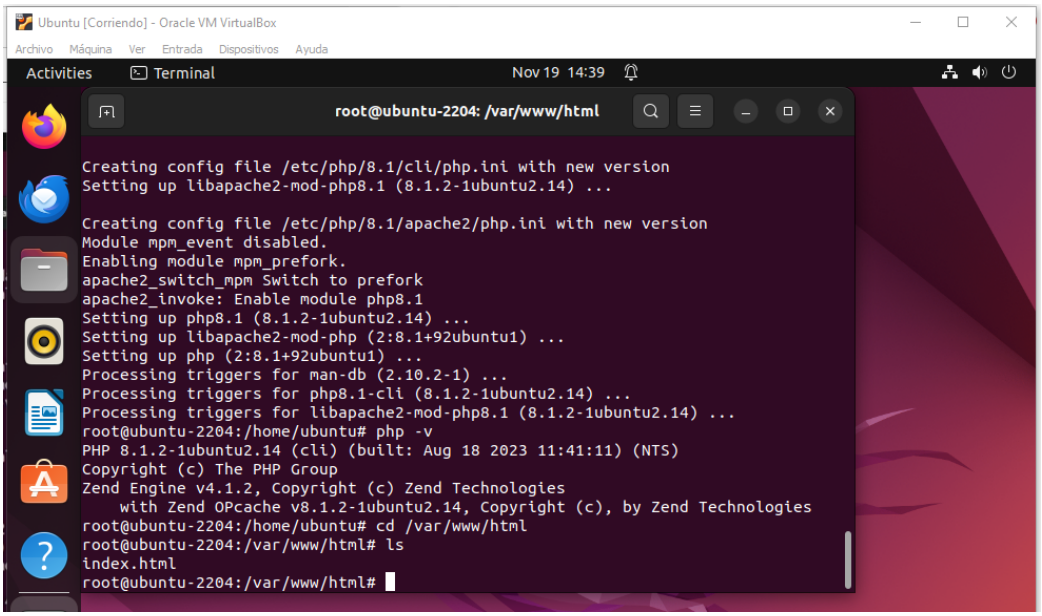


Figura 110: Acceso a la carpeta de origen

Se procederá a eliminar este archivo mediante el código **rm index.html** y luego verificando con **ls** que el contenido esté vacío.

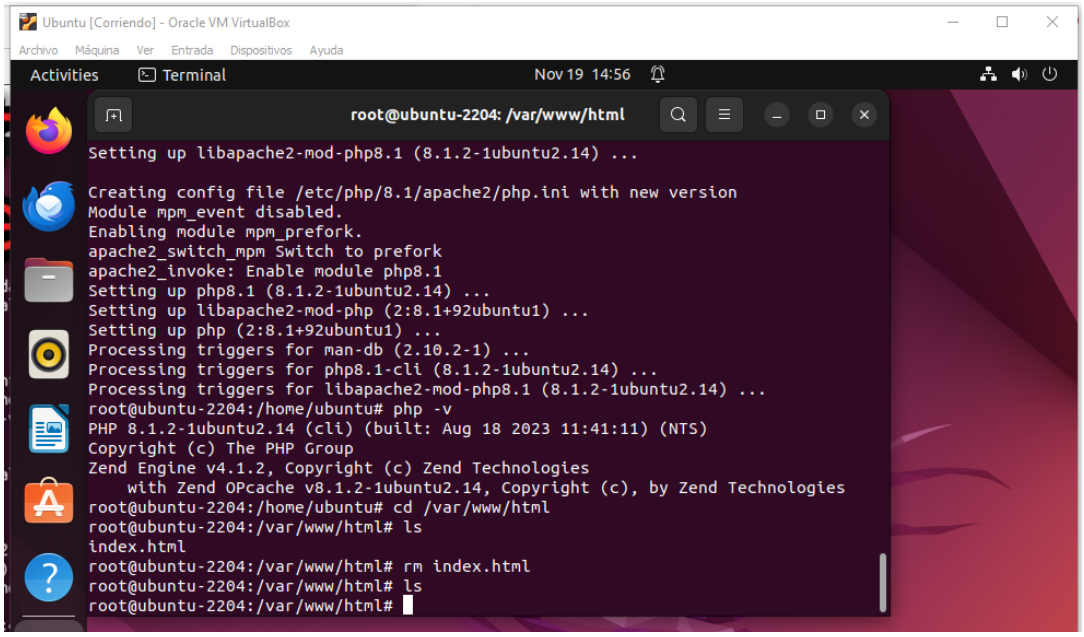


Figura 111: Eliminación del archivo

Se crea un nuevo documento index.php para la inicialización del servidor web; esta será la página de inicio. Para esto, se usa el comando **pico index.php**.

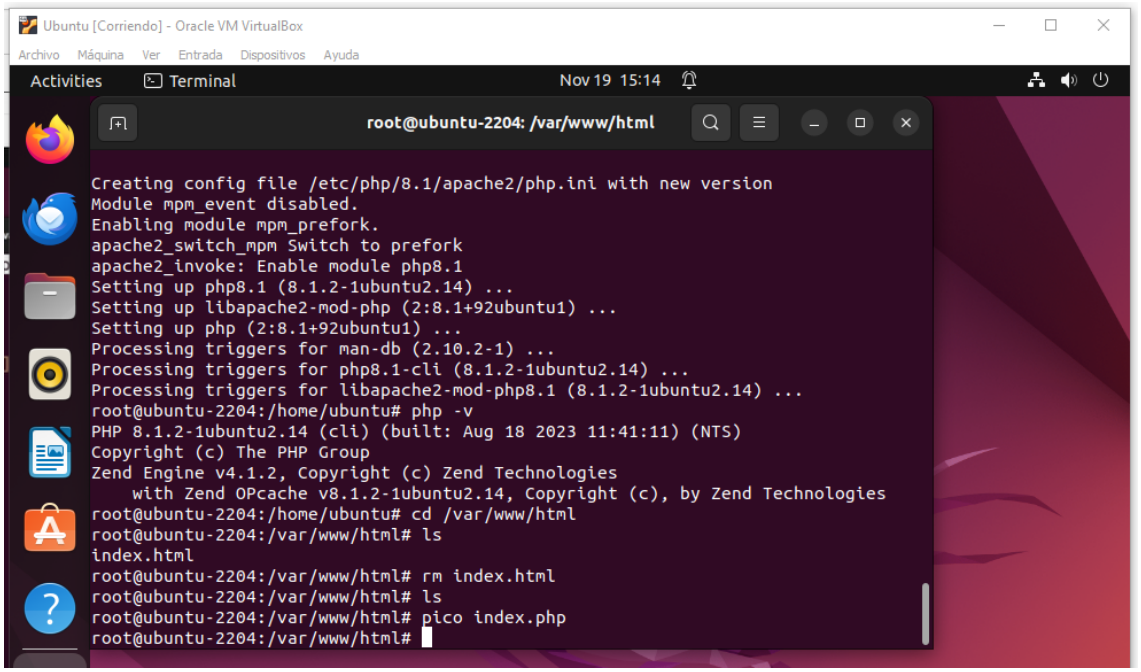


Figura 112: Creación de nuevo documento INDEX

Previamente se abrirá un editor de texto en donde se deberá poner la codificación de la página de inicio que se está creando.

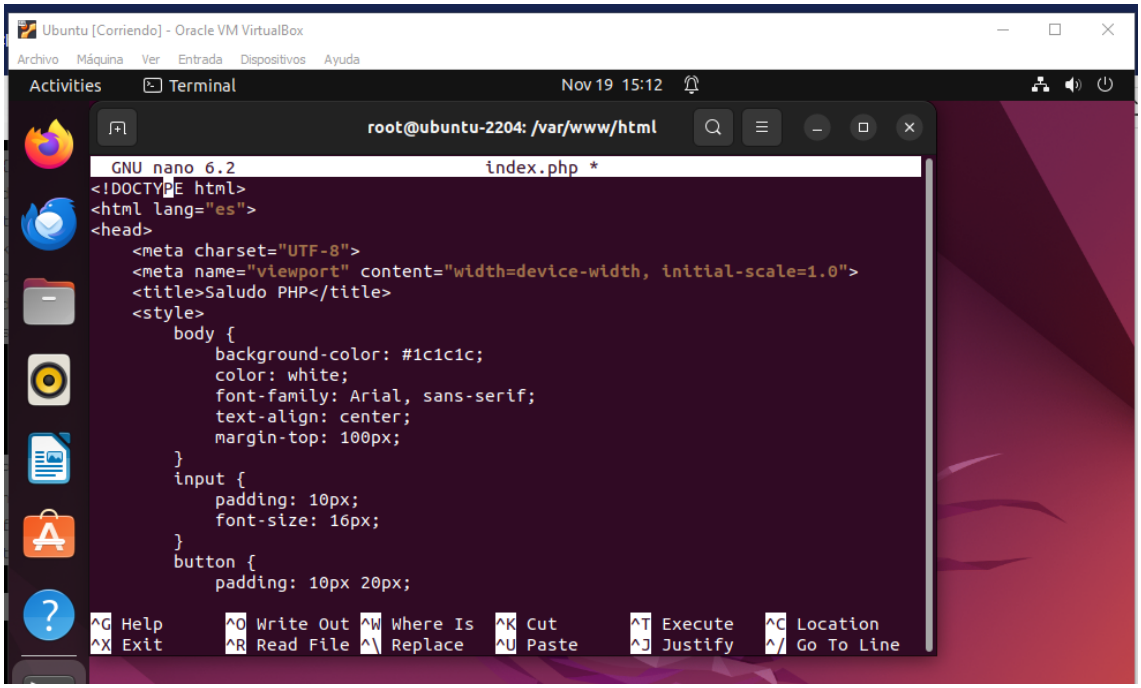


Figura 113: Abrir editor de texto

Una vez guardada la página, para que el servidor la reconozca se debe de reiniciar con el comando **service apache2 restart**.

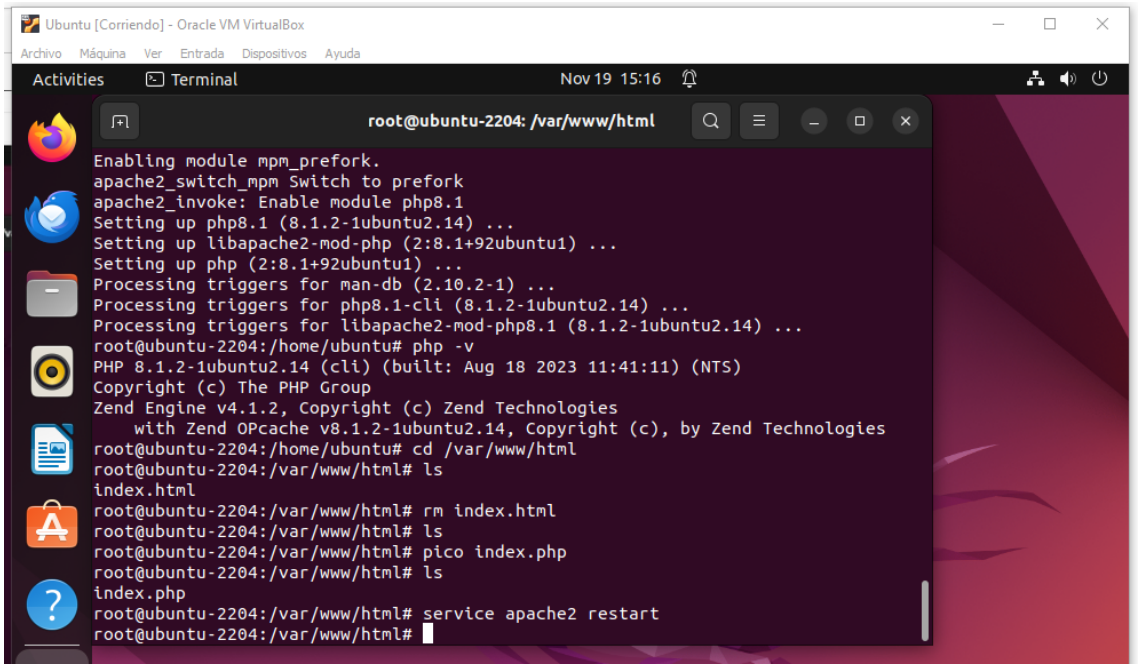


Figura 114: Guardar la página

Terminado este proceso, se constata que la página web índex arranque en los sistemas operativos tanto en la máquina de origen Windows 10 como en la otra máquina virtual de Kali.

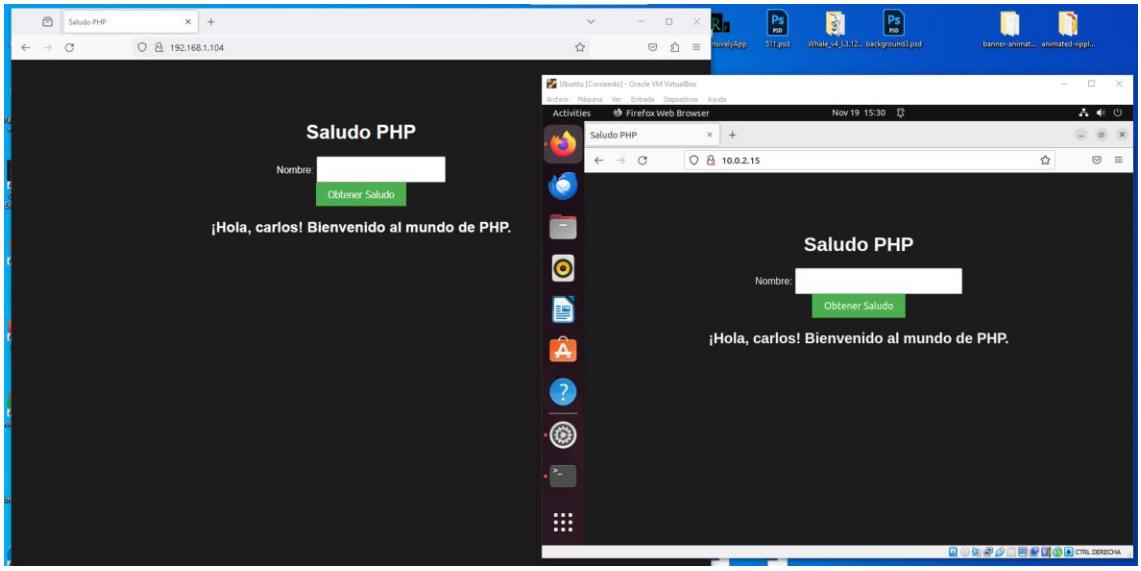


Figura 115: Arranque de los sistemas operativos

Monitoreo de los paquetes del servidor

Para monitorear un servidor en Ubuntu, se requiere una herramienta pre establecida, la cual, para poder arrancarla, solo se escribe el código **top**.

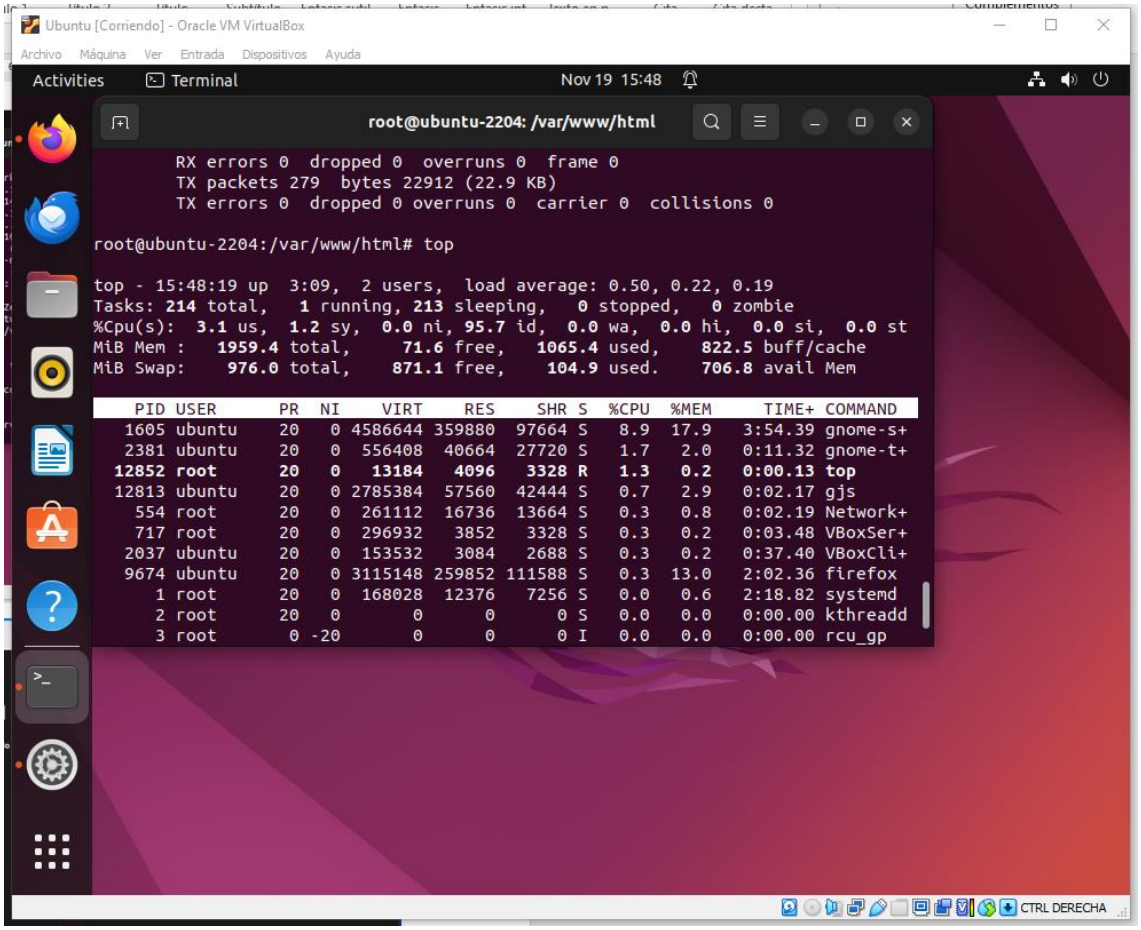


Figura 116: Monitoreo del servidor

Luego muestra los paquetes entrantes en el servidor, pero como este laboratorio requiere de un monitoreo más robusto en donde se puedan visualizar formatos como el porcentaje del CPU y otras herramientas de arranque, se procede a instalar htop, para ello se utiliza el código **apt install htop**.

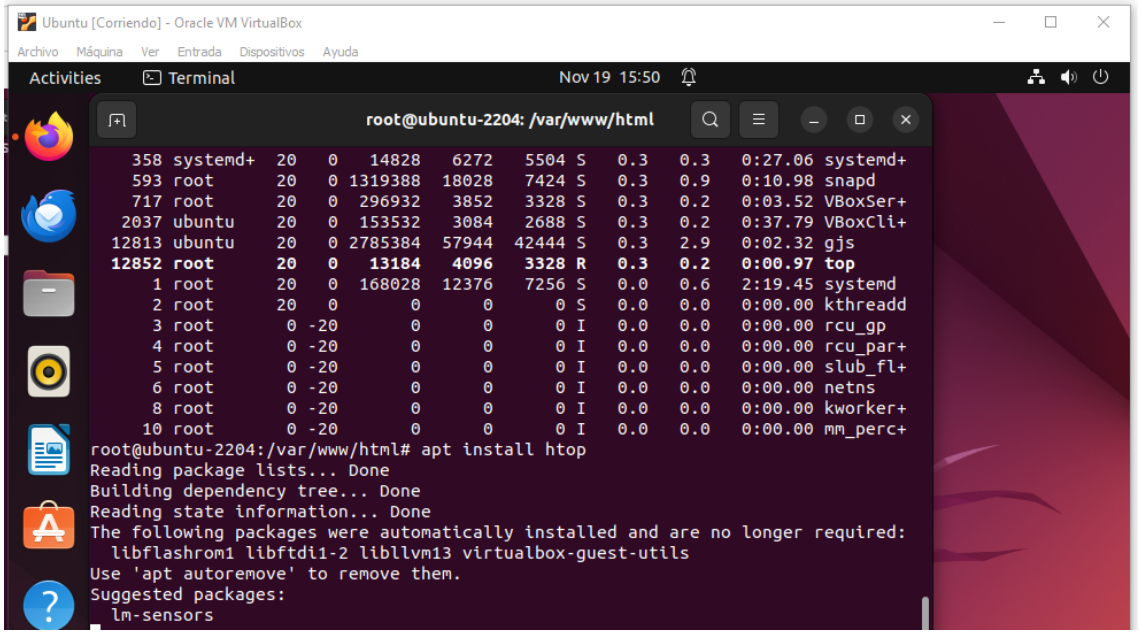


Figura 117: Paquetes entrantes en el servidor

El cual, al ejecutarse se mostrará de la siguiente manera.

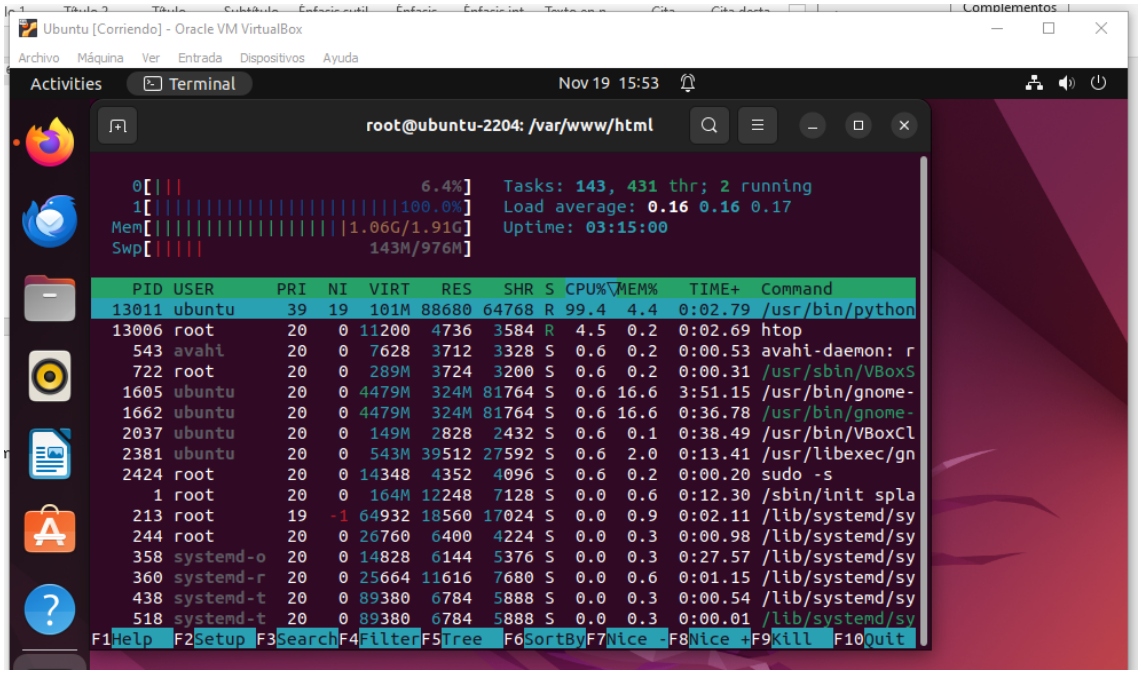


Figura 118: Ejecución

Para culminar con las herramientas de monitoreo, se procederá a instalar el wireshark mediante el código **apt install wireshark**.

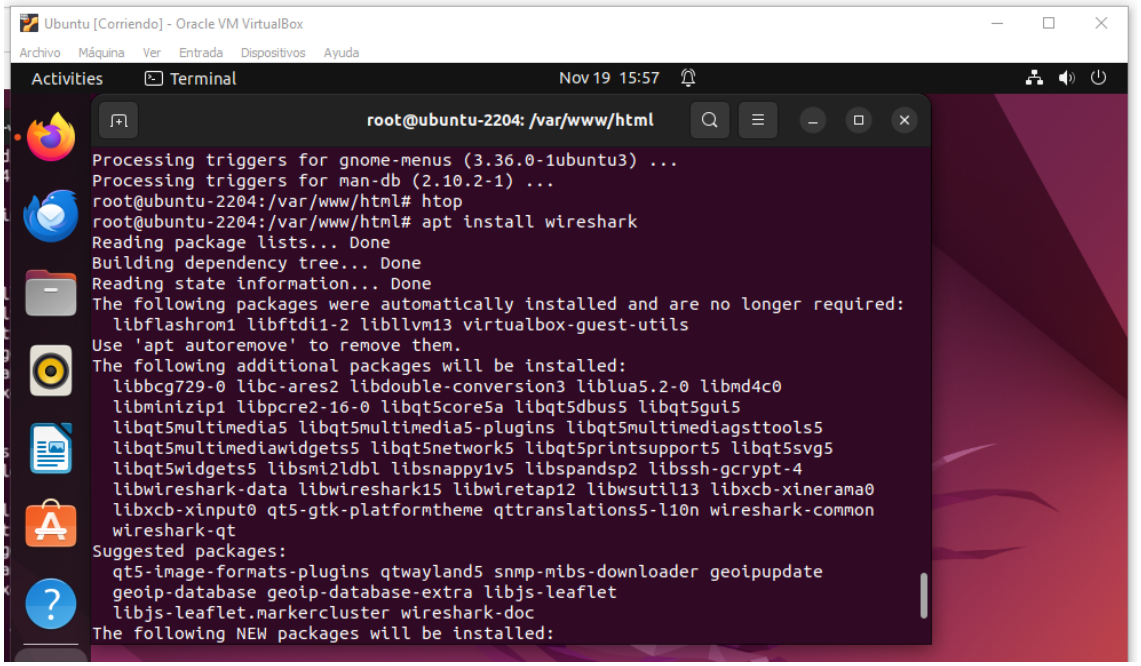


Figura 119: Instalación de Wireshark

A diferencia de las otras herramientas, esta se presenta de manera visual.

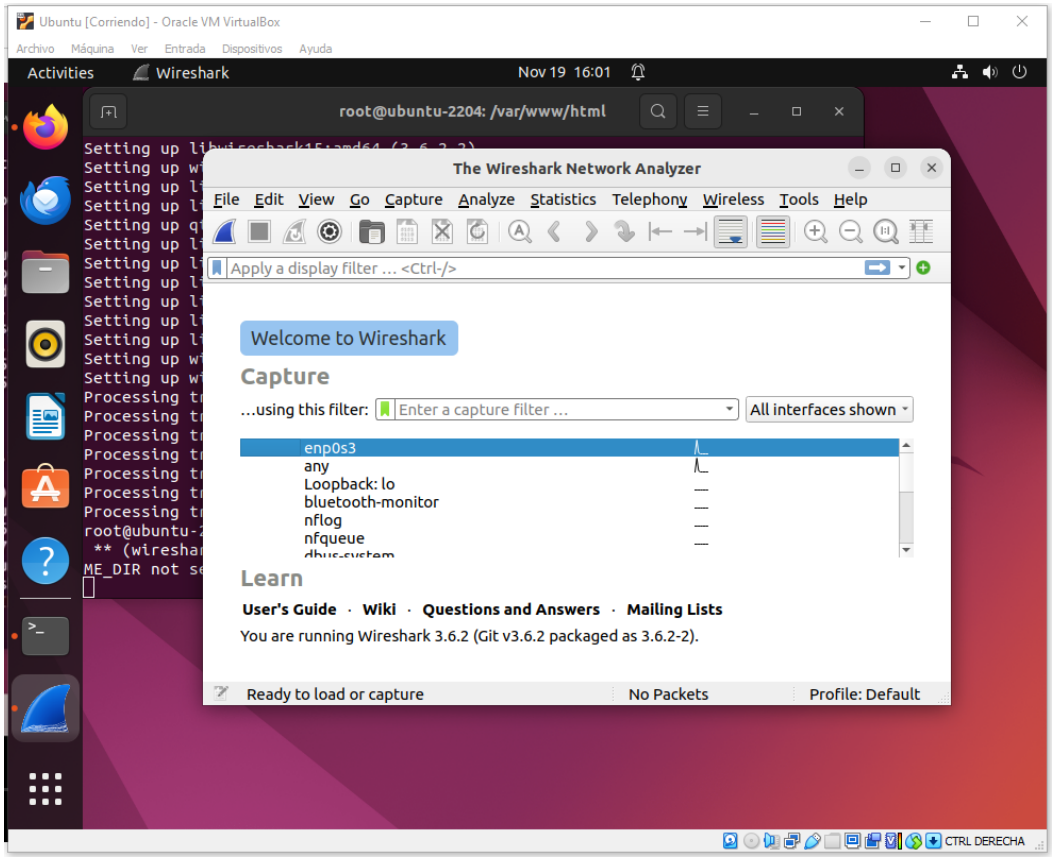


Figura 120: Presentación de la herramienta

Personalización para máquina atacante Kali

Para la configuración de la máquina atacante, de la misma forma que la máquina del servidor, se debe realizar una actualización.

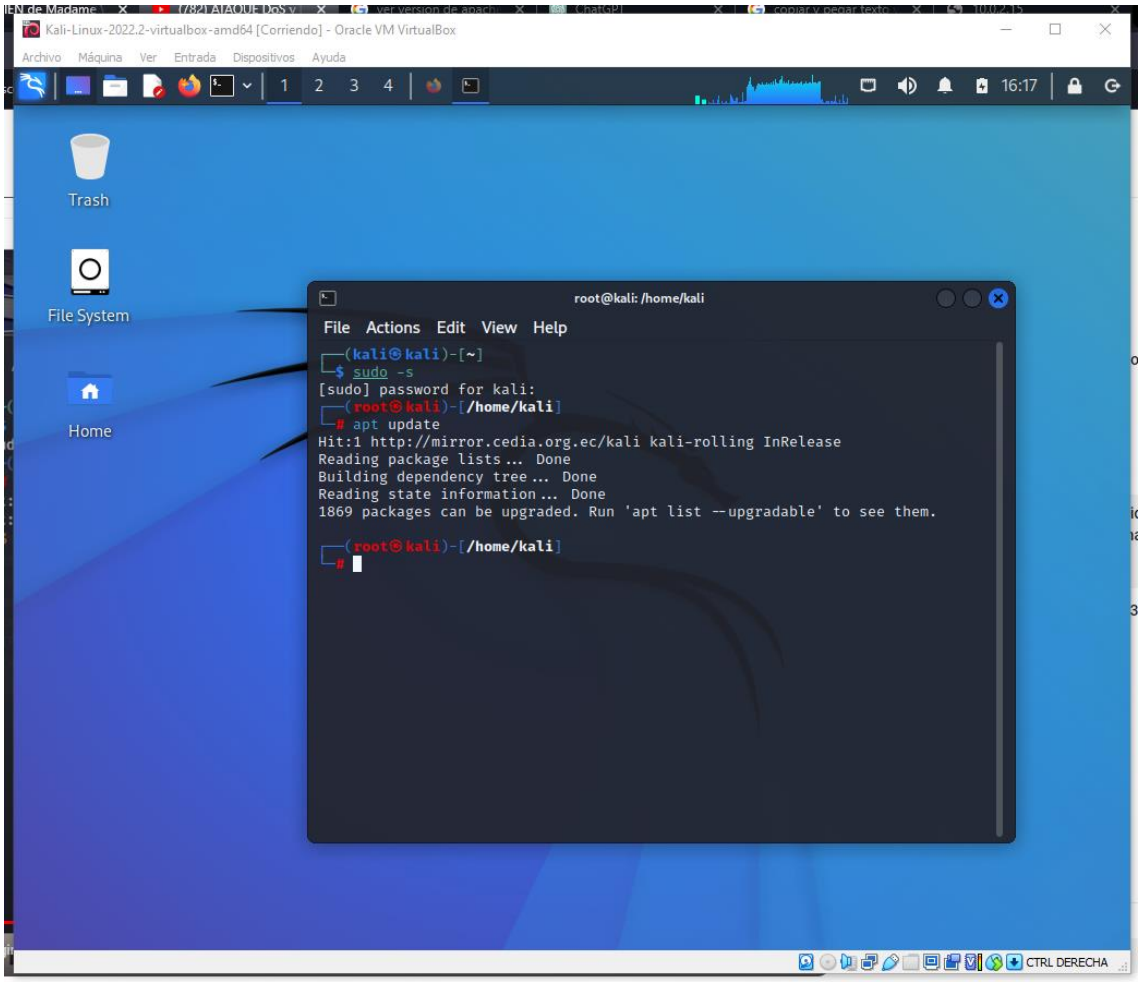


Figura 121: Configuración de la máquina atacante

Ataque y pruebas al servidor

Para el envío del empaquetado se utilizará la herramienta hping3, cuyo objetivo es enviar varios paquetes a un servidor, de los cuales se puede modificar su tamaño y cantidad de envío, direccionándolos a la ip del servidor. Para esto, se escribirá el código **hping3 -c 200000 -d 120 -S -p 80 --flood --rand-source [IP victima].**

Código	Propósito
-c (# paquetes)	Cantidad de paquetes a enviar al ataque
-d (# tamaño)	Tamaño de cada paquete enviado
-S	Protocolo a alterar

-p (# puerto)	La numeración del puerto
--flood	Velocidad del envío (flood(inmediata))
--rand-source	Genera ip aleatorio en cada envío
ip	Ip del servidor a atacar

Tabla 4: Ataque y pruebas al servidor

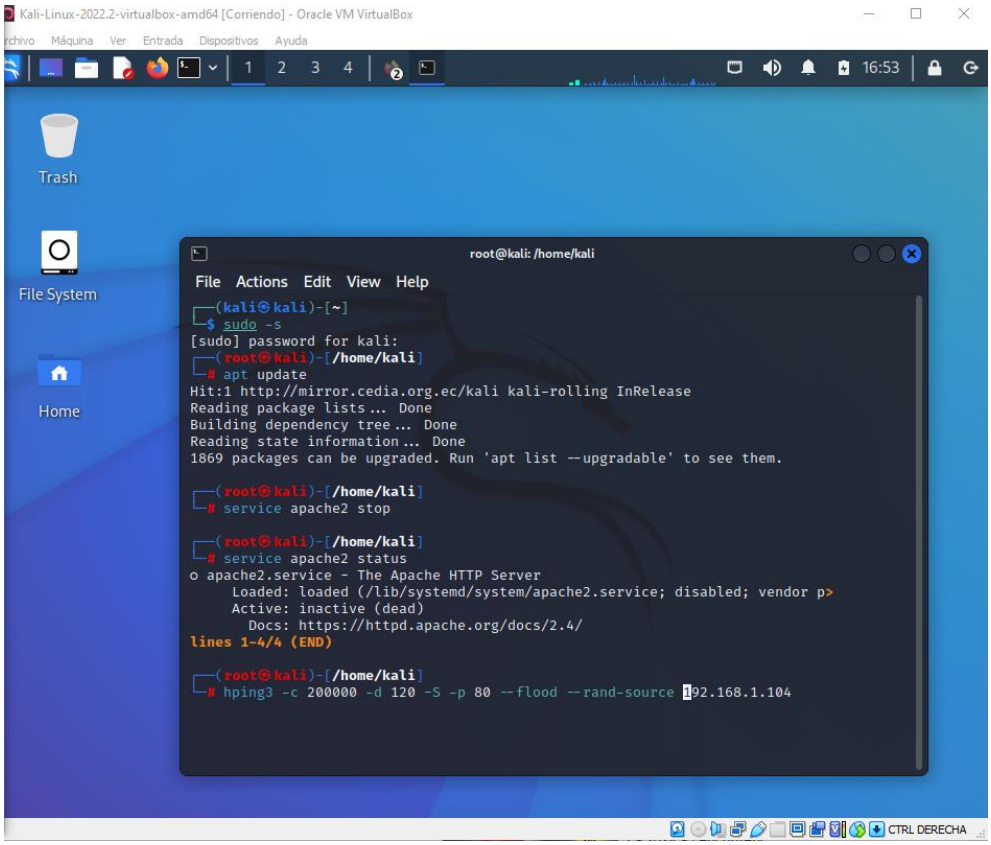
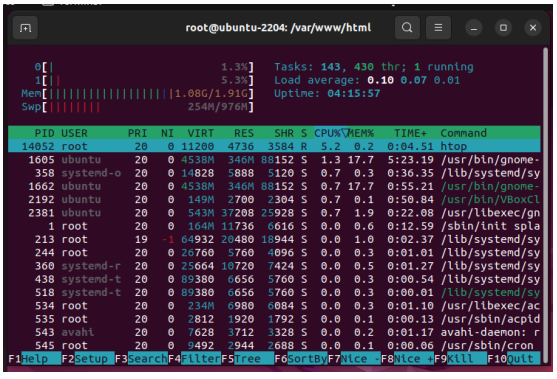


Figura 122: Ataque al servidor

Una vez arrancado este envío de paquetes, se comienza a monitorear en el Ubuntu con el comando htop de la consola y se empezará a mostrar la diferencia en el rendimiento.



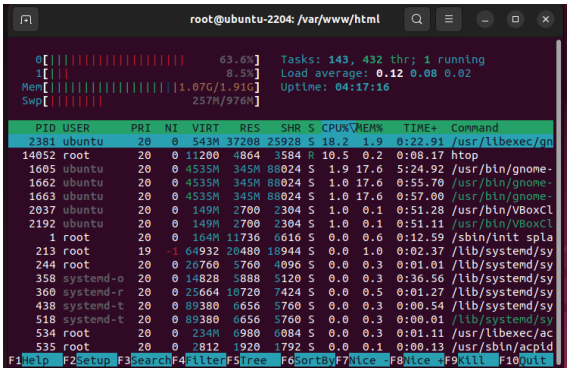


Figura 123: Monitoreo de Ubuntu

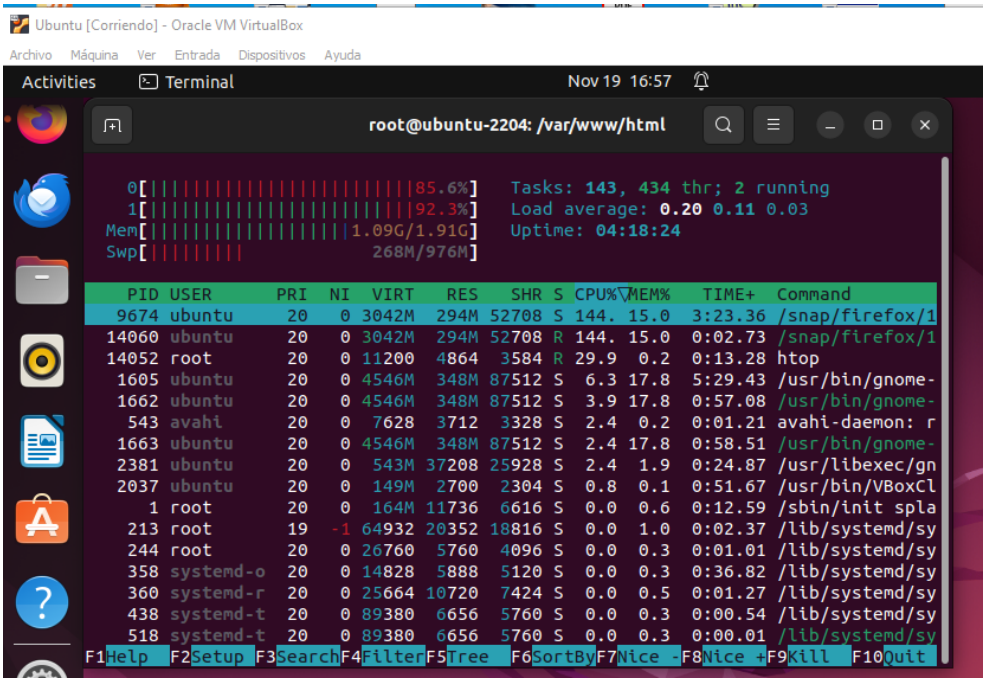


Figura 124: Muestra de diferencia del rendimiento

En este proceso si se elimina -c, el envío de empaquetado se hará infinito.

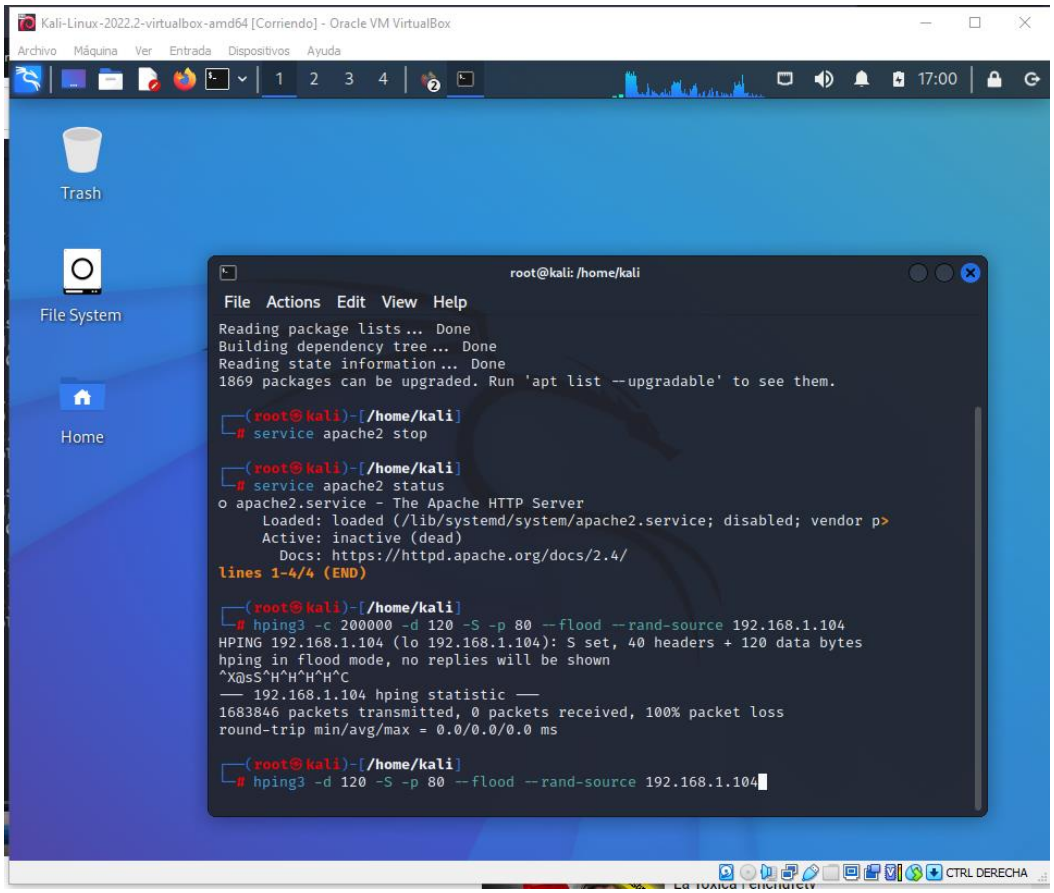


Figura 125: Empaquetado infinito

Mostrando una considerable diferencia al ataque anterior.

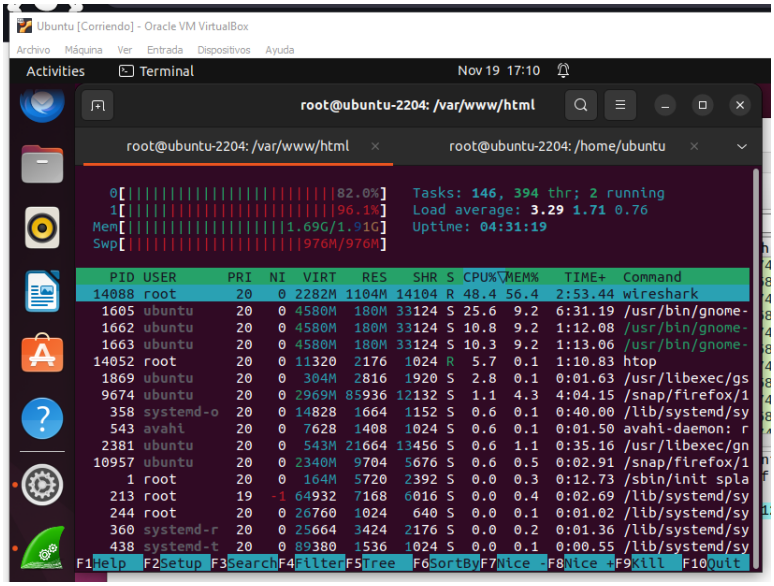


Figura 126: Diferencia del ataque anterior

En el terminal de Ubuntu se abrió otra pestaña para arrancar el wireshark.

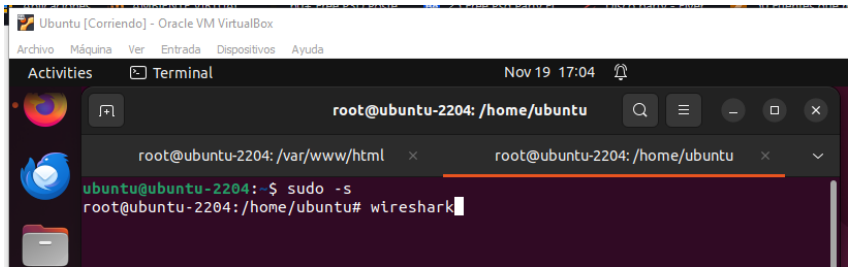


Figura 127: Terminal de Ubuntu

Se da doble clic a la red en este caso enp0s3 y se visualiza el monitoreo de paquetes.

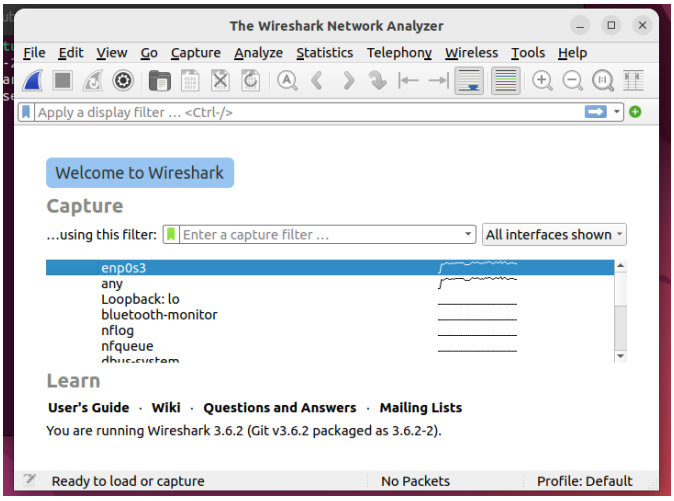


Figura 128: Visualización del monitoreo de paquetes

Mostrando como resultado la ip del destinatario y se observa que los paquetes se envían sin fin con protocolo TCP.

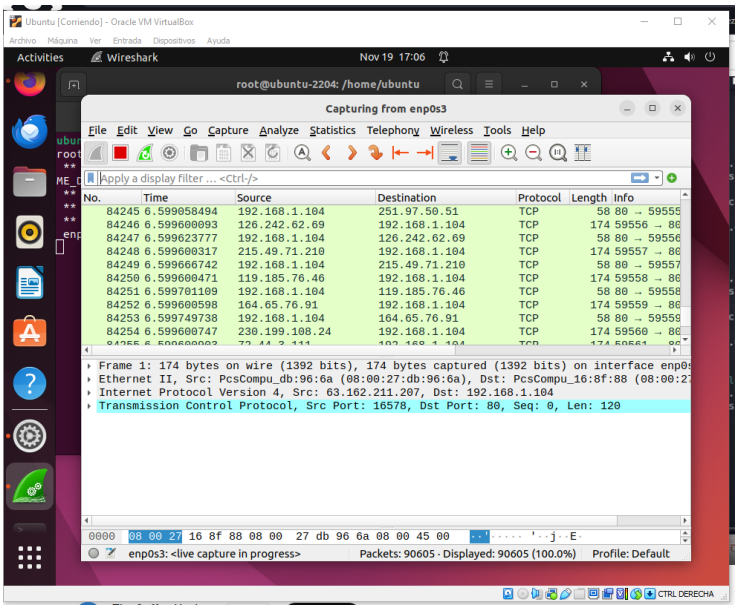


Figura 129: IP del destinatario

Si se usa otro protocolo de ataque de envío de paquetes para saturar el servidor y ver activo este ataque, se escribe el comando **hping3 [IP victima] --flood --rand-source –icmp**.

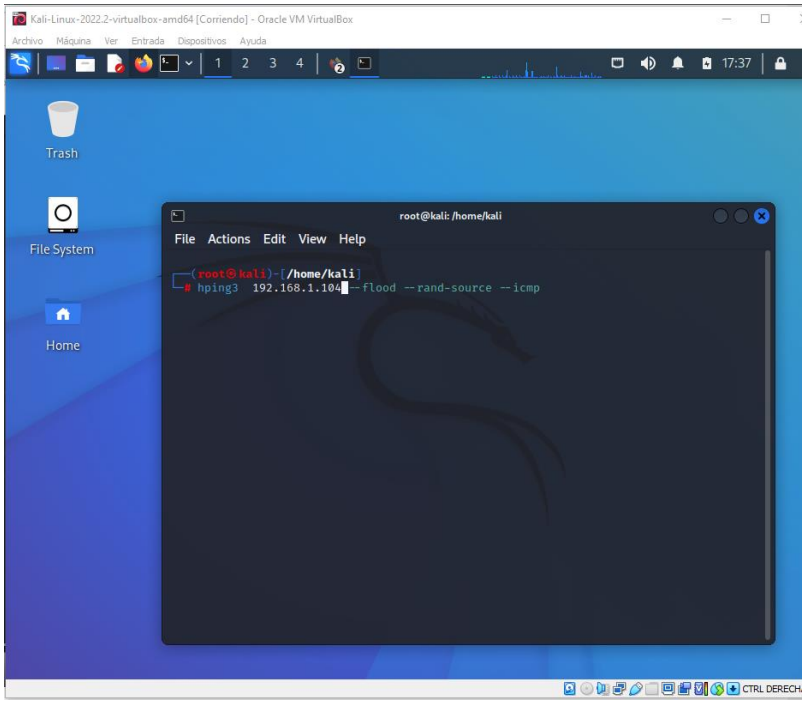


Figura 130: Protocolo de ataque

Mostrando como resultado, un índice de llenado al usar los dos ataques al mismo tiempo.

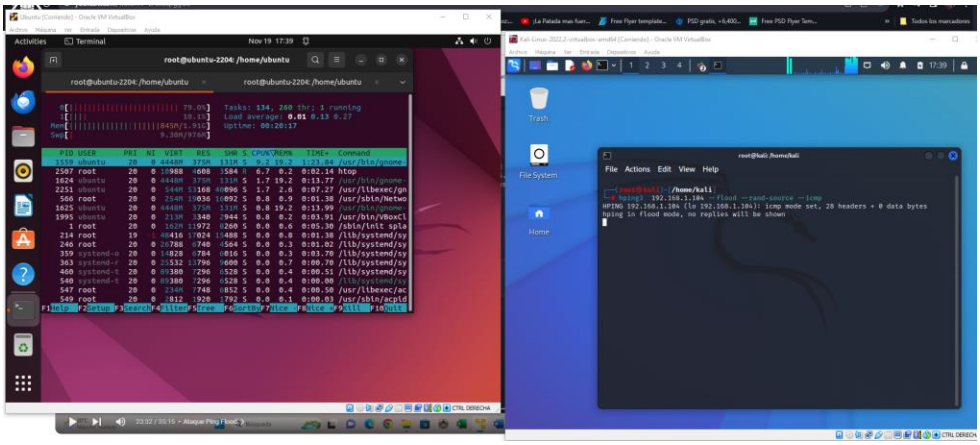


Figura 131: Resultado

Esto provocará un volcado de memoria, el cual hará que el servidor web se demore al cargar.

Figura 132: Volcado de memoria

Y si se abre en otro navegador no podrá arrancar.

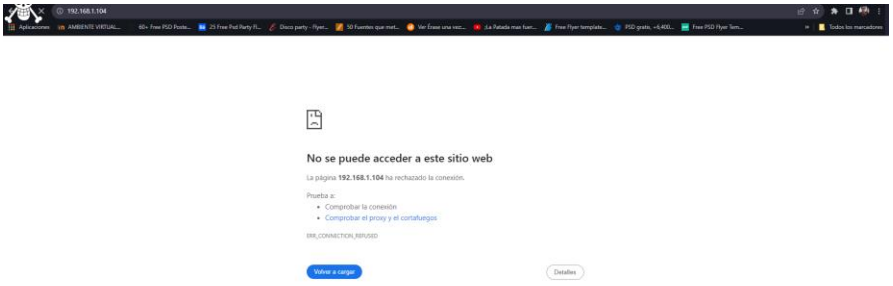


Figura 133: Navegador

Anexo 9. Caso 2 – Infección de malware

Para este caso forense de infección malware, se utilizará el Windows 10 del equipo, además se empleará de forma virtualizada los sistemas operativos Windows 7 y Ubuntu, que previamente se instalarán en la máquina virtual, para luego proceder a instalar las siguientes configuraciones y herramientas para cada una de las máquinas virtuales.

Se debe tomar en cuenta que la máquina Ubuntu será la encargada de ser el servidor de datos y la máquina víctima será el Windows 7, al ser una prueba de laboratorio con riesgo de infectar la máquina física, el modo de red cambiará para tener comunicación solo entre estas dos máquinas.

Preparación e instalación de los sistemas operativos

Al igual que el ataque anterior, se debe actualizar el sistema, pero al ya estar actualizado este paso se omitirá. Se debe recordar que las redes al inicio deben de estar como red Nat para poder tener internet y hacer las descargas debidas de las herramientas.

Se instala el paquete de locatebase para poder visualizar y realizar cambios de las direcciones ip del equipo Ubuntu; para esto se usa el comando **apt install plocate**.

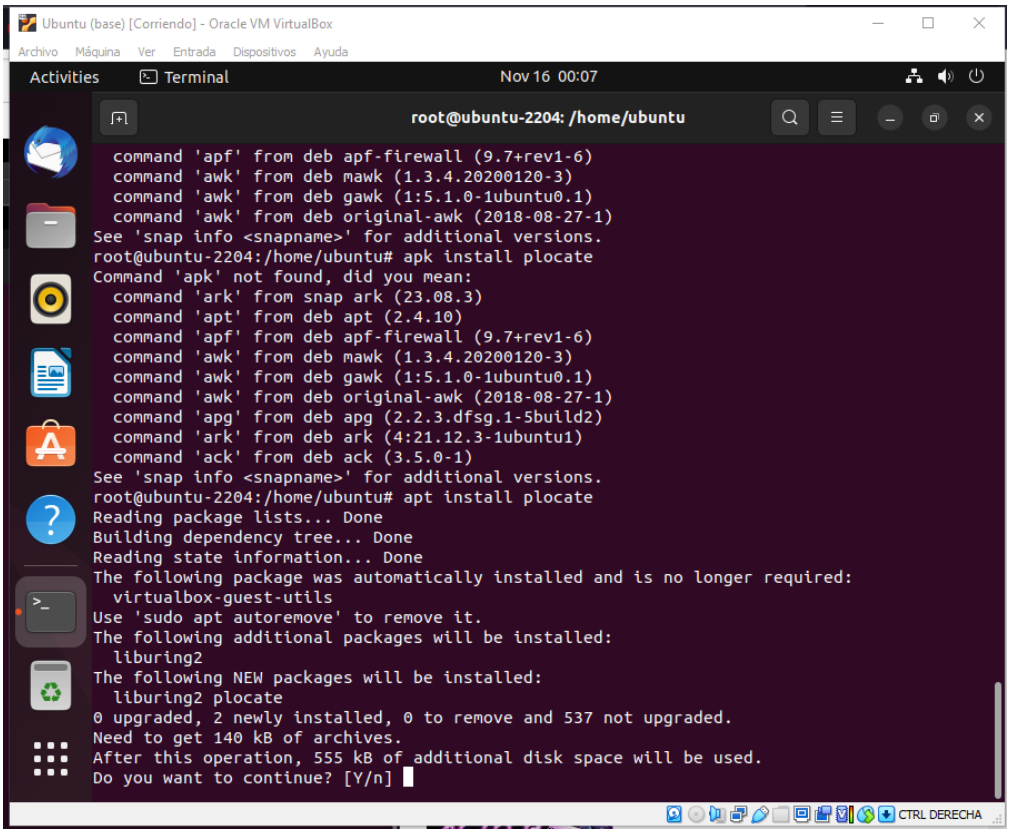


Figura 134: Preparación de los S.O.

Se realiza una prueba con ifconfig para verificar que esté en funcionamiento el comando de identificación de las redes.

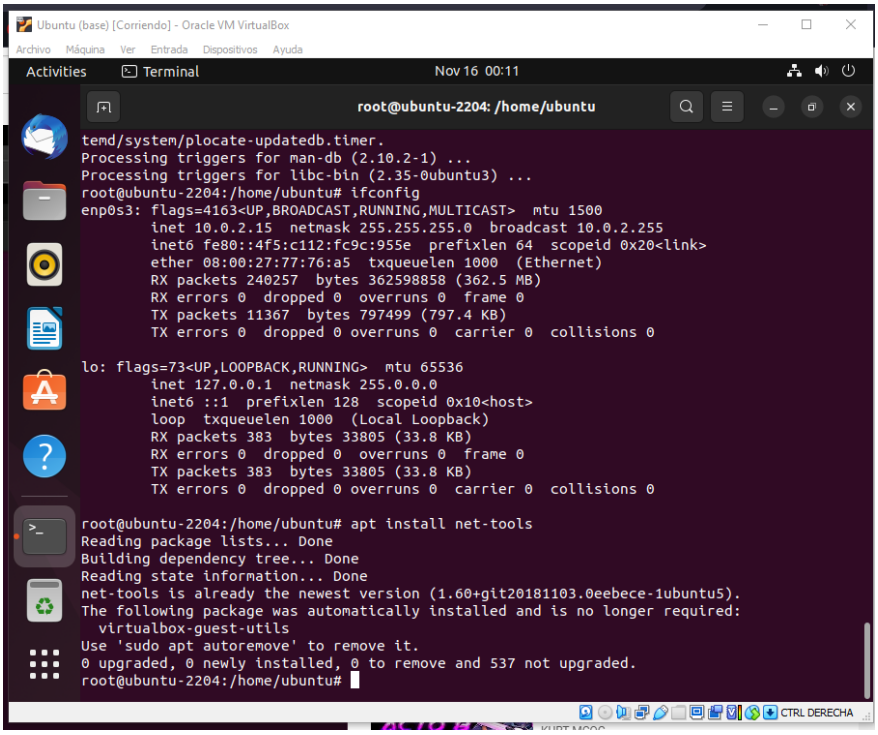


Figura 135: Prueba de ifconfig

Una vez ejecutado este comando, se ejecuta el navegador Mozilla para instalar el **Fakenet,** que permitirá el monitoreo del ataque que se va a realizar al sistema operativo Windows en la red por malware.

Este programa se descargará del repositorio del GitHub y que a su vez indicará la forma de instalarlo en la máquina virtual.

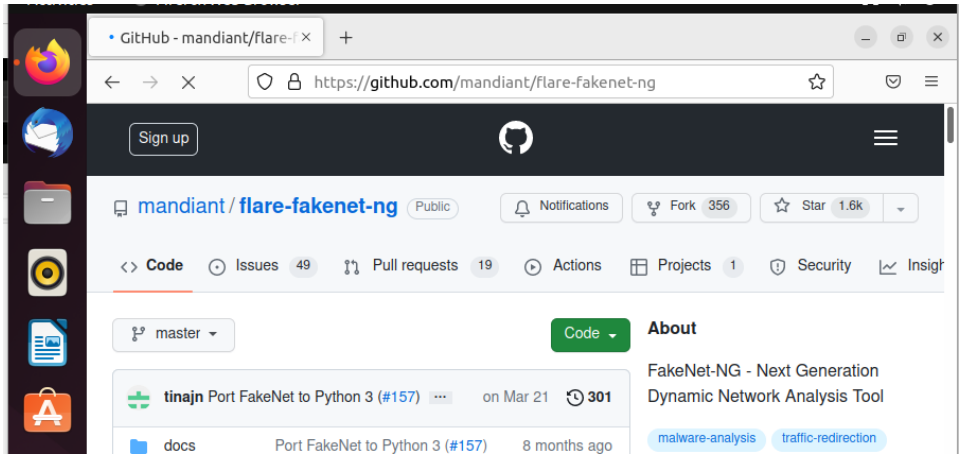


Figura 136: Repositorio de GitHub

Previo a la instalación de este repositorio, se debe ejecutar la herramienta net-tools que permitirá el acceso a las instalaciones del GitHub, utilizando la línea de código **apt install net-tools** para su uso.

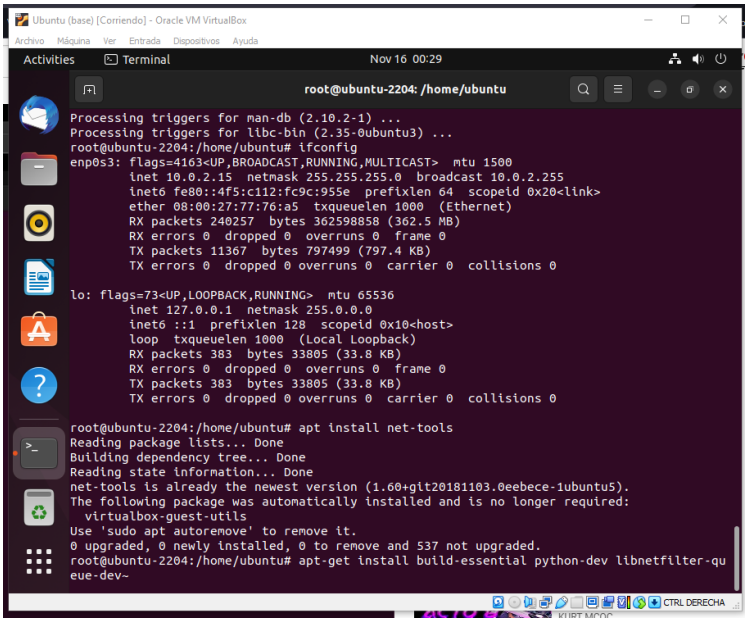


Figura 137: Ejecutar herramienta net tools

Una vez hecho esto, se procede a la instalación del repositorio del GitHub, pero se presentan problemas con el uso del Python, el cual también se debe ejecutar con anticipación.

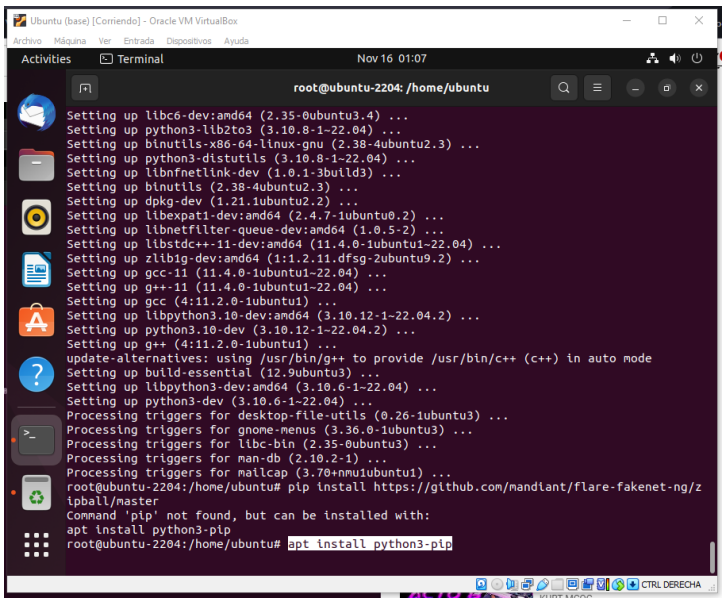


Figura 138: Instalación del repositorio de GitHub

Una vez resueltos los inconvenientes de requerimiento de instalación, se procede a instalar el repositorio GitHub.

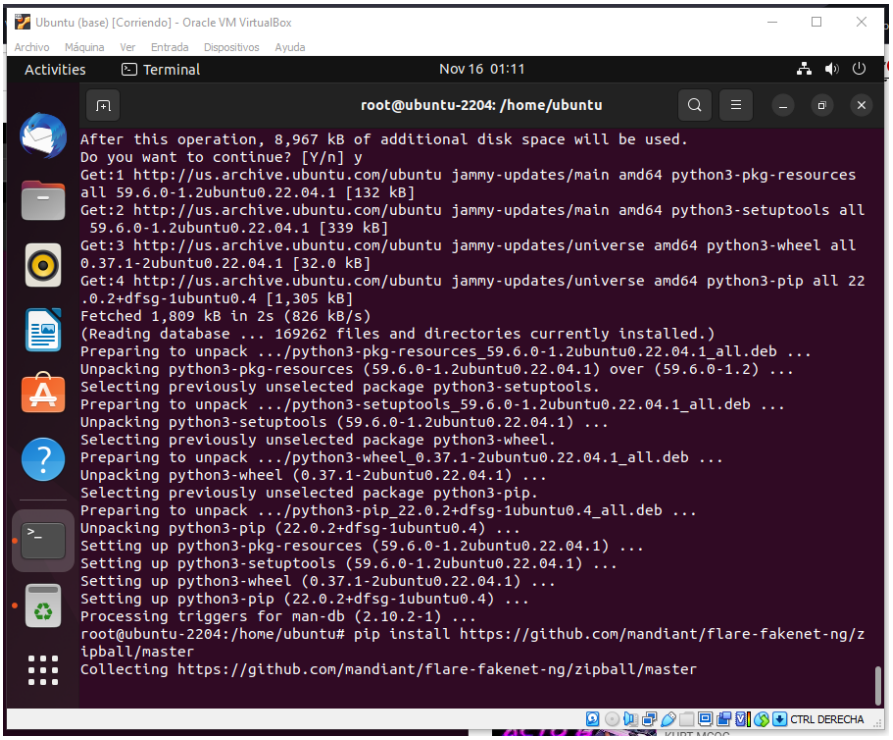


Figura 139: Instalación del repositorio

Se realizan pruebas para ver el funcionamiento y arranque del **fakenet-ng**.

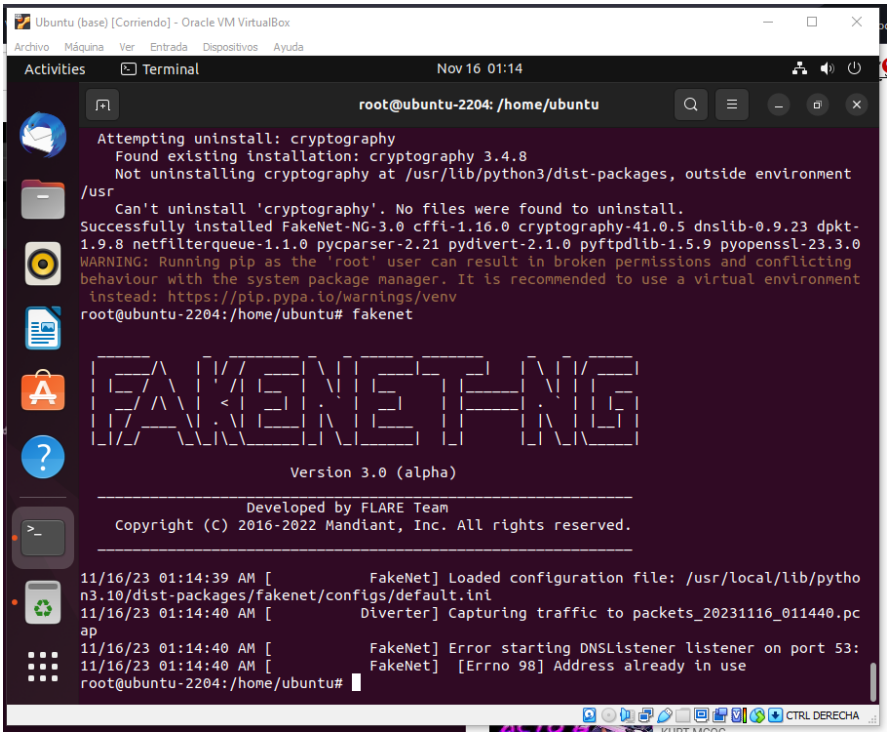


Figura 140: Pruebas de arranque y funcionamiento

Implementación y adecuación del Windows

Utilizando el Google Chrome, se busca thezzo malware, el cual es un repositorio en donde se hallará una variedad de malware para la práctica (los mismos están activos, por ende, es recomendable utilizar máquinas virtuales aisladas de la red).

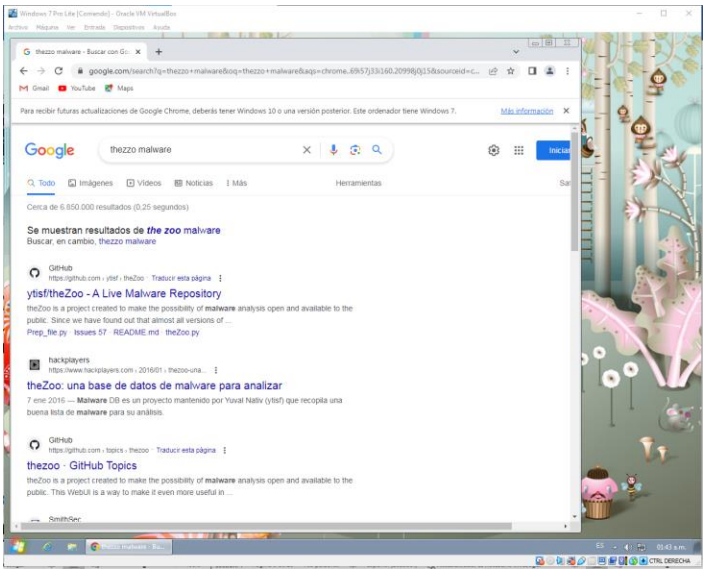


Figura 141: Adecuación del Windows

Esto también se encuentra en un repositorio de GitHub, en el cual se indagará hasta encontrar el ransomware que se usará.

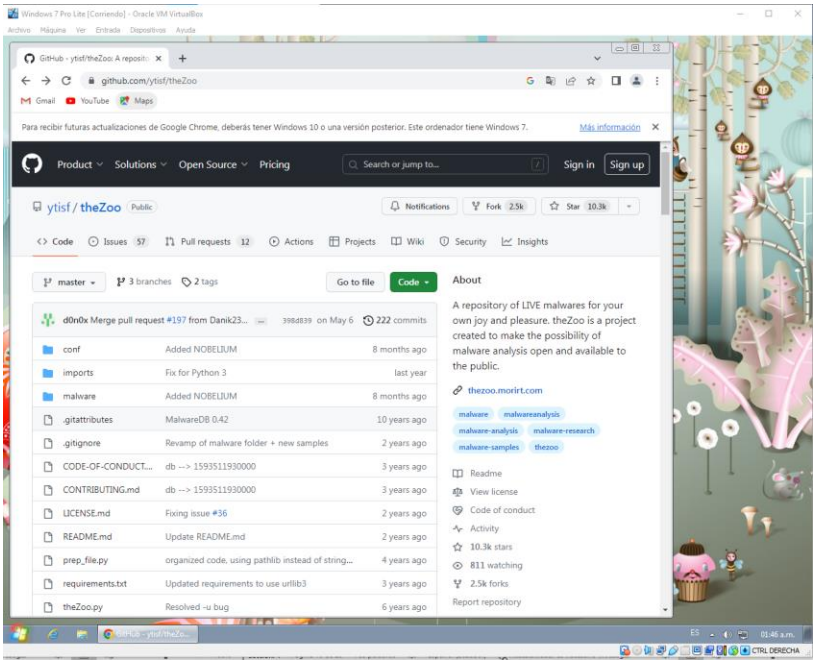


Figura 142: Indagar el ransomware

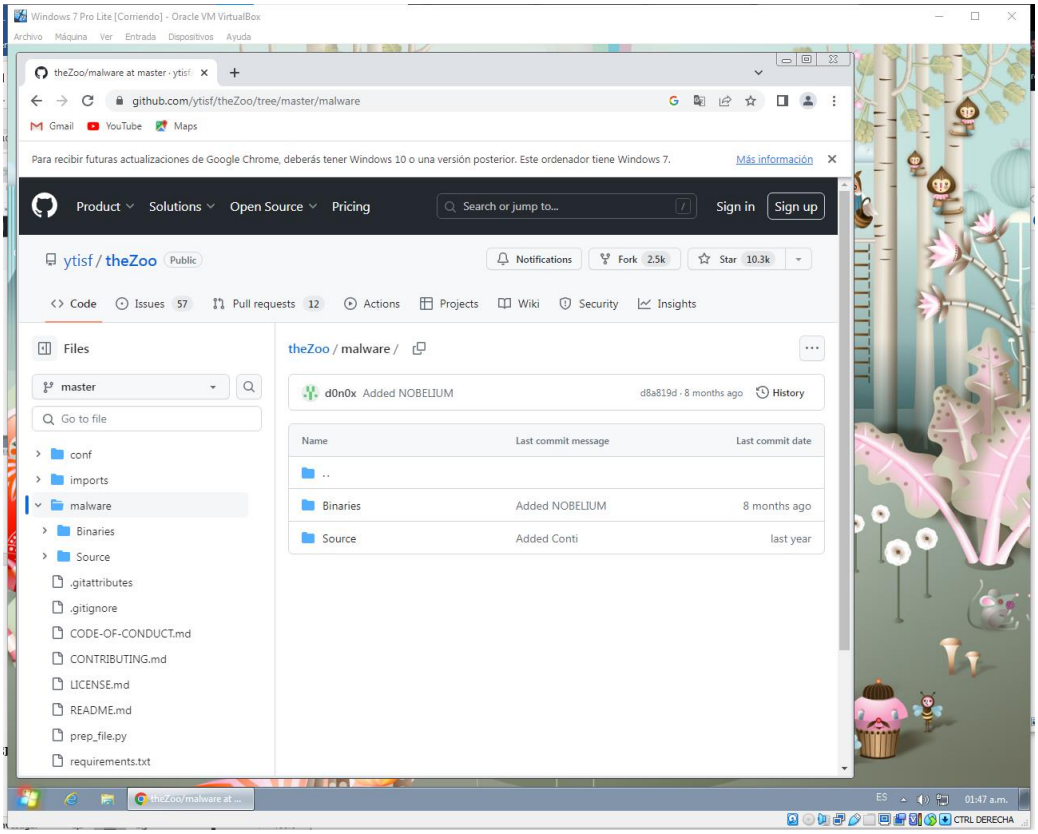


Figura 143: Indagar el ransomware

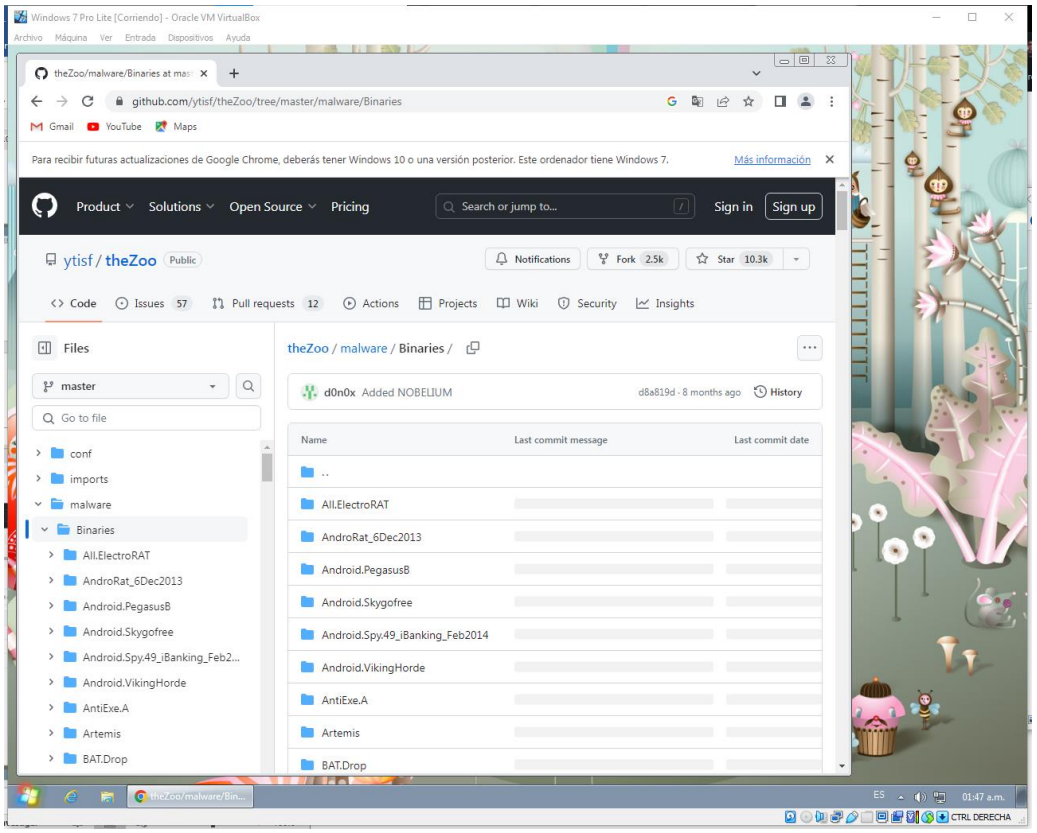


Figura 144: Indagar el ransomware

Se busca y se descarga el ransomware TeslaCrypt.

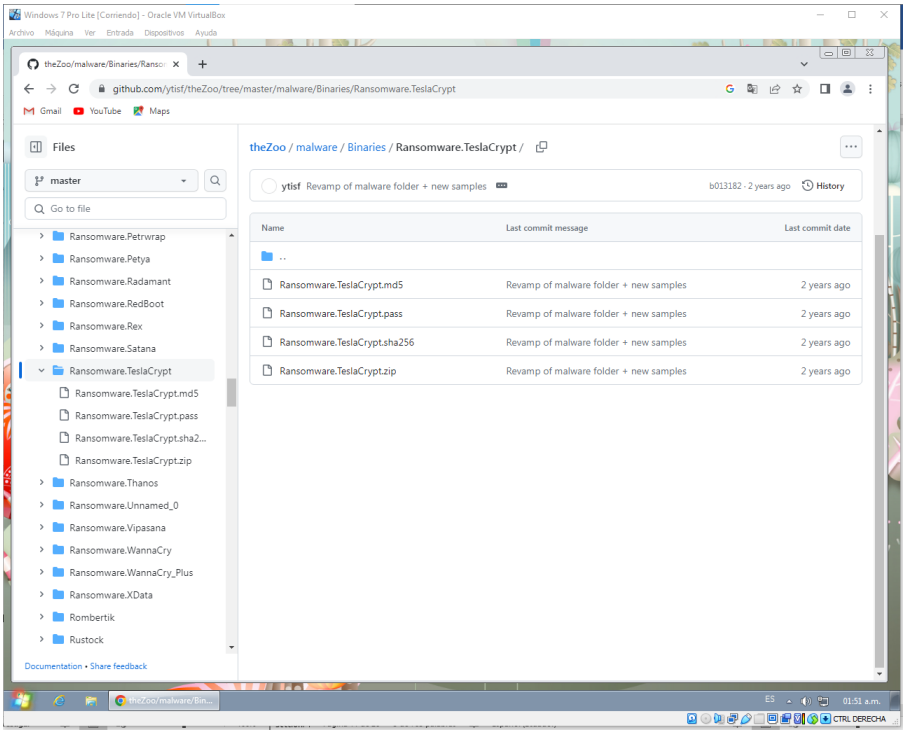


Figura 145: Descarga del ransomware

Se debe tener en cuenta que las defensas del Windows Firewall u otro antivirus deben mantenerse desactivadas.

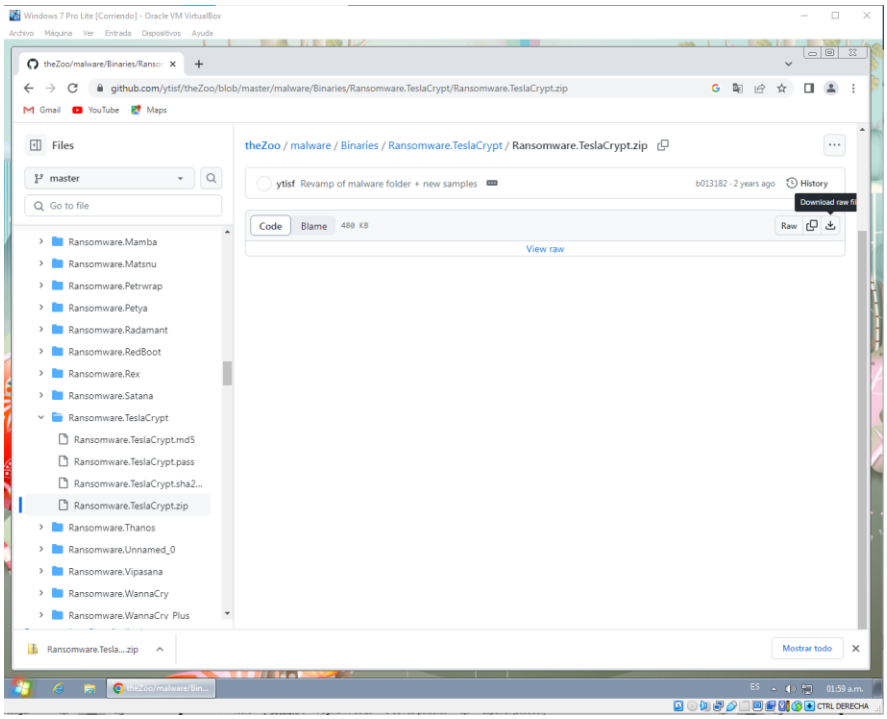


Figura 146: Defensa del Windows Firewall

Este archivo en WinRAR, se deberá pasar al escritorio para tenerlo al alcance del ataque.

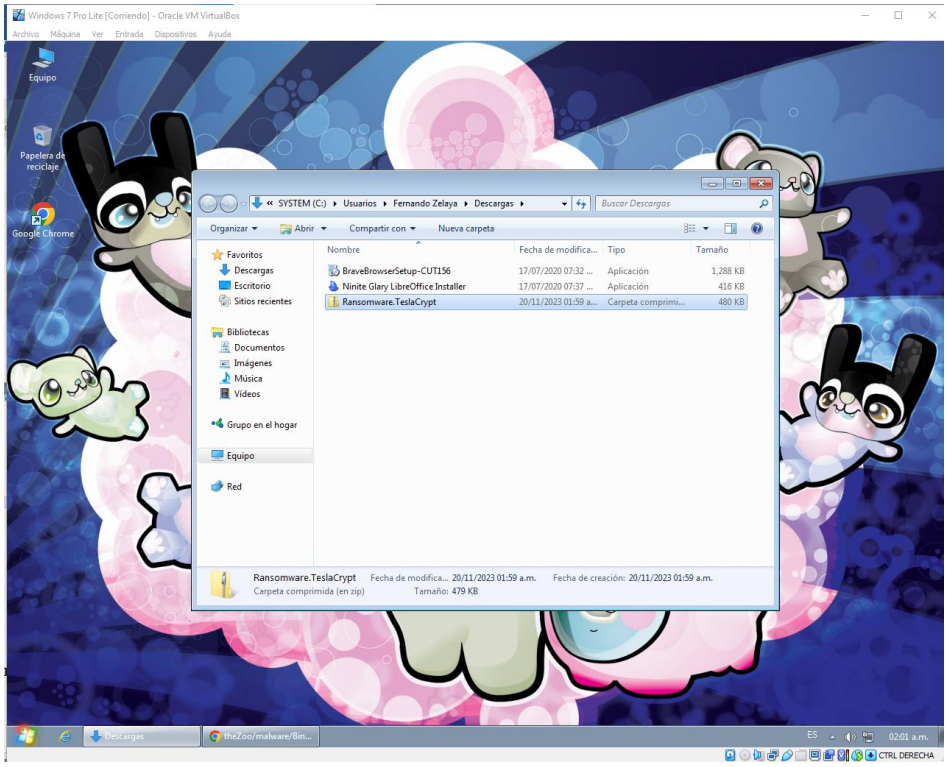


Figura 147: Archivo en WinRAR

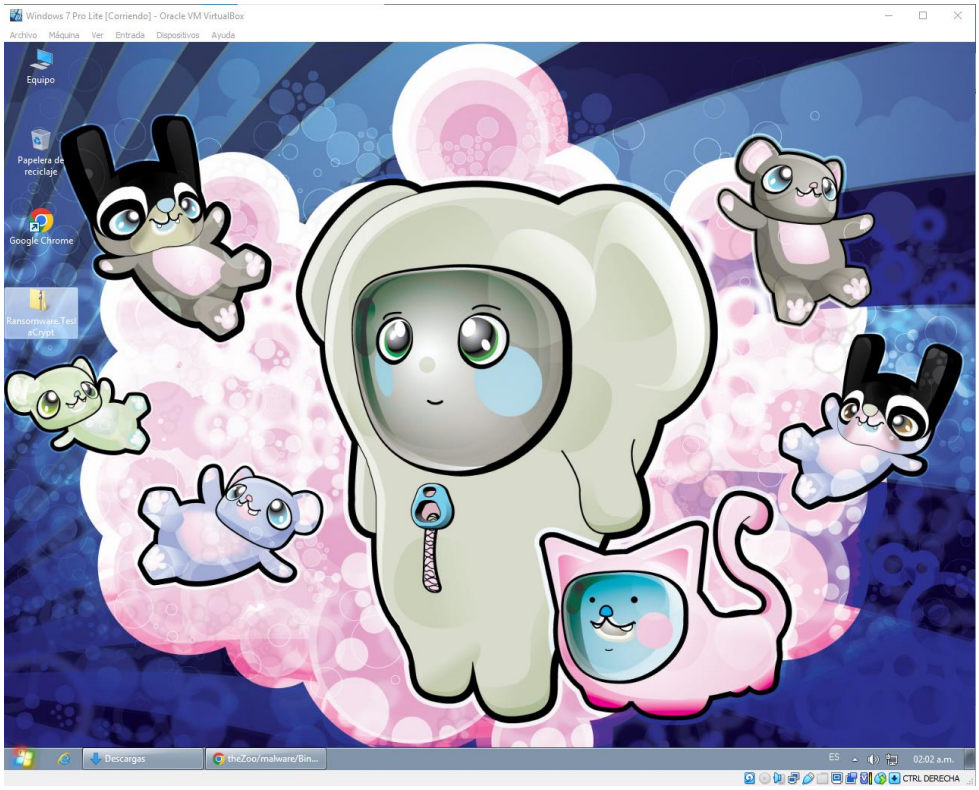


Figura 148: Pasar al escritorio

Configuración de la red

Para la configuración de la red privada, se tendrán que cerrar las máquinas virtualizadas e ingresar a una configuración de red del virtual box.

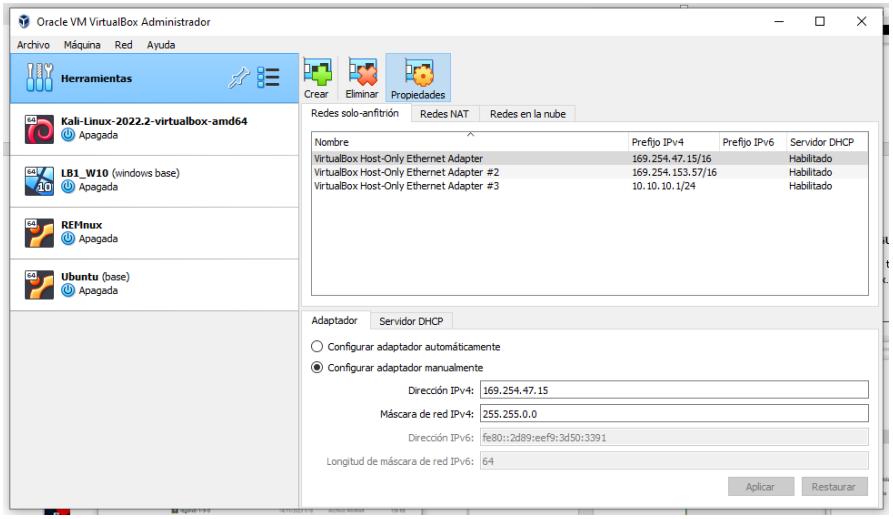


Figura 149: Configuración de la red

Se creará una nueva, en la cual estarán vinculadas los dos sistemas operativos. En este caso, será VirtualBox Host-Only Ethernet Adaptador #3, estando configurada de la siguiente forma.

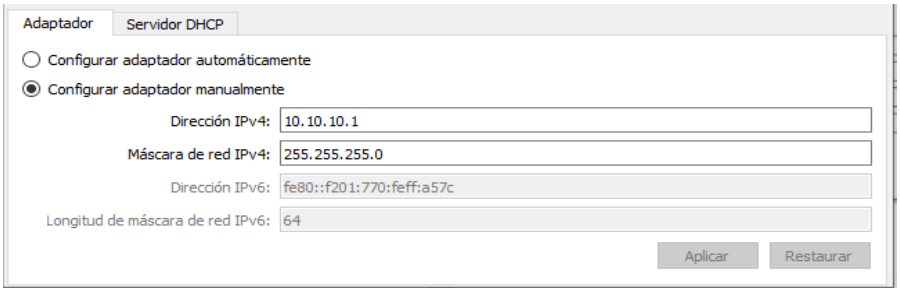


Figura 150: Crear nueva máquina

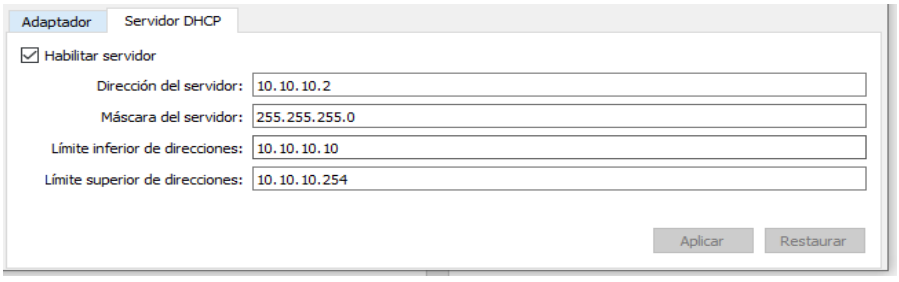


Figura 151: Adaptador

Una vez terminada la configuración, se anclan las redes de los sistemas operativos a este adaptador de internet.

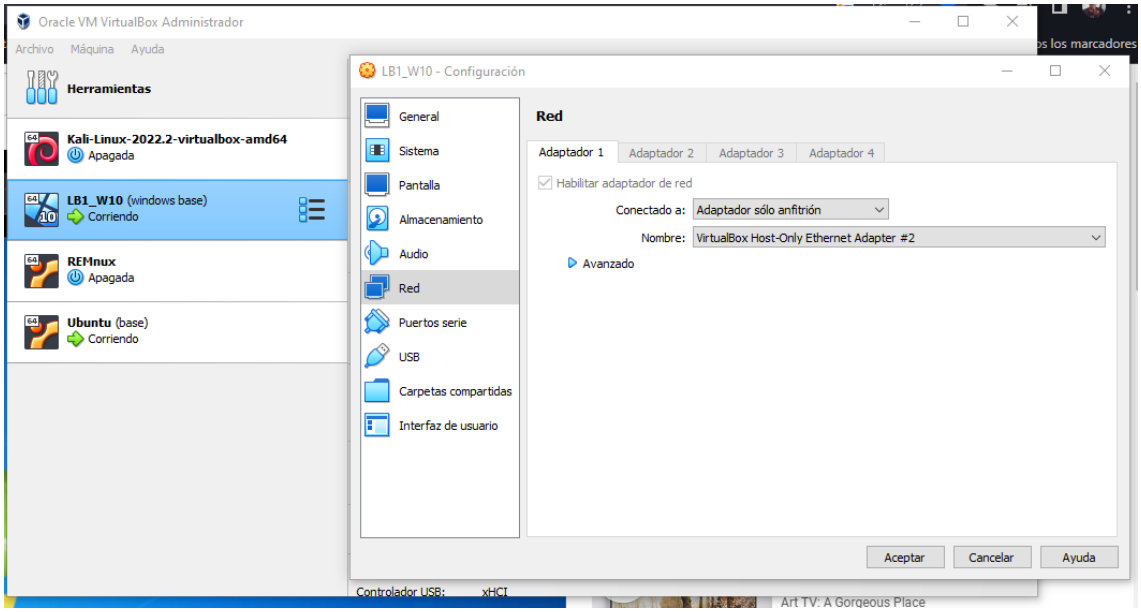


Figura 152: Anclar redes

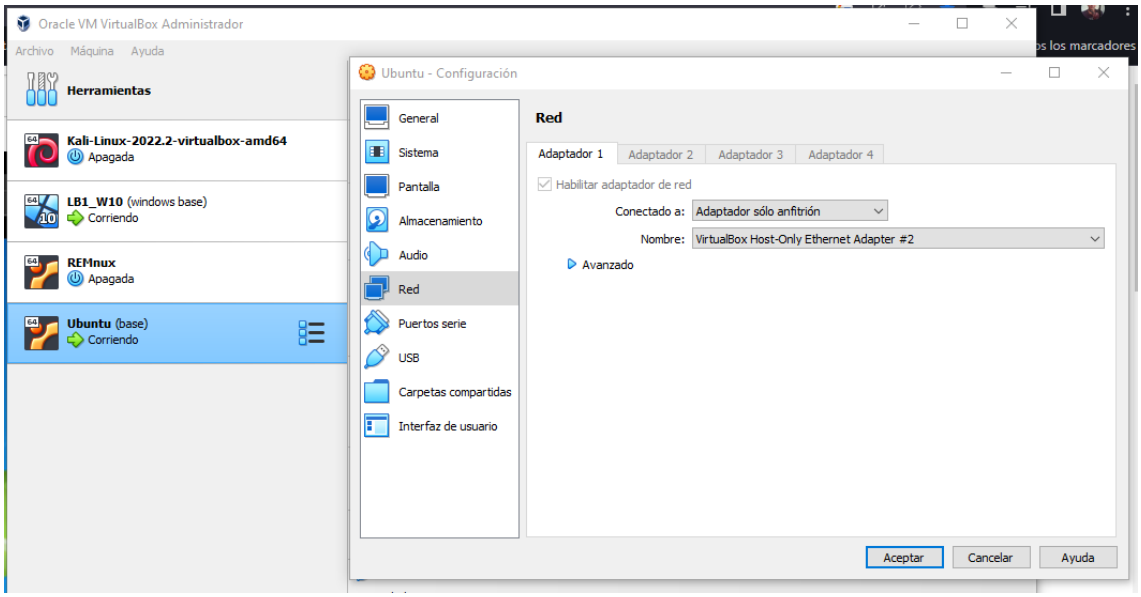


Figura 153: Anclar redes

Se procede a abrir el Windows virtualizado para realizar un cambio de red de dinámico a estático, el cual vinculará el servidor del Linux con el sistema operativo de Windows.

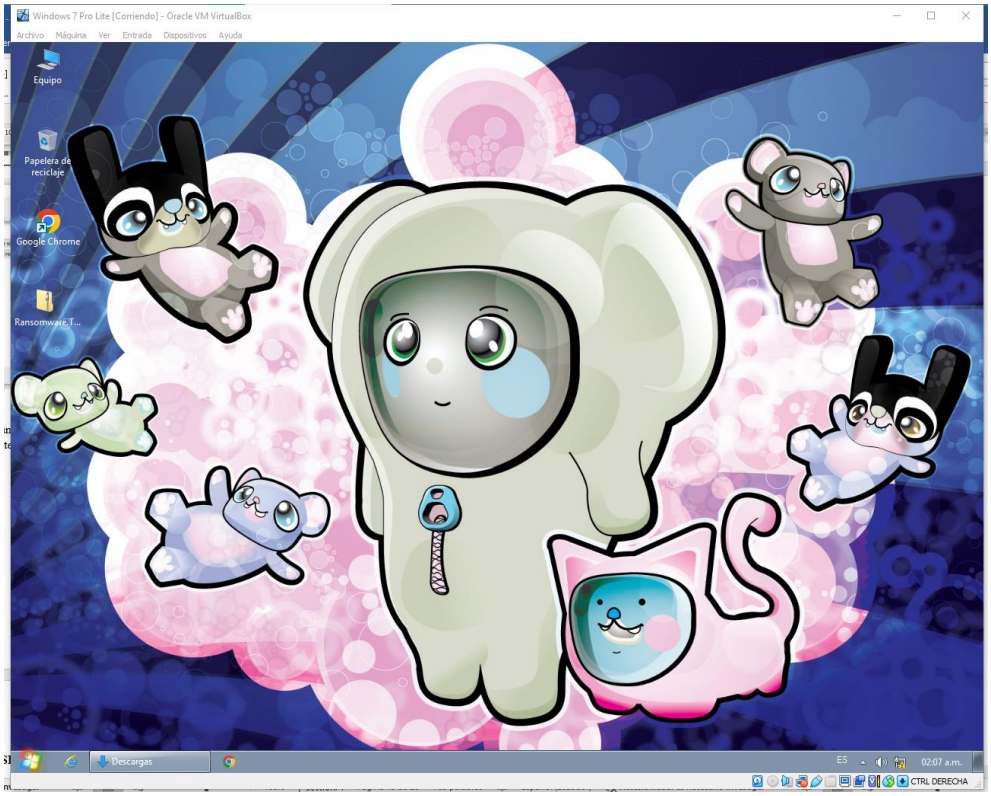


Figura 154: Abrir Windows

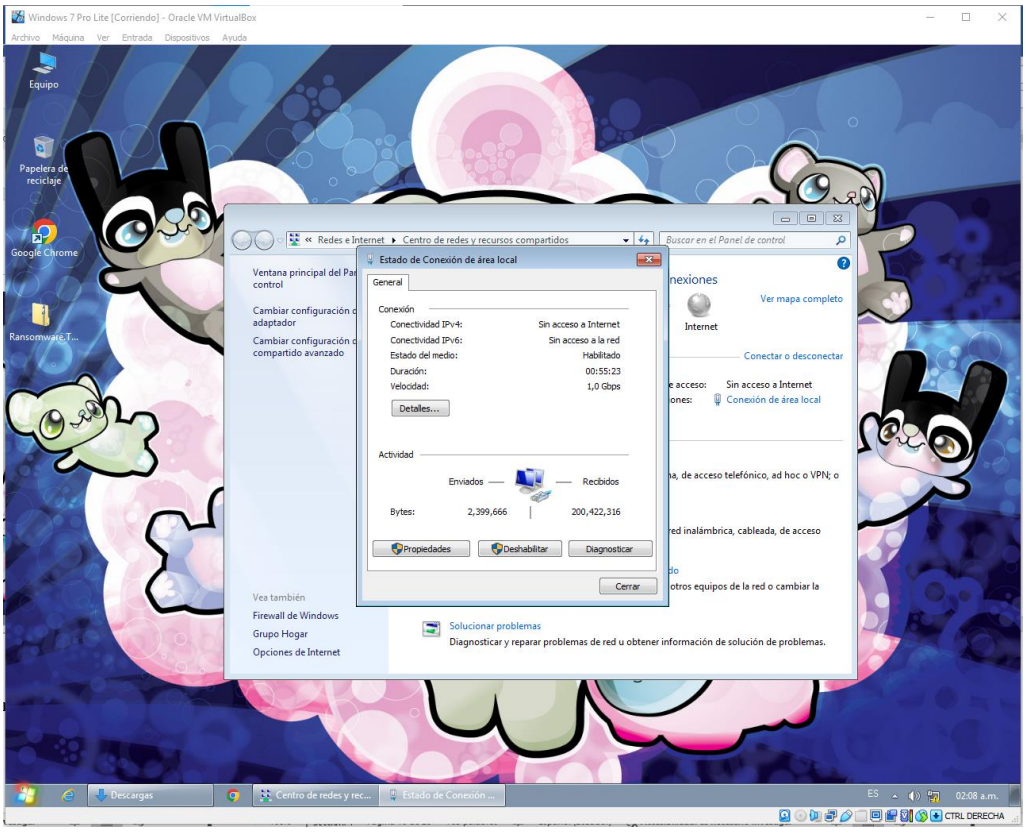


Figura 155: Cambio de red

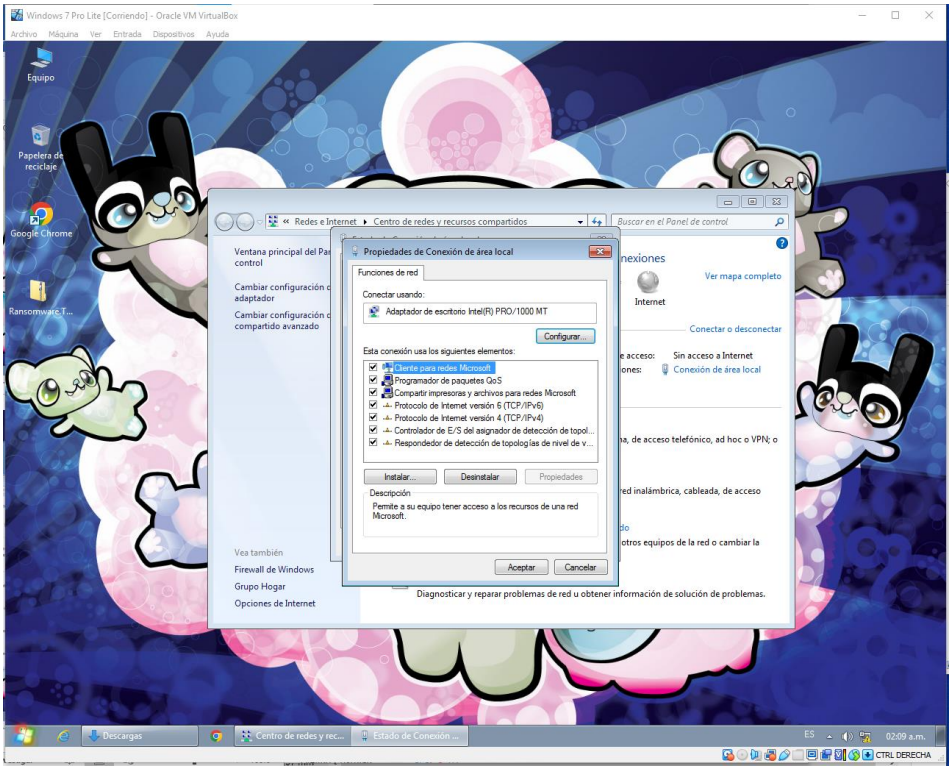


Figura 156: Vincular a servidor

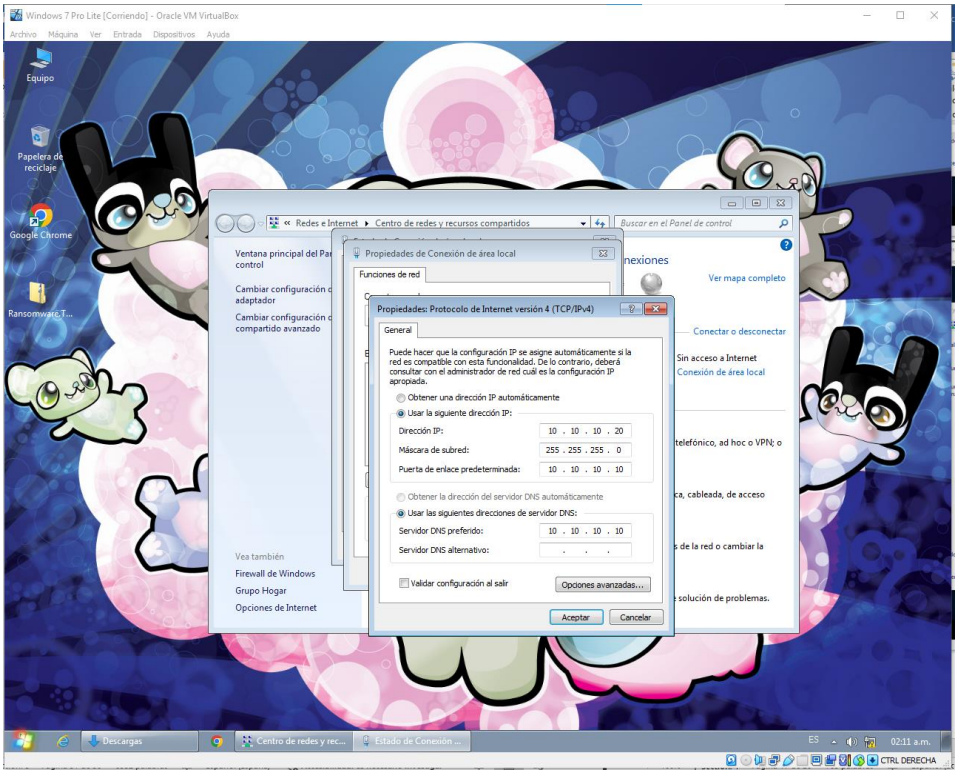


Figura 157: Vincular a servidor

Se realiza un ipconfig para asegurarse que la red cambió como se planificó.

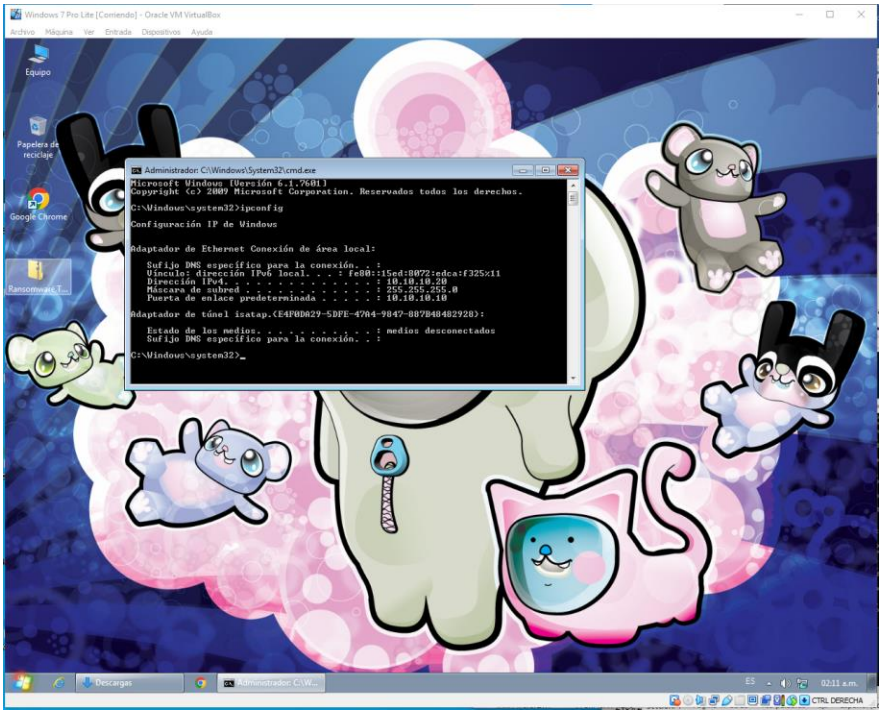


Figura 158: Ifconfig

Montar el servidor en Linux Ubuntu

Para montar el servidor, se deberán ejecutar ciertos pasos y condiciones. Para realizarlos se debe acceder como administrador usando el comando **sudo us.**

E ingresando a la dirección **cd /etc/netplan.**

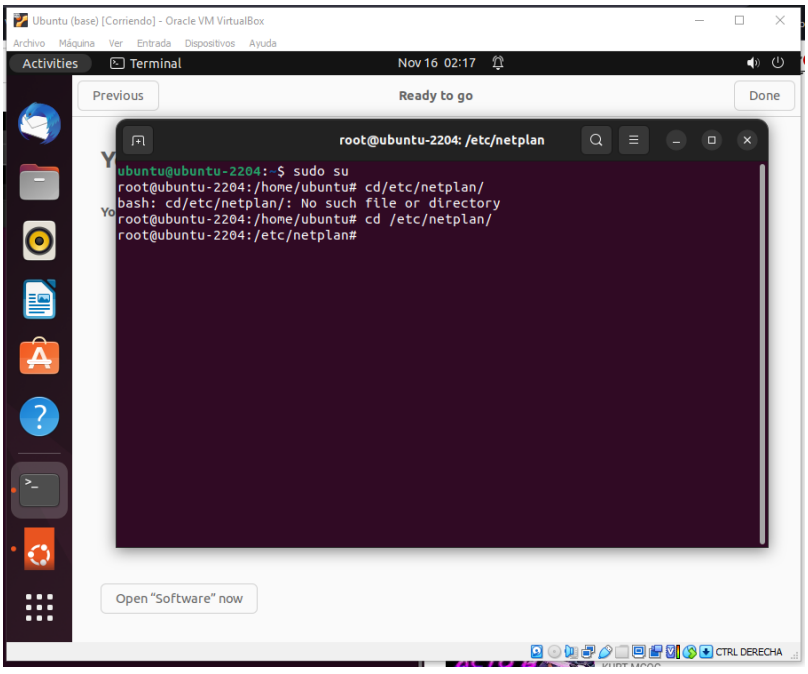


Figura 159: Montar servidor en Ubuntu

Luego de esto, escribimos el comando LS para que muestre el contenido de la carpeta.

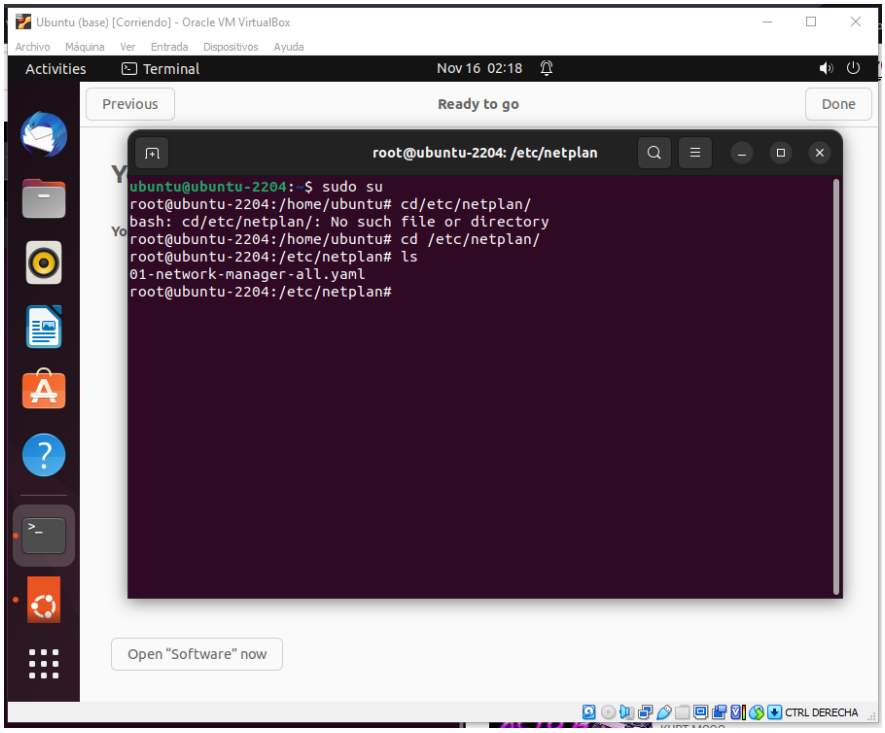


Figura 160: Comando LS

Hallando el contenido 01-network-manager-all-yaml se procede a editarlo con nano para cambiar la dirección establecida.

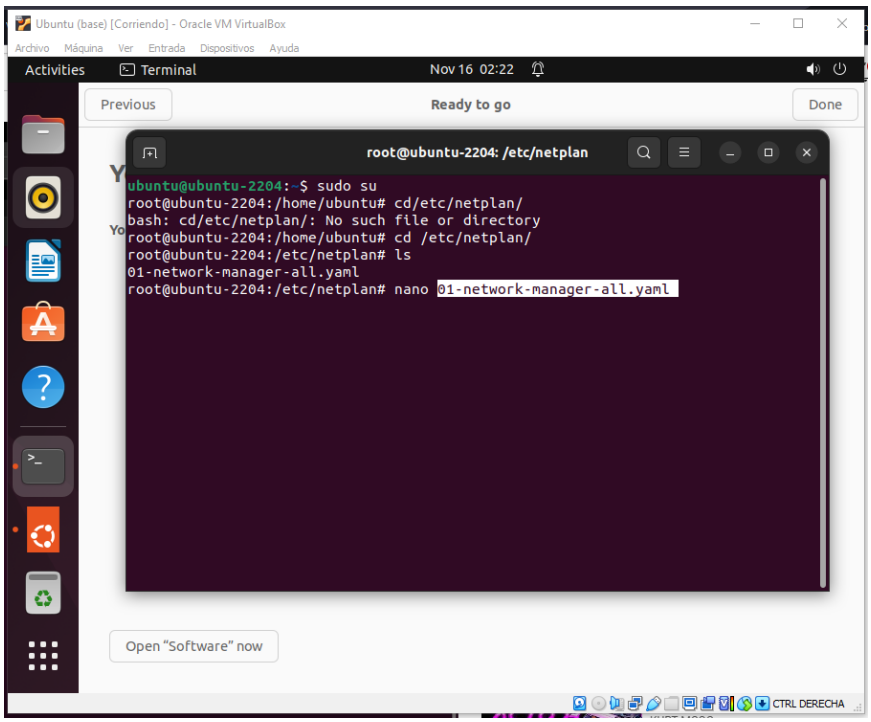


Figura 161: Hallar el contenido

Rellenando de la siguiente manera y utilizando la dirección ya antes prevista.

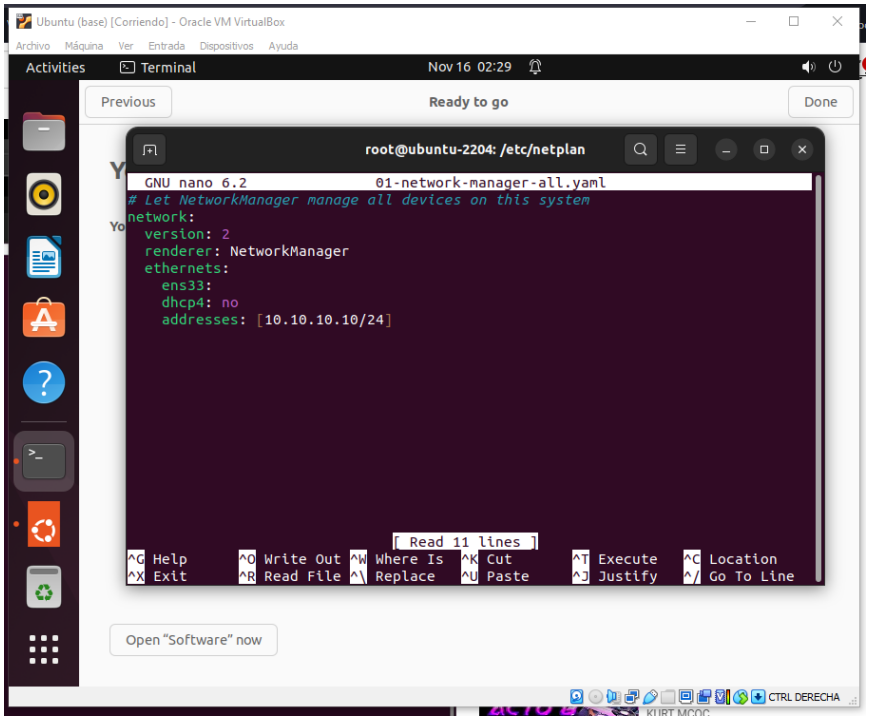


Figura 162: Relleno de información

Para guardar en el editor, se utilizará control + O y para cerrar control + X.

Una vez guardado, se ejecutará el comando netplan apply para aplicar la configuración prevista.

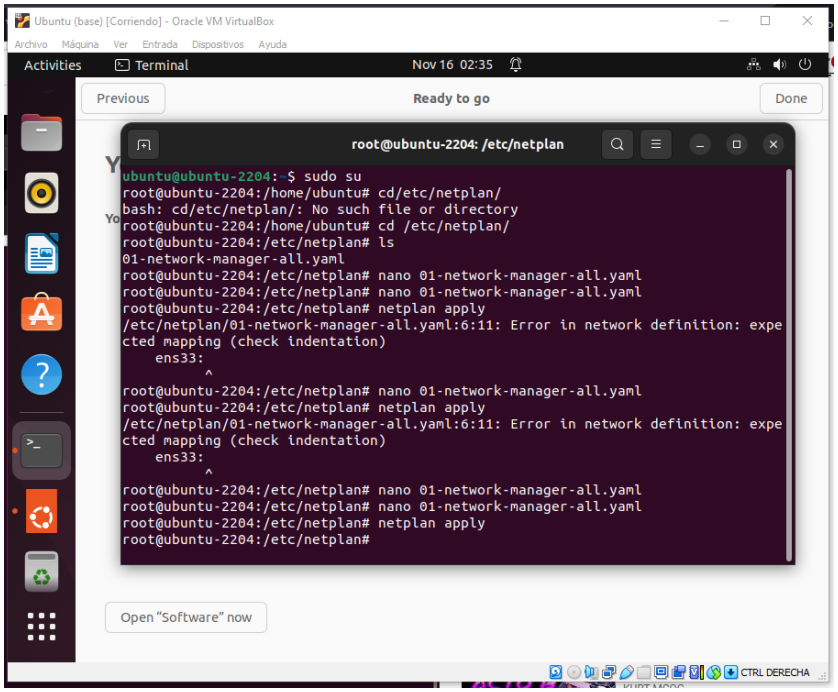


Figura 163: Guardar en el editor

Para verificar que todo haya salido perfecto, se ejecuta el comando ifconfig para ver las direcciones ip dadas.

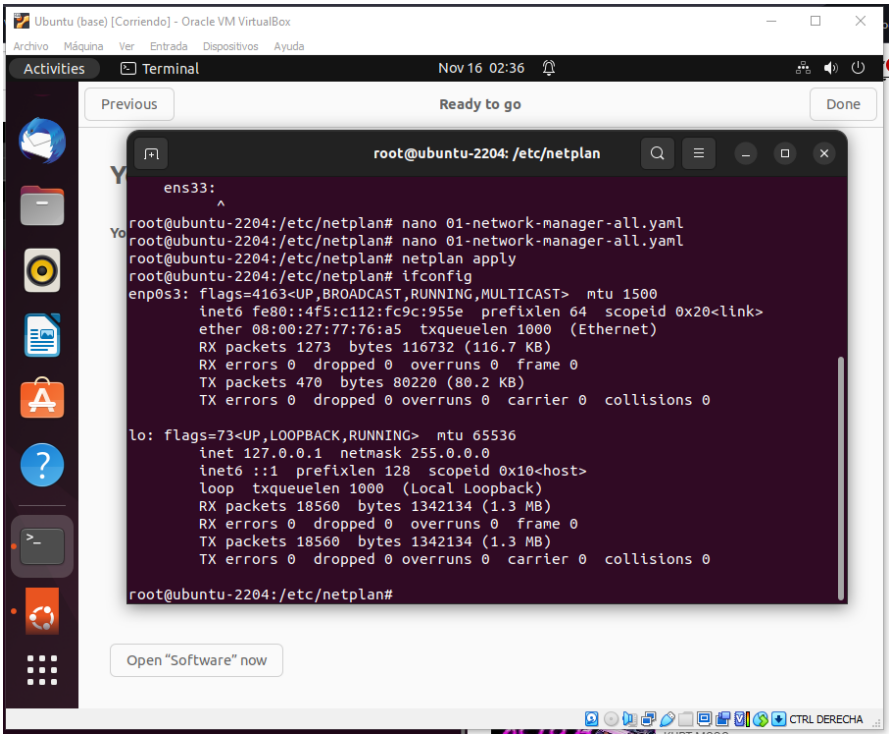


Figura 164: Verificación

Y a su vez un ping para ver si establece conexión con el Windows y viceversa.

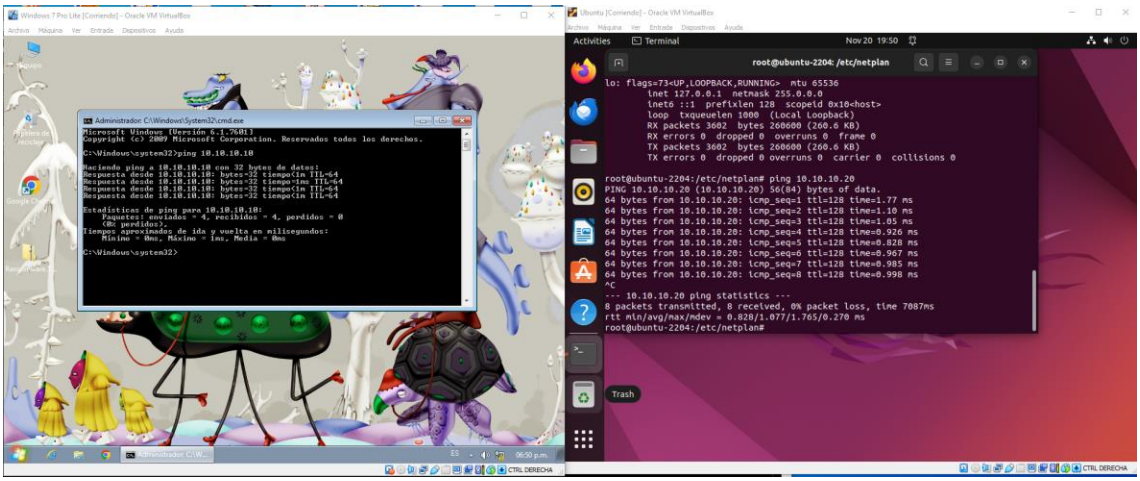


Figura 165: Ping para establecer conexión

Activando el ataque

Para comenzar esta práctica, en la máquina Linux se arranca el Fakenet-ng, pero genera un error, siendo normal, ya que, usa un puerto que es empleado por algún otro servicio.

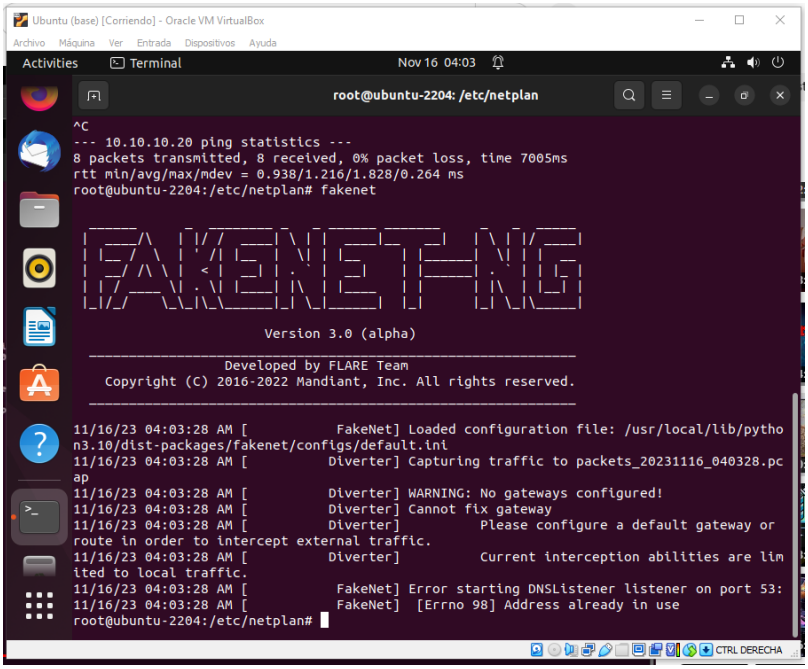


Figura 166: Activación del ataque

Para mandar abajo el uso de este puerto 53, se utilizará el comando lsof -¡:53.

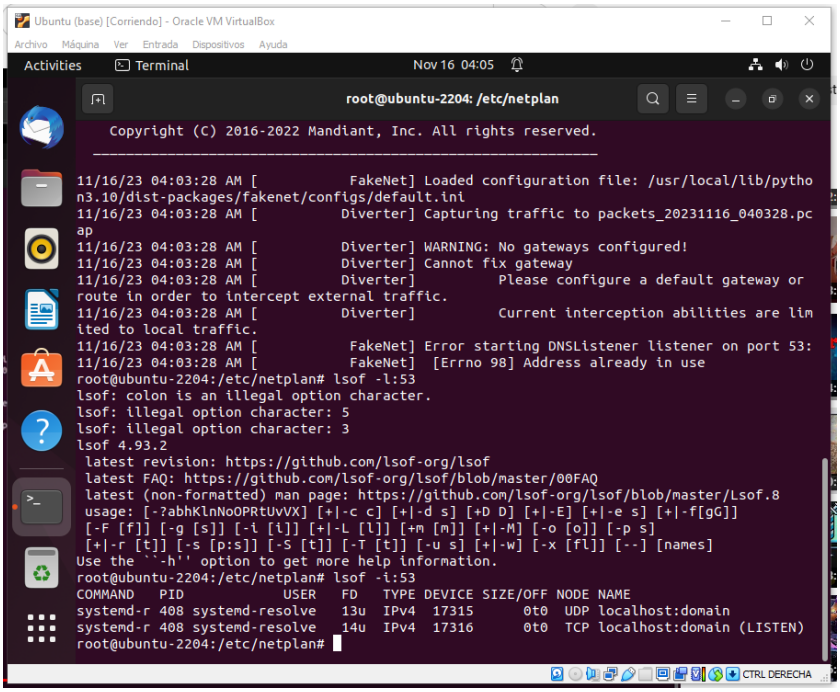


Figura 167: Comando lsof

Para bajarlo del sitio se usa el comando systemctl disable systemd-resolved.service

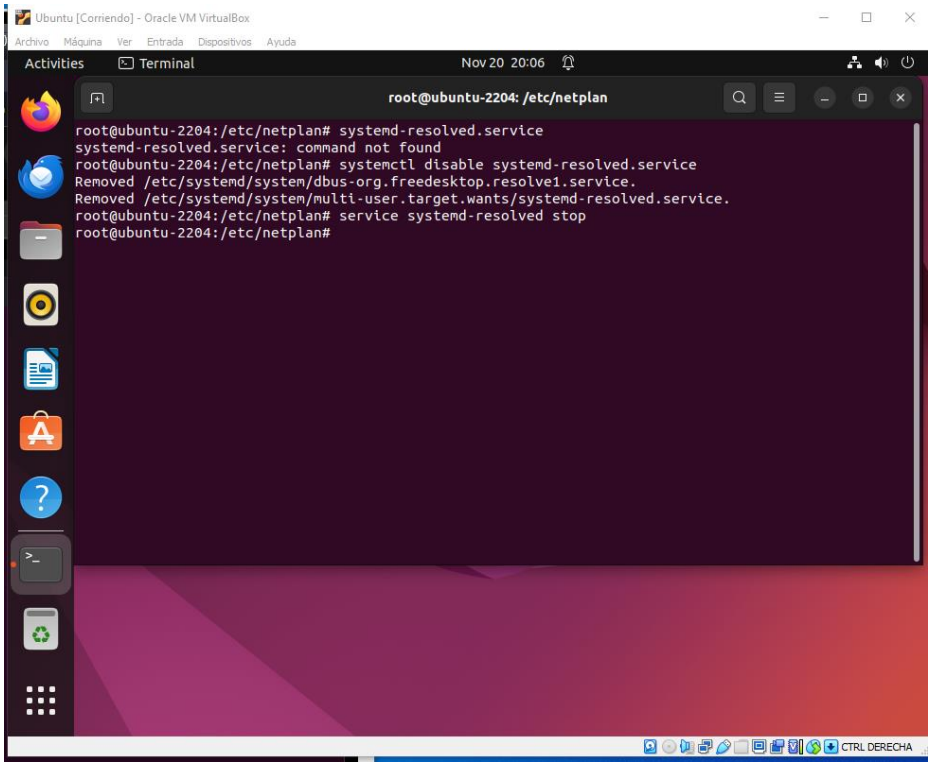


Figura 168: Bajar el sitio

Se vuelve a probar para ver si arranca correctamente el fakenet-ng

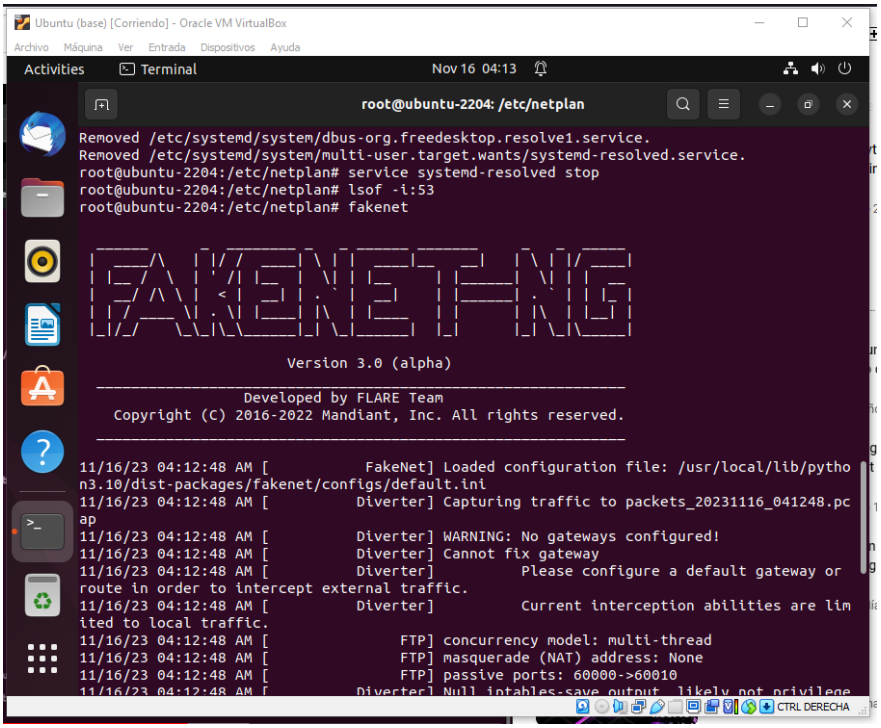


Figura 169: Arrancar correctamente

Resuelto el problema del puerto, se genera un segundo error de permiso de servicio, el cual se resolvió con el comando modprobe nfnetlink_queue

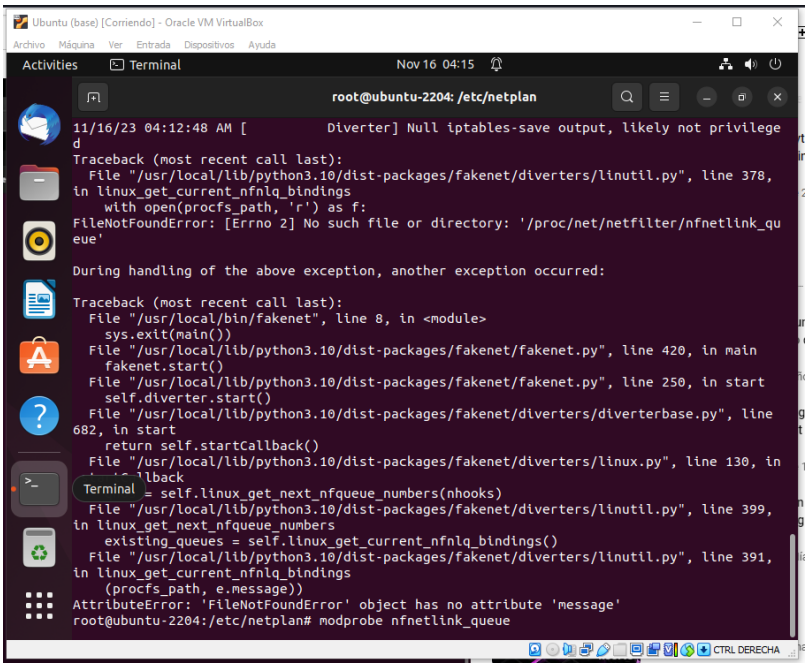


Figura 170: Problema del puerto

Arrancando de manera satisfactoria el Fakenet-ng

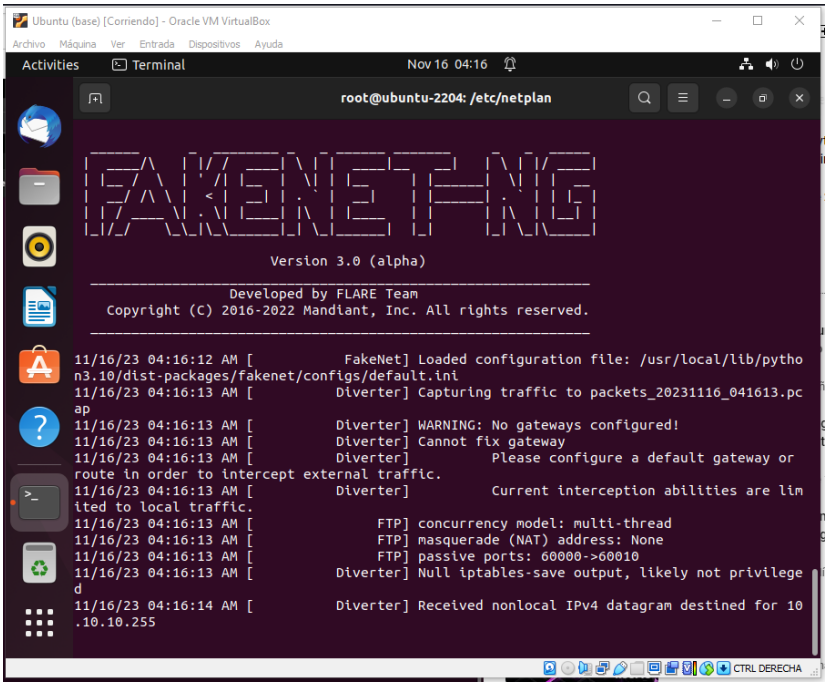


Figura 171: Arrancar de forma satisfactoria

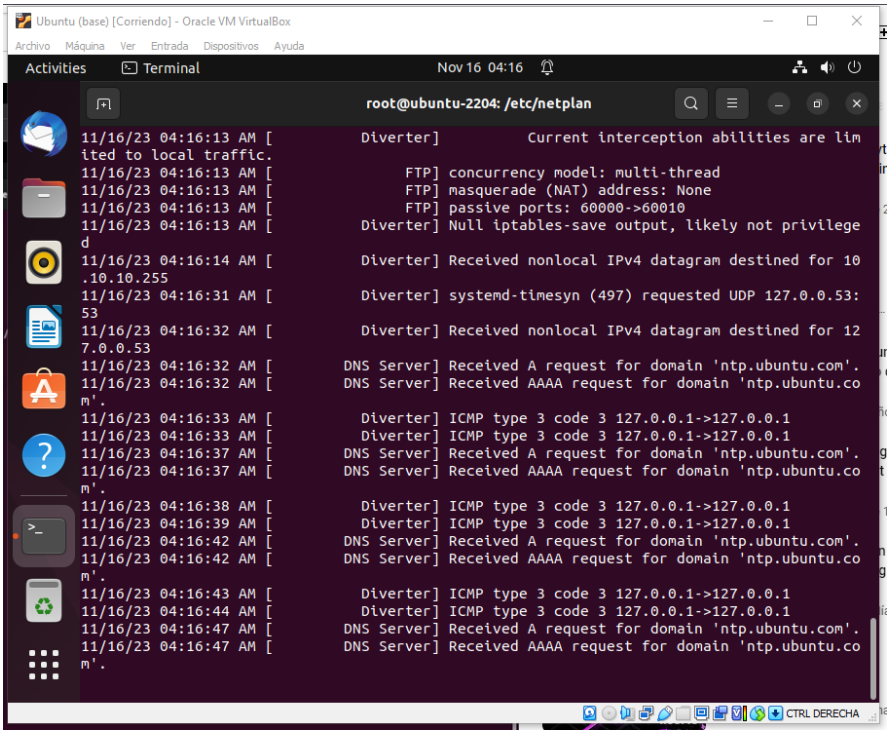


Figura 172: Arranque del sistema

Para verificar el funcionamiento, en el Windows se abre una pestaña con una página y muestra lo siguiente.

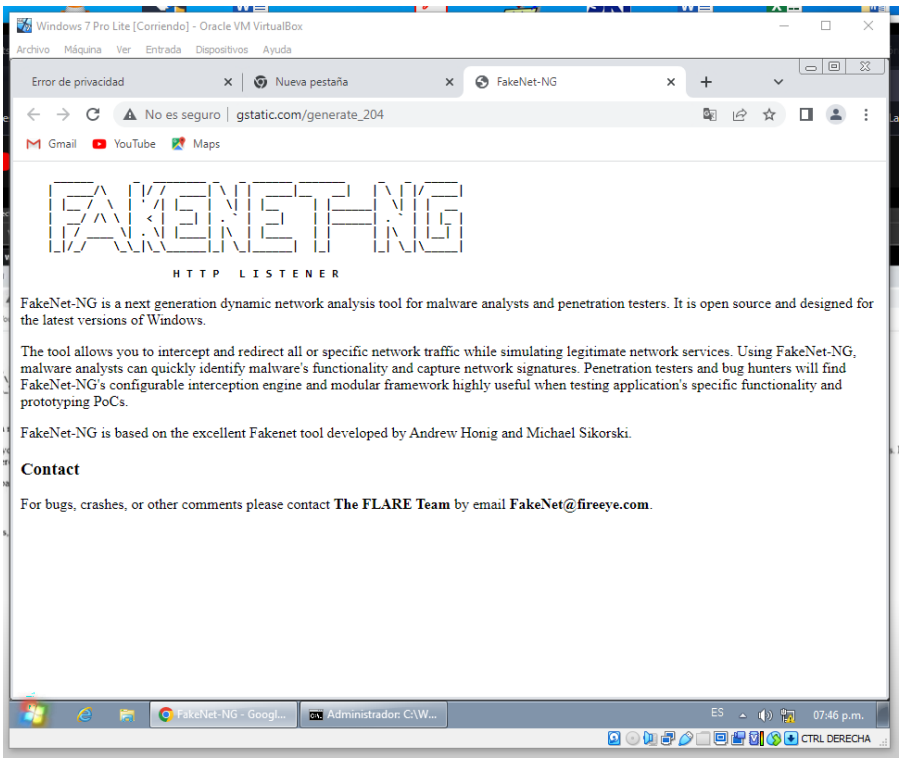


Figura 173: Verificar funcionamiento

Se procederá a arrancar el ransomware descomprimiendo el archivo.

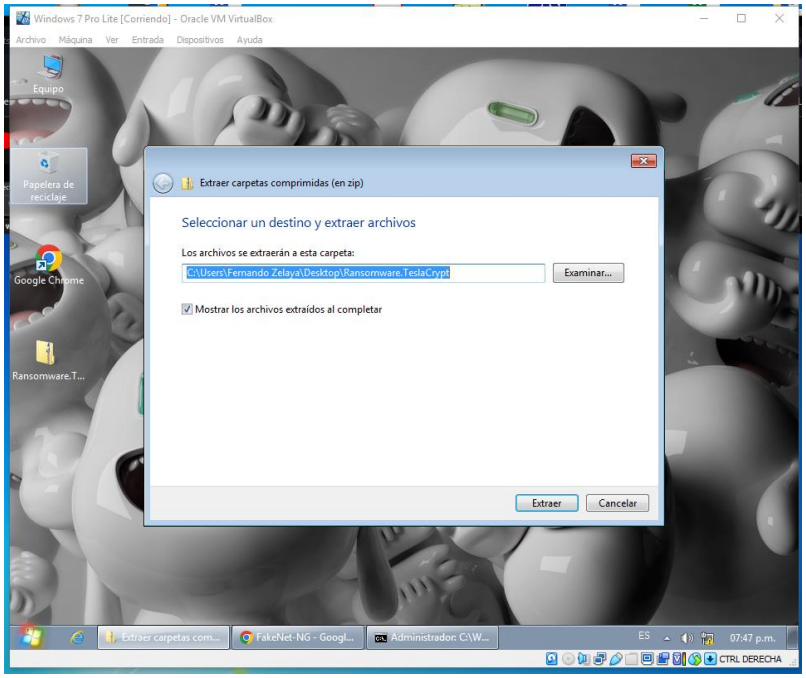


Figura 174: Arranque de ransomware

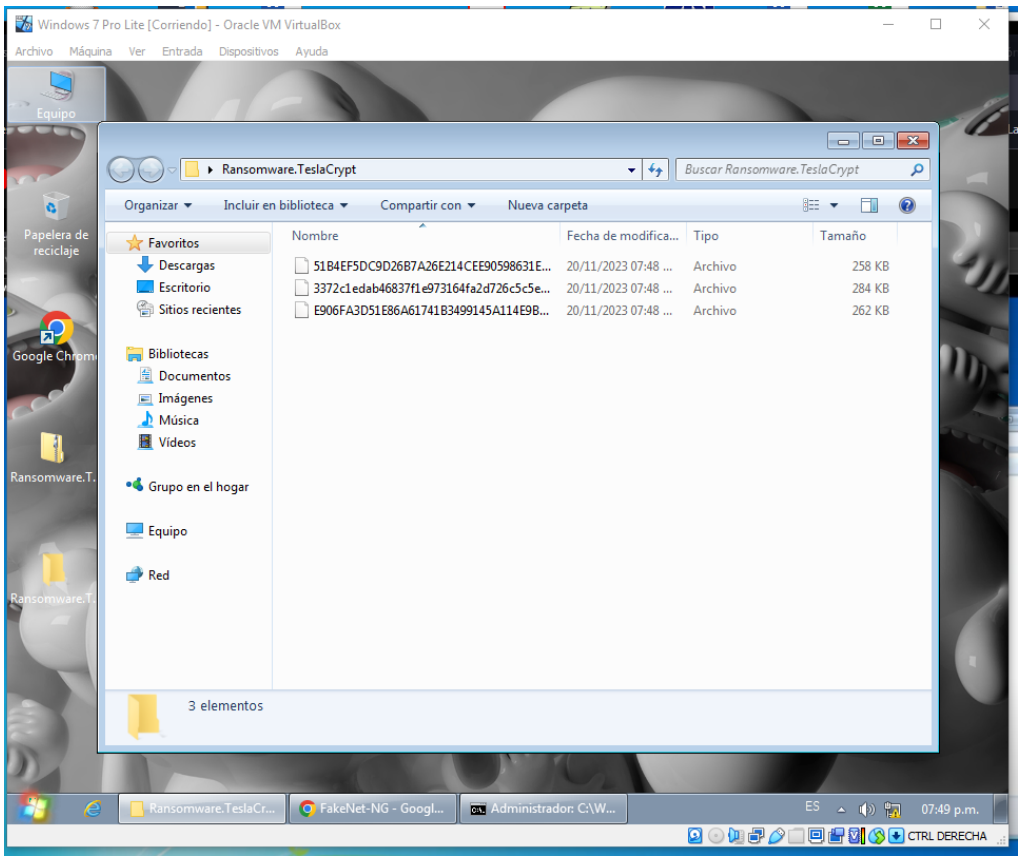


Figura 175: Descomprimir archivo

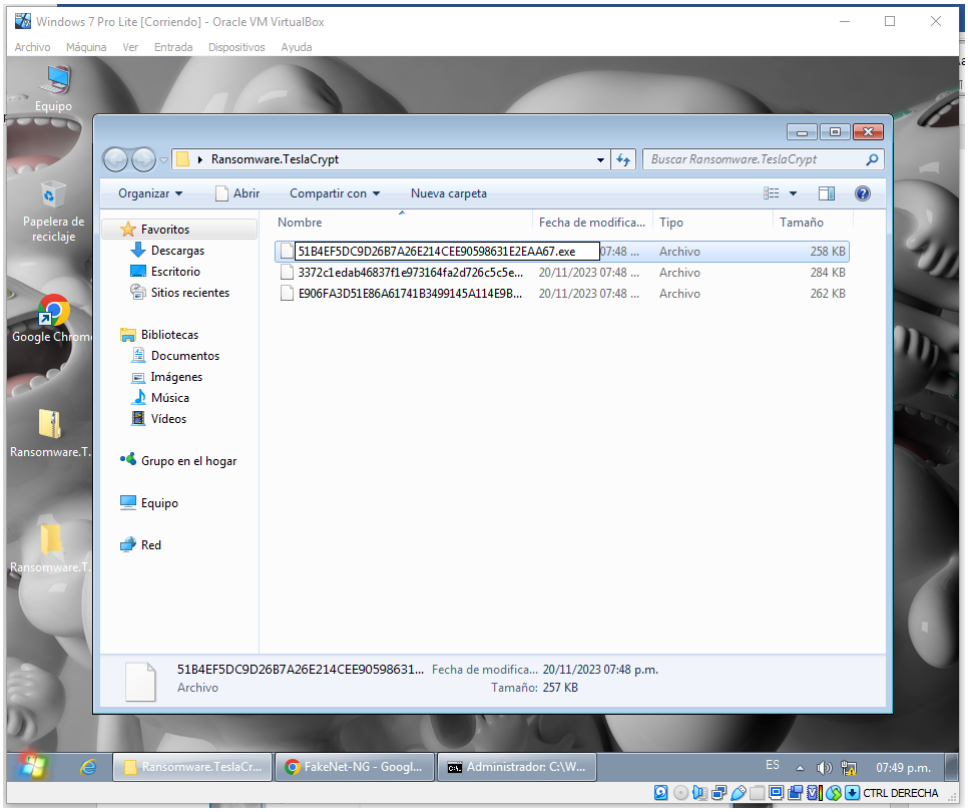


Figura 176: Descomprimir archivo

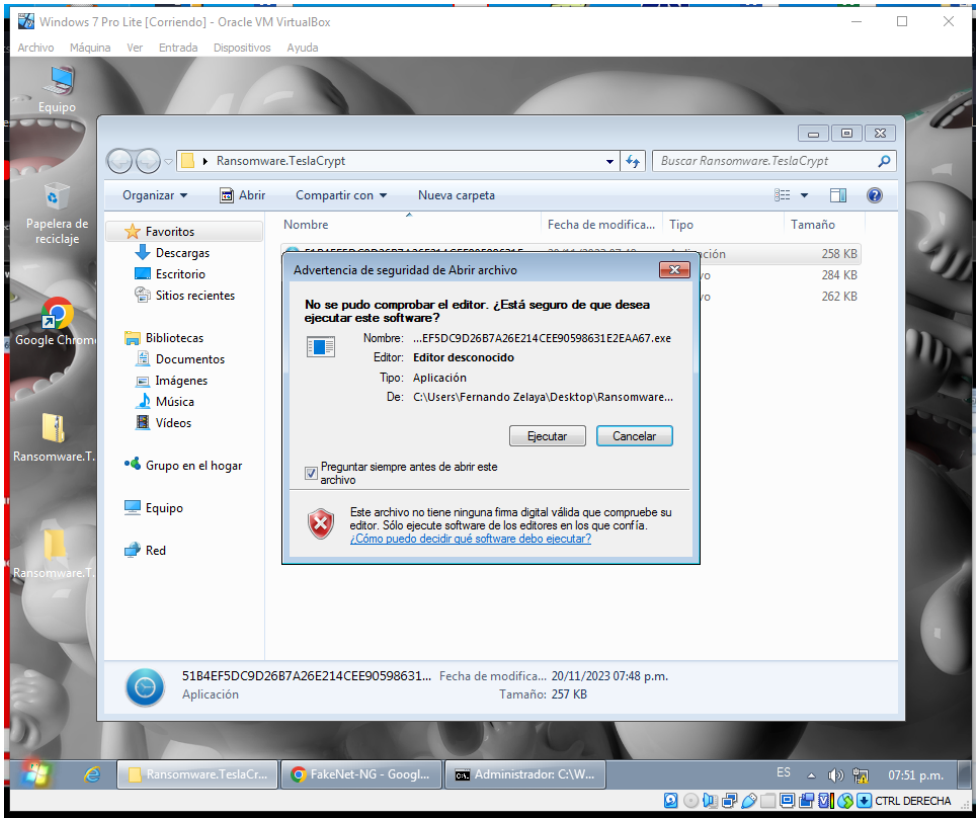


Figura 177: Descomprimir archivo

Figura 178: Verificación

En el monitoreo del Linux, se aprecia los arranques de funcionalidad, mostrando lo que el ransomware provocará.

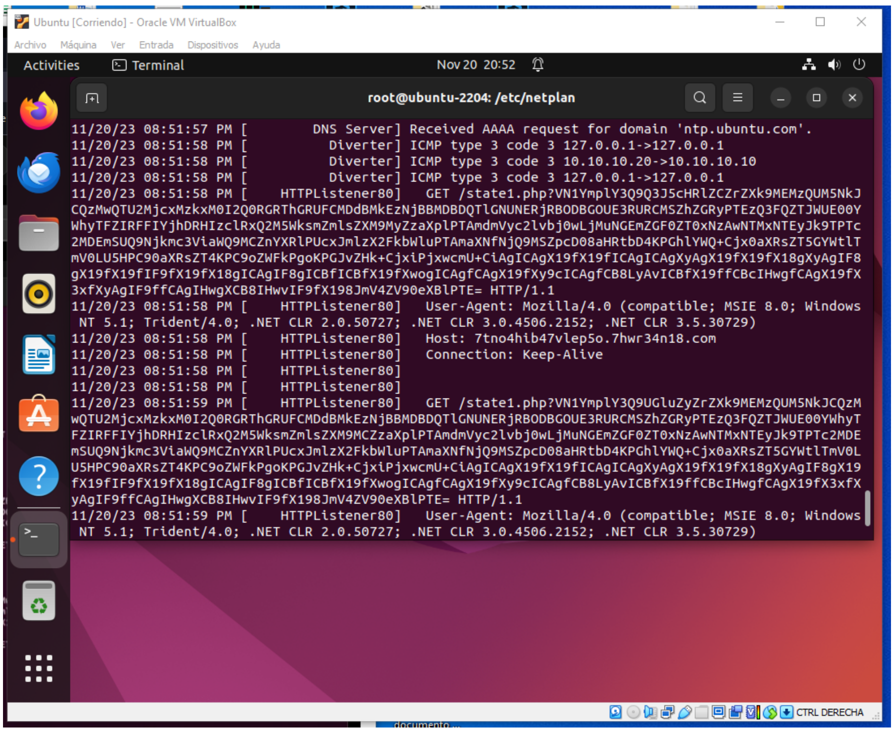


Figura 179: Monitoreo de Linux

Se llegan a denotar diversos dominios que no están existentes.

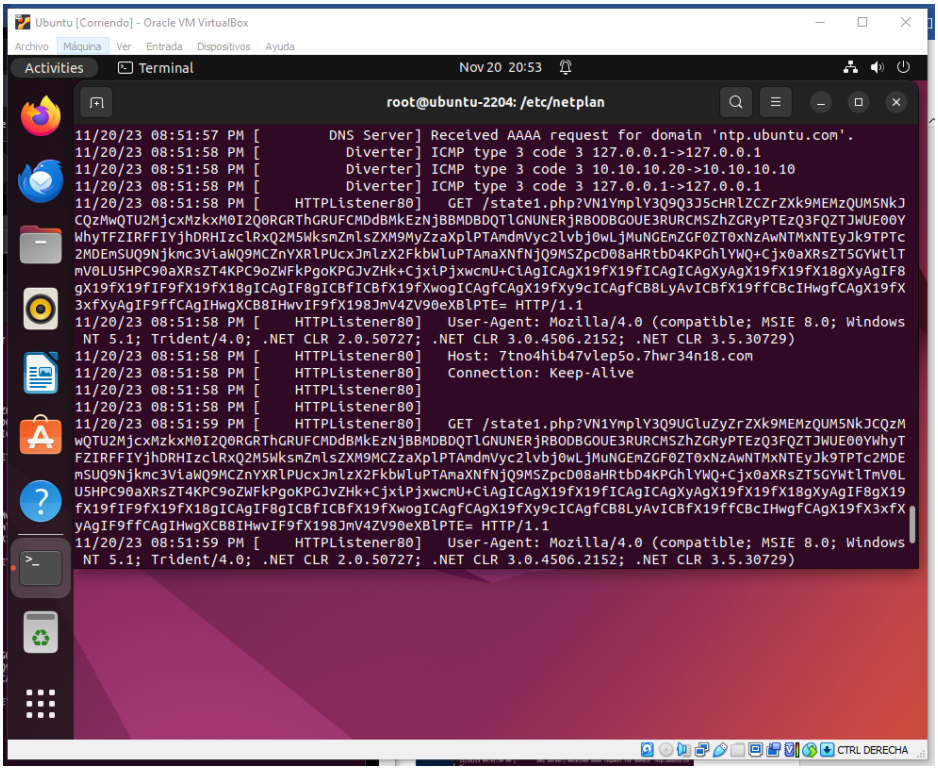


Figura 180: Dominios inexistentes

Se muestran decodificaciones en base 64.

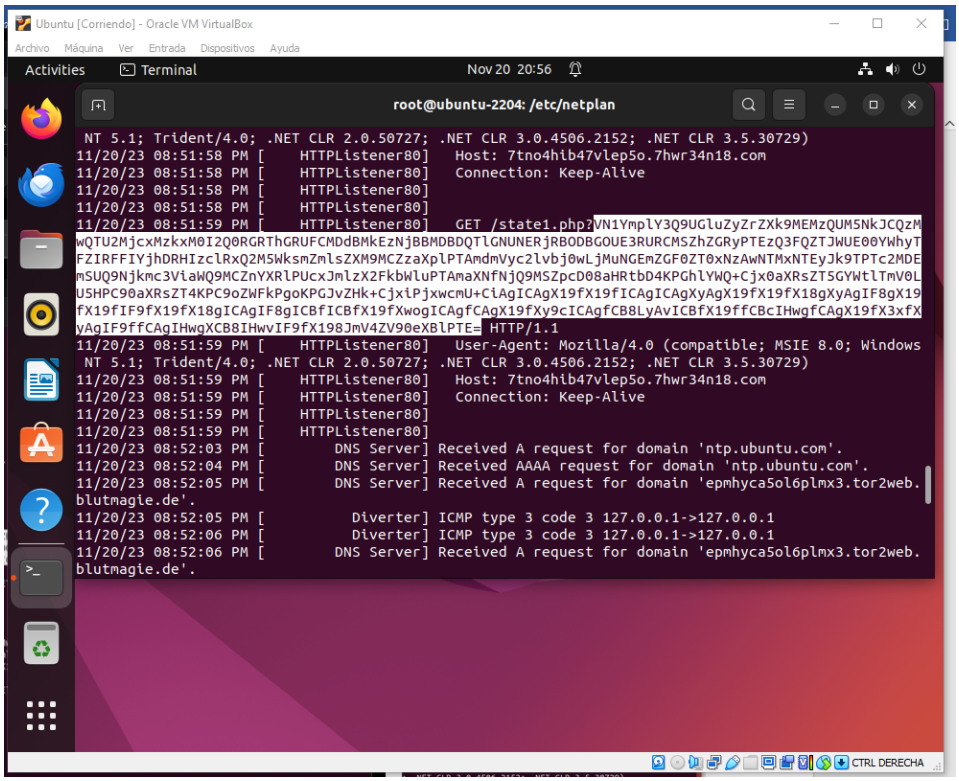


Figura 181: Decodificaciones en base 64

Verificaremos mediante la página base64 decoder para ver que se encuentra dentro de esta decodificación.

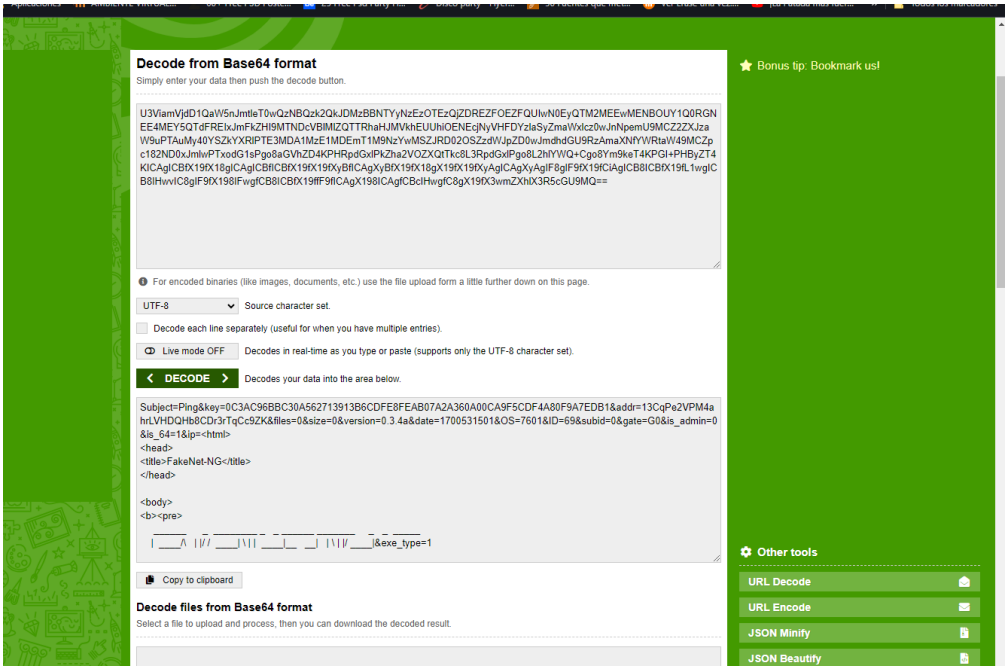


Figura 182: Página de base 64

Sospecha de páginas de Bitcoin para el pago, ya que, nos muestran un link interno.

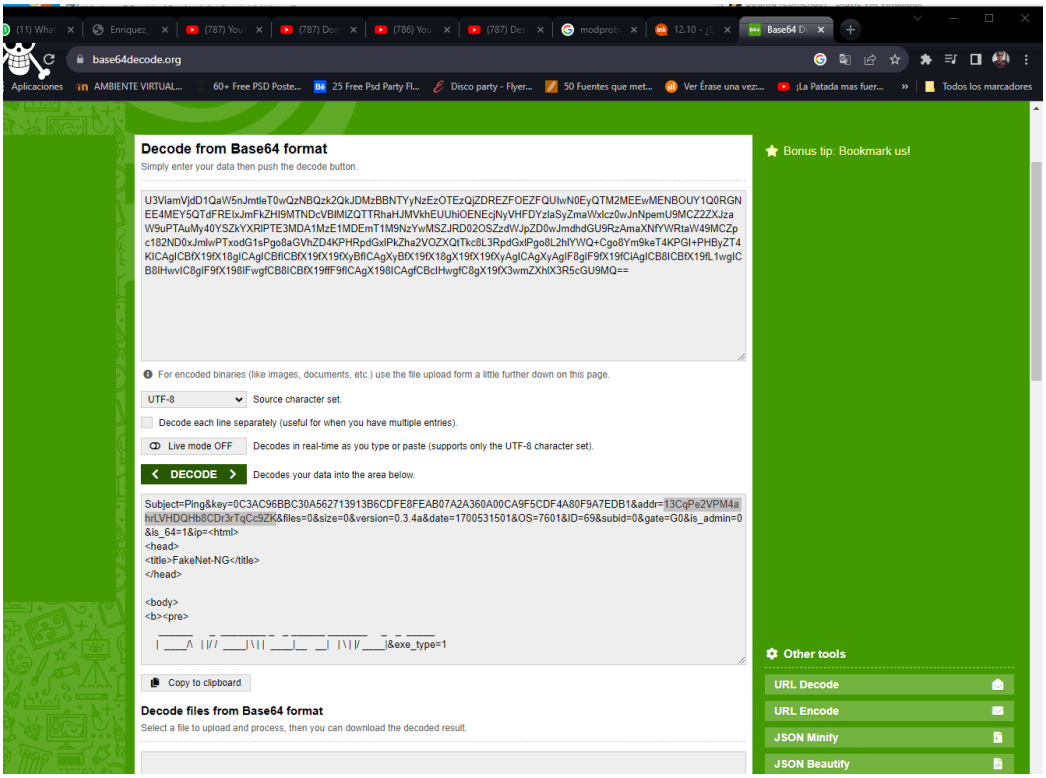


Figura 183: Sospecha de páginas

Analizamos con el navegador la dirección de bitcoin para validar su existencia.

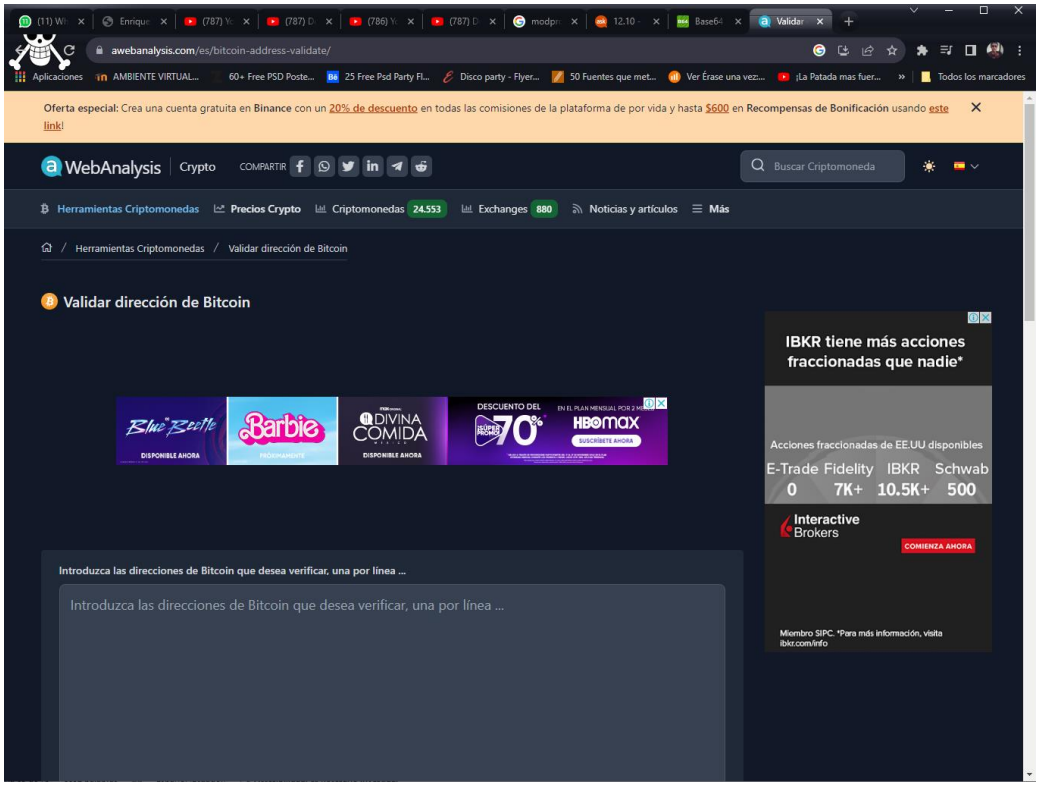


Figura 184: Análisis del navegador

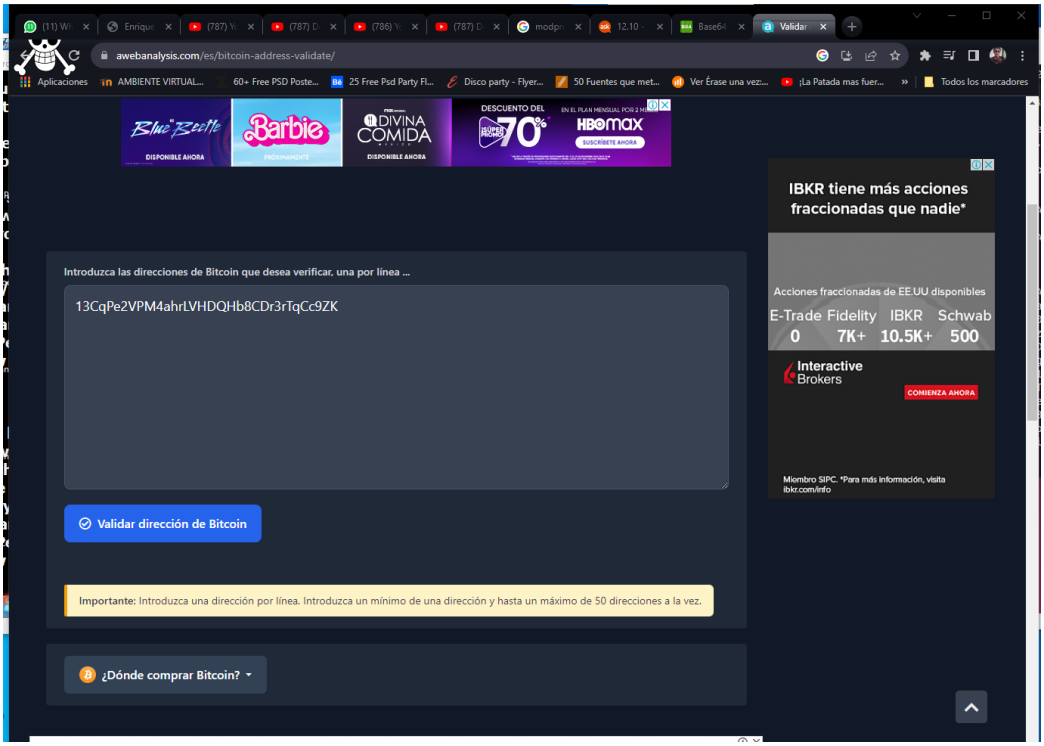


Figura 185: Análisis del navegador

Mostrando como resultado que si existe y mirando sus estadisticas, se verifica que se genera un usuario de bitcoin por máquina atacada.

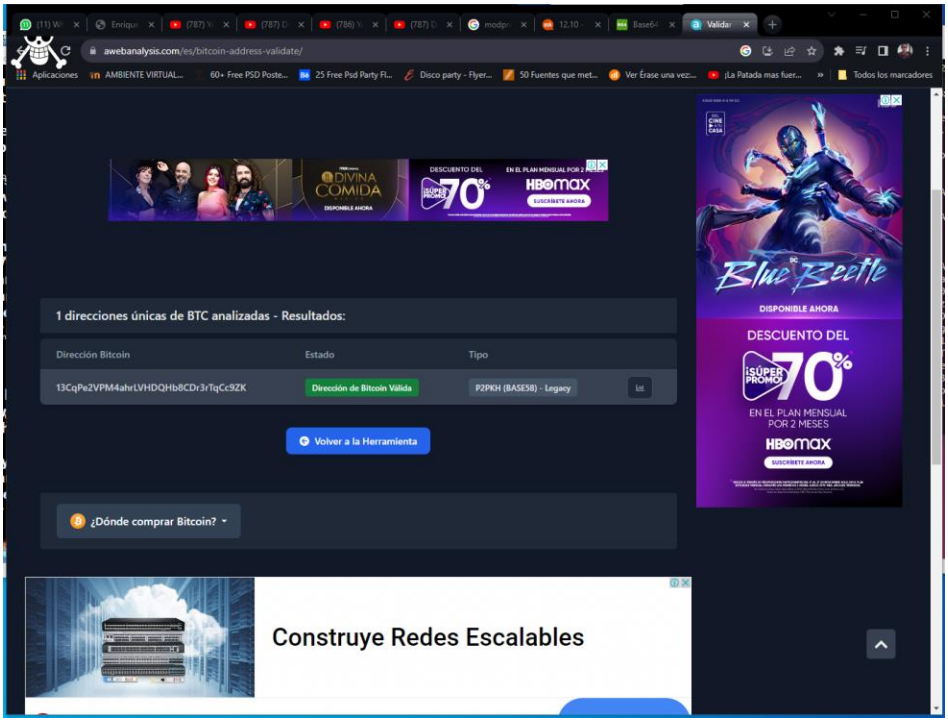


Figura 186: Estadísticas

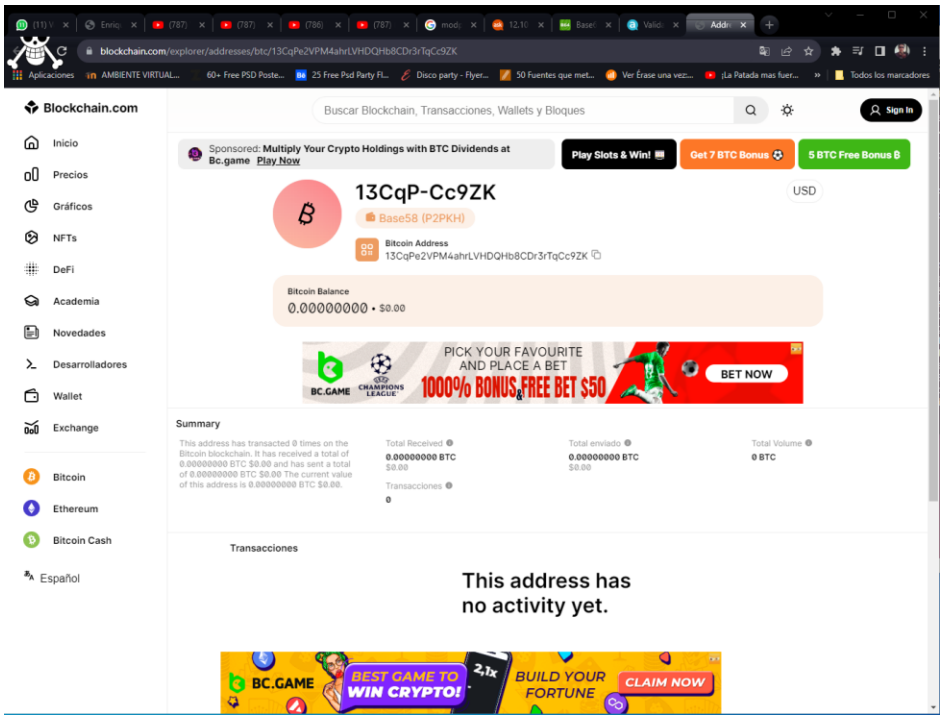


Figura 187: Verificación final

Anexo 10. Caso 3 – Defacement

Para realizar un ataque de defacement, el cual consiste en cambiar el entorno de una página web como un ataque de cambio de copia de una web. En este caso se hará con un servidor local para ilustrar los pasos a realizar.

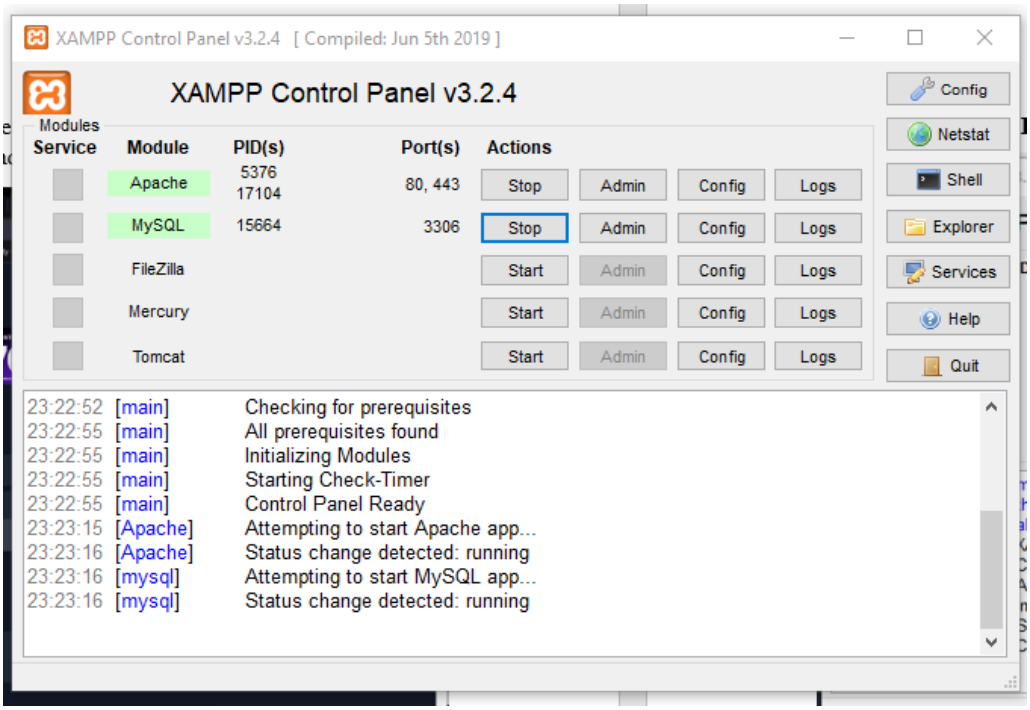


Figura 188: Ataque de defacement

En este caso, se utilizará una página web que se creó para el turismo de Ballenita, el cual se procederá con los cambios debidos para la demostración del arranque de este tipo de ataque.

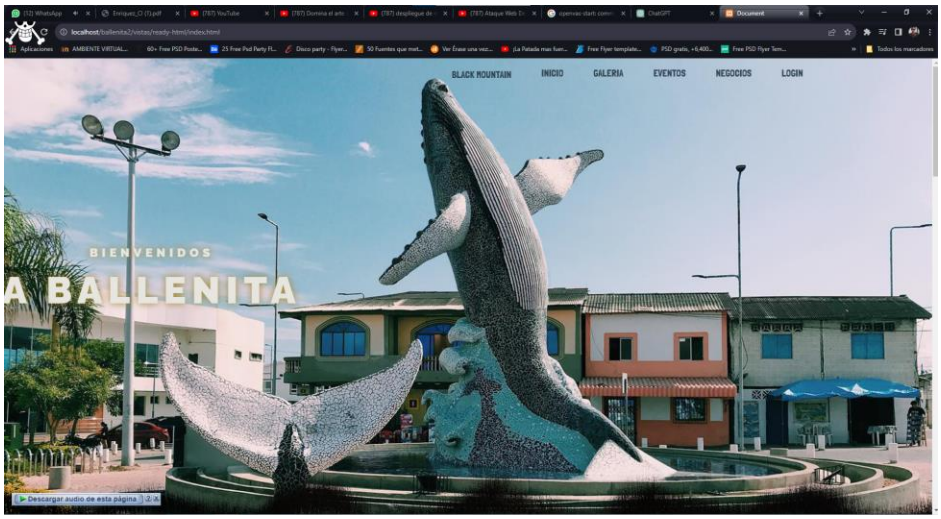


Figura 189: Página web

En caso que se requiera un servidor para este tipo de ataques el entorno del Cpanel se ilustraría de la siguiente manera, ya que, este actuaría como un servidor de la página web a atacar para el ensayo de defacement.

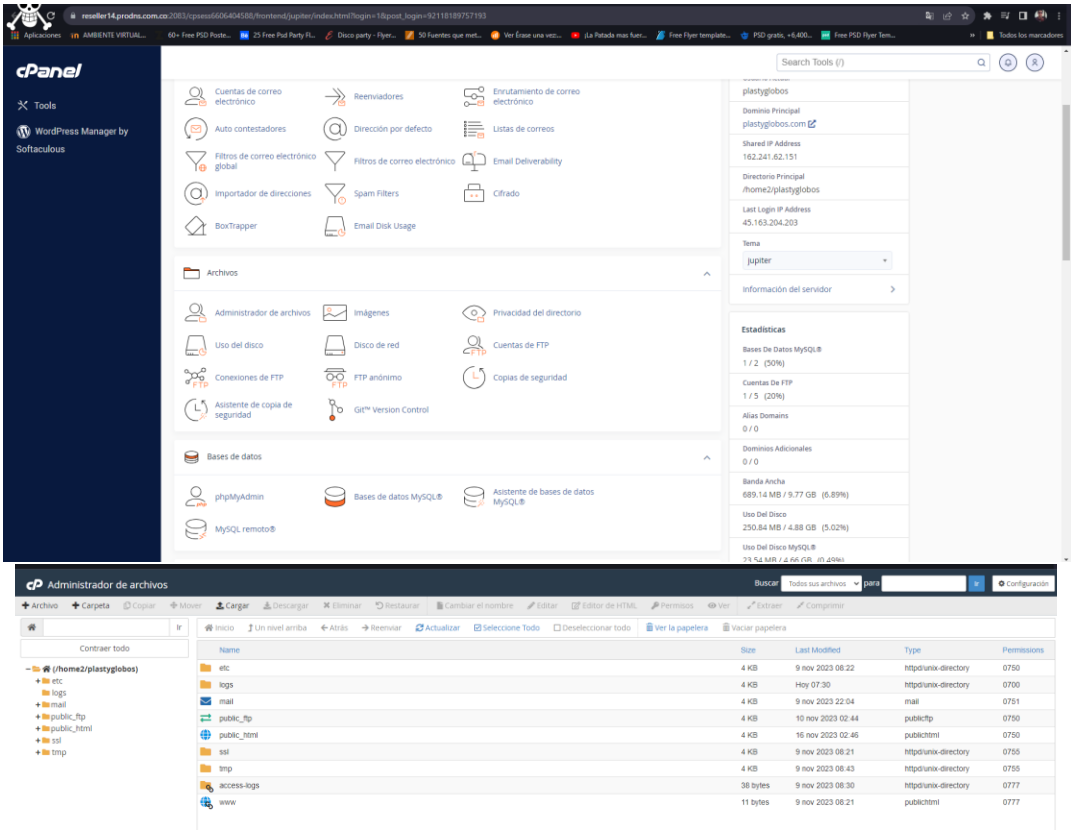


Figura 190: Cpanel

El entorno para el cambio de la programacion de la página web a editar, se muestra de diferentes formas para cada entorno tanto para el servidor de la red y un servidor local en la programación.

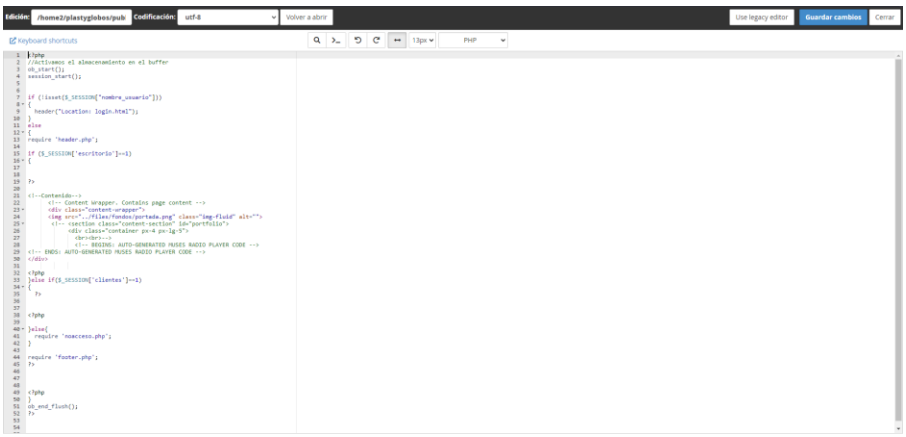


Figura 191: Firmas para cada entorno

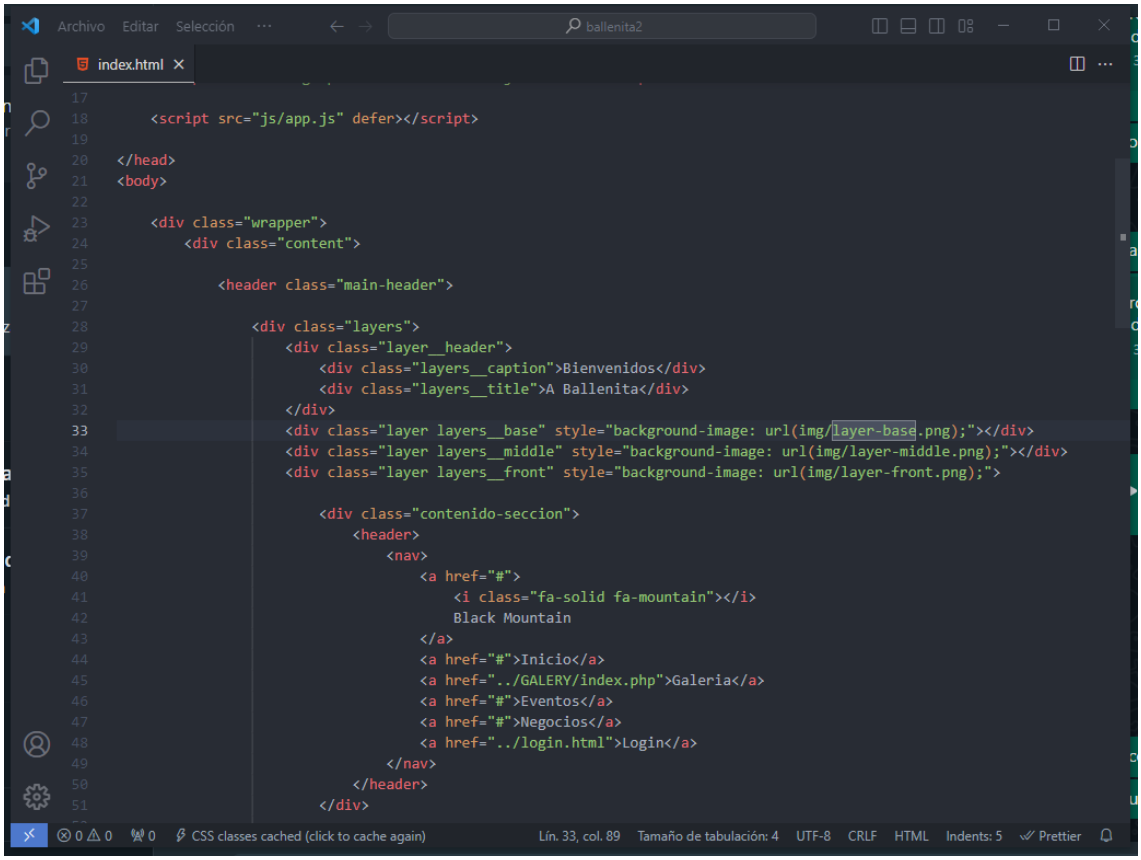


Figura 192: Código fuente

Una vez que se realizan los cambios, se arranca el sistema para contemplar la página que se ha modificado para el ataque defacement.

Figura 193: Página web

Anexo 11 Informes de los casos

El informe contiene información obtenida mediante herramientas de informática forense que se han utilizado en distintas etapas para cada caso cubierto por el proyecto: servidores, malware ransomware y fraude. Tomar las precauciones y procedimientos adecuados para preservar la información obtenida y el equipo físico en el que se realizará el análisis. El proceso de investigación se rige por la norma UNE 71506:2013 y consta de 4 fases: adquisición, conservación, análisis y documentación.

Se utilizan herramientas de análisis forense para analizar el contenido como se describe en el punto anterior, utilizando el conocimiento de la generación de hash para verificar la autenticidad de la información, el análisis, paquetes y los posibles atacantes asociados a cada rastro.

Analizando los documentos obtenidos y guardados se llegó a las siguientes conclusiones, destacando que lo más importante en el análisis de los ataques del delincuente, en este caso: volcados y dirección IP.

Caso 1. Volcado de Memoria

Al analizar este tipo de ataque, cabe destacar que existen diversas formas de ataque de volcado de memoria, en este caso el envío de paquetes infinitos a un aplicativo web desde un sistema Kali Linux hacia una máquina en Ubuntu, entonces se usaron diversos tipos de análisis, ya que, el contenido de estos paquetes sumamente de gran tamaño es receptados y leídos por IP falsas. Por otro lado, diferentes direcciones IP son verificadas para localizar su ubicación, pero de igual manera en la paginas dedicadas a este proceso nos dan como resultado IP inexistentes.

HACKING ETICO

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA NUBE

DATOS DEL EXPERIMENTO			
Título del experimento:	Denegación de servicios	Realizado por:	Carlos Pita
No. Prueba:	Caso-01	Fecha inicio:	16/11/2023
Tipo prueba:	Laboratorio Forense	Fecha fin:	16/11/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Volcado de memoria	Fase:	Adquisición de evidencia
Nivel complejidad prueba:	Dificil	Tiempo ejecución:	10 horas
HERRAMIENTAS APLICADAS			
Hardware:		Virtualización:	Ubuntu Kali Linux
Software:	SE hacking Access Data Virtual box	Redes:	wifi domestica
DISEÑO DEL EXPERIMENTO			
Procedimientos: 1. Instalacion de Maquinas virtuales 2. Instalacion de herramientas 3. Ataque de Volcado con paquetes 4.Resultados obtenidos		Descripción del procedimiento: Anexo 1. Instalaciones Anexo 2. Ataque Anexo 3. Resultados	
Resultados esperados: 1. Envio de paquetes correctamente 2. Deteccion de paquetes 3. Deteccion de ip falsas 4. caida de la pagina por volcado de memoria		Resultados obtenidos: 1. Envio de paquetes correctamente 2. Deteccion de paquetes 3. Deteccion de ip falsas 4. caida de la pagina por volcado de memoria	
Conclusiones: Se establecio que el volcado de memoria en un ambiente web dio resultados satisfactorios mostrando que el ataque rindio los propositos propuesto en la documentacion documentada. El contenido de un volcado de memoria es un plan definido y diseñado a seguir para encontrar patrones, inconsistencias, tendencias y relaciones entre los rastros dejados por el sistema operativo en el volcado de memoria, tales como: procesos, memoria, recursos de almacenamiento. , así como dispositivos de entrada y salida.			Validado ■ Invalidado ☐ No concluyente ☐

Figura 194: Volcado de memoria

Caso 2. Ataque Malware

Al realizar este tipo de ataque, cabe destacar que se analizará el ataque de Ransomware con el fin de analizar mediante un servidor de datos los datos que genera este tipo de virus y el origen de los mismos, para ello en el servidor se mantendrá un analizado de monitoreo para este TeslaCrypt, analizando uno de los link que nos envía por interno y verificando su autenticidad, también se mostrara el origen de encriptación de este link para así manejar los datos que nos solicitan para que el creador deje de infectar nuestra información y nos permita trabajar en el equipo.

HACKING ETICO
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA NUBE

DATOS DEL EXPERIMENTO			
Título del experimento:	Infección de Malware	Realizado por:	Carlos Pita
No. Prueba:	Caso-02	Fecha inicio:	17/11/2023
Tipo prueba:	Laboratorio Forense	Fecha fin:	17/11/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Ataque Ransomware (teslacrypt)	Fase:	Adquisición de evidencia
Nivel complejidad prueba:	Dificil	Tiempo ejecución:	8 horas
HERRAMIENTAS APLICADAS			
Hardware:		Virtualización:	Windows 7 Kali Linux
Software:	SE hacking Access Data Virtual box	Redes:	Red solo-anfitrion
DISEÑO DEL EXPERIMENTO			
Procedimientos: 1. Instalacion de Maquinas virtuales 2. Instalacion de herramientas 3. Instalacion y ataque de Teslacrypt 4.Resultados obtenidos		Descripción del procedimiento: Anexo 1. Instalaciones Anexo 2. Ataque Anexo 3. Resultados	
Resultados esperados: 1. Configuracion de red 2. Arranque de Ransomware 3. Deteccion de informacion del virus 4. Analisis de la informacion encriptada		Resultados obtenidos: 1. Configuracion de red 2. Arranque de Ransomware 3. Deteccion de informacion del virus 4. Analisis de la informacion encriptada	
Conclusiones: Se establecio que el ataque ejecutado intencionalmente hacia una red de servidores de archivos se produjo de manera efectiva con teslacrypt produciendo que se muestres los resultados enviados por el virus ejecutado. Mediante el analisis se obtuvieron los datos que este virus envio y extrayendo un apartado se determino que el virus envia un link de acceso hacia big coin para el pago del mismos tambien se determino que cada vez que este ataque se ejecuta se crea una nueva cuenta para poder despitar al atacantes de este virus			Validado ■ Invalidado ☐ No concluyente ☐

Figura 195: Ataque Malware

Caso 3. Defacement

Aquí se analizará la clonación de una página web o aplicativo web cambiando la apariencia de su index para poder demostrar que se puede realizar ataques con páginas similares o hacer arrancar una página similar para que la víctima muestre datos relevantes.

HACKING ETICO
REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA NUBE

DATOS DEL EXPERIMENTO			
Título del experimento:	Defacement	Realizado por:	Carlos Pita
No. Prueba:	Caso-03	Fecha inicio:	20/11/2023
Tipo prueba:	Laboratorio Forense	Fecha fin:	20/11/2023
DETALLES DEL EXPERIMENTO			
Objetivo del experimento:	Defacement a pagina web	Fase:	Adquisición de evidencia
Nivel complejidad prueba:	Dificil	Tiempo ejecución:	8 horas
HERRAMIENTAS APLICADAS			
Hardware:		Virtualización:	Apache Windows 10 SQL
Software:	Xampp Virtual box	Redes:	Red wifi
DISEÑO DEL EXPERIMENTO			
Procedimientos: 1. Instalacion de Servidor Xampp 2. Instalacion de programas 3. Cambio de pagina a atacar 4.Resultados nueva pagina ya hackeada		Descripción del procedimiento: Anexo 1. Instalaciones Anexo 2. Ataque Anexo 3. Resultados	
Resultados esperados: 1. Configuracion de Xampp 2. Visualizacion de pagina victima 3. Programacion de pagina victima index 4. Visualizacion de pagina hackeada		Resultados obtenidos: 1. Configuracion de Xampp 2. Visualizacion de pagina victima 3. Programacion de pagina victima index 4. Visualizacion de pagina hackeada	
Conclusiones: Se establecio un servidor local para este estudio y un pagina web creada por auditoria propia (victima) ejecutandose de manera correcta y luego se programo el cambio para que se complete este tipo de ataque defacement mostrando el cambio entre una pagiana original y una atacada.		Validado ■ Invalidado ☐ No concluyente ☐	

Figura 196: Defacement