Maestría en

Ciberseguridad

Trabajo previo a la obtención de título de

Magister en Ciberseguridad

AUTOR/ES:

ALDAZ SANCHEZ DAVID ISRAEL
ANDRADE PAZMIÑO GABRIEL HERNAN
GONZALON MALDONADO CHRISTIAN FABRICIO
VASQUEZ RIVAS HECTOR EDUARDO

TUTOR:
Iván Reyes Chacón

RECOLECCIÓN, IDENTIFICACIÓN Y ANÁLISIS DE ARTEFACTOS FORENSES GENERADOS DURANTE VIDEOLLAMADAS DE ZOOM.

Quito - Ecuador

Junio – 2025

REINVENTEMOS EL FUTURO

Certificación de autoría

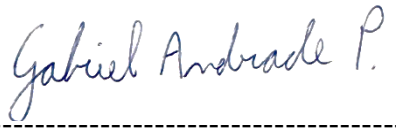
Nosotros, David Aldaz, Héctor Vásquez, Christian Gonzalón y Gabriel Andrade, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firma del graduando
David Aldaz

Firma del graduando
Héctor Vásquez

Firma del graduando
Christian Gonzalón



Firma del graduando
Gabriel Andrade

Autorización de Derechos de Propiedad Intelectual

Nosotros, David Aldaz, Héctor Vásquez, Christian Gonzalón y Gabriel Andrade, en calidad de autores del trabajo de investigación titulado “Recolección, identificación y análisis de artefactos forenses generados durante videollamadas de Zoom.”, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, junio 2025

Firma del graduando
David Aldaz

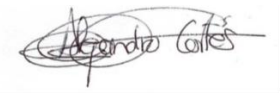
Firma del graduando
Héctor Vásquez

Firma del graduando
Christian Gonzalón

Firma del graduando
Gabriel Andrade

Aprobación de dirección y coordinación del programa

Nosotros, Alejandro Cortés López e Iván Reyes, declaramos que: David Aldaz, Héctor Vásquez, Christian Gonzalón y Gabriel Andrade son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



_____ _____

Alejandro Cortés L.
Maestría en Ciberseguridad

Iván Reyes Ch.
Maestría en Ciberseguridad

DEDICATORIA

Nosotros, David Aldaz, Héctor Vásquez, Christian Gonzalón y Gabriel Andrade, dedicamos este Trabajo Final a cada uno de los integrantes de cada familia, gracias por su compresión y respaldo incondicional durante toda la duración del proceso de maestría en Ciberseguridad, por la motivación para seguir adelante y alcanzar cada uno de los objetivos en todas las materias que formaron parte. Su presencia fue una de las principales motivaciones.

A cada uno de los maestros de esta Maestría en Ciberseguridad, por su tan importante guía, conocimientos impartidos en cada una de las clases asíncronas, por sus experiencias compartidas e inspirarnos a ir más adelante en la obtención de la excelencia en el ámbito profesional.

Dedicamos este trabajo final a nuestros padres, que con su esfuerzo, valores y enseñanzas han sido fundamentales en cada una de las etapas para la formación personal, profesional y académica.

AGRADECIMIENTOS

La finalización de esta maestría en Ciberseguridad y la realización del trabajo final denominado “Recolección, identificación y análisis de artefactos forenses generados durante videollamadas de Zoom” no habría sido posible sin el apoyo y ayuda de las personas y Universidad, a quienes deseamos expresar nuestro sincero agradecimiento.

En primera instancia, agradecemos a nuestras familias, por el apoyo absoluto en el transcurso de toda esta maestría y también a lo largo de cada una de nuestras carreras profesionales. Sin su apoyo, no sería posible la obtención de este título tan importante en cada una de nuestras vidas.

Agradecemos de una manera especial a la Universidad Internacional del Ecuador por brindarnos la oportunidad de formarnos académicamente en un área tan importante como la seguridad informática. La calidad de académica demostrada por la universidad y el programa tan interesante han sido importantes en el desarrollo de cada uno de los integrantes de este grupo en el ámbito profesional

Este trabajo final de maestría es el resultado del arduo esfuerzo y compromiso de cada uno de los integrantes del grupo de estudio. A cada uno de los integrantes de este grupo de trabajo, el más profundo agradecimiento.

Este trabajo es un reflejo del esfuerzo colectivo y el compromiso de muchas personas. A todos ellos, mi más profunda gratitud.

RESUMEN

En el presente documento se detallan todas las actividades realizadas como parte del trabajo final de la maestría de Ciberseguridad. Se puntualizan todas las configuraciones que se realizaron para la instalación, implementación y obtención de resultados del trabajo final de la maestría, el cual tiene como nombre “Recolección, identificación y análisis de artefactos forenses generados durante videollamadas de Zoom.”

La elección del tema “Recolección, identificación y análisis de artefactos forenses generados durante videollamadas de Zoom” como trabajo final se lo realizó dado que en el mundo digital que actualmente estamos viviendo, las plataformas digitales para videoconferencias, en especial Zoom, se usan a cada momento en las cuales se tratan diversos temas que pueden ser sensibles e información confidencial, que, por tal motivo con este trabajo, se puede comprender qué tipo de datos pueden ser recuperados, evaluar su relevancia en investigaciones y proponer metodologías para su extracción y análisis sin comprometer su integridad. Así, se podrá mejorar la seguridad digital y proporcionar herramientas para profesionales en ciberseguridad y peritaje forense.

Para la ejecución del trabajo final se utilizaron tres máquinas virtuales con tres diferentes sistemas operativos (Microsoft Windows 10, Mac OS (Catalina) y Linux Ubuntu). Con el uso de tres sistemas operativos diferentes se pudo validar el comportamiento de la plataforma Zoom durante una videoconferencia. Se realizaron pruebas con video y audio activo, utilización de chat para compartición de texto y documentos. Estas pruebas se ejecutaron en un ambiente controlado, se extrajeron las imágenes con ayuda de diferentes herramientas forenses como FTK Imager y Autopsy para poder evaluar toda la información que fue registrada, análisis de logs e identificación de patrones en almacenamiento de información. Con lo cual se pudo tener un resultado integral.

ABSTRACT

This document outlines the activities conducted as part of the final project for the Master's Degree in Cybersecurity. It describes the configurations and processes implemented during the installation, and results analysis of the project titled "Collection, Identification, and Analysis of Forensic Artifacts Generated During Zoom Video Calls."

The selection of this topic was motivated by the constant use of technology with videoconferencing platforms in modern communication, specially Zoom; this platform is frequently used for discussions involving sensitive and confidential information. As such, this project aims to examine the types of data that can be recovered from videoconferences used during Zoom calls, evaluate their relevance in digital investigations, and propose methodologies for extraction and analysis while maintaining data integrity. This research is designed to improve digital security practices and provide effective tools for cybersecurity professionals and forensic investigators.

To accomplish this, three virtual machines were used in different operating systems: Microsoft Windows 10, macOS Catalina, and Linux Ubuntu. The use of these different operating systems enabled a comparative analysis of Zoom's behavior in each environment. Tests were made with active video and audio, chat functionality, and document sharing. Following the completion of video calls in each environment, system images were captured using forensic applications like FTK Imager and Autopsy. These images were then analyzed to identify recorded data, examine log files, and detect patterns in information storage.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPÍTULO 1

1. INTRODUCCIÓN

1.1. Definición del proyecto.

En los últimos años especialmente, desde el año 2020 por la pandemia COVID-19, las plataformas de videollamadas han experimentado un crecimiento exponencial, impulsado por la necesidad de comunicación remota en diversos entornos y facilitar la interacción entre las personas por trabajo, estudios, etc. La plataforma Zoom, como una de las herramientas más utilizadas y populares a nivel mundial, ha generado preocupaciones en el ámbito de la seguridad digital debido a incidentes relacionados con accesos no autorizados, vulnerabilidades y la gestión de datos de los usuarios.

El incremento en el uso de Zoom en sectores estratégicos como educación, gobierno, empresas privadas y negocios, ha convertido a esta plataforma en un objetivo para atacantes cibernéticos. Los riesgos incluyen la exposición y filtración de información confidencial, la interceptación de comunicaciones y el acceso no autorizado a cuentas de usuarios.

Este trabajo final de maestría denominado “Recolección, identificación y análisis de artefactos forenses generados durante videollamadas de Zoom” busca examinar los artefactos digitales generados por Zoom y su relevancia en investigaciones de ciberseguridad. A través del análisis de archivos y registros del sistema, se busca determinar qué información puede ser recuperada y cómo esta podría ser utilizada en procesos forenses.

Esta información podrá servir como base para el desarrollo de nuevas estrategias de investigación digital, permitiendo establecer métodos efectivos para la recopilación y preservación de evidencia digital.

1.2. Justificación e importancia del trabajo de investigación

El análisis de artefactos digitales en plataformas de videoconferencia es fundamental para fortalecer la seguridad digital a nivel mundial. La plataforma de videoconferencias Zoom, al ser ampliamente utilizado en diferentes contextos como sociales, empresariales, educativos y

gubernamentales, genera información que podría ser clave en investigaciones relacionadas con delitos cibernéticos.

Los equipos digitales proporcionan información de gran valor sobre la actividad de los usuarios dentro de la plataforma de videoconferencia como historiales de reuniones, datos de inicio de sesión, detalles de conexión, usuarios conectados, documentación e información compartida entre participantes y metadatos de videollamadas. Comprender la manera en que Zoom almacena y gestiona toda esta información puede permitir mejorar las técnicas de investigación forense y contribuir a la creación de herramientas especializadas para la recuperación de evidencia digital para cualquier tipo de investigación.

El trabajo permite comprender qué tipo de datos son almacenados y pueden ser recuperados, evaluar su relevancia en investigaciones y proponer metodologías para su extracción y análisis sin comprometer su integridad ni vulnerar derechos. Así, se podrá mejorar la seguridad digital y proporcionar herramientas para profesionales en ciberseguridad y peritaje forense.

1.3. **Alcance.**

El presente trabajo final se centrará en la investigación de artefactos digitales generados por la plataforma Zoom, mediante la utilización de máquinas virtuales alojadas en VirtualBox como equipo host; las máquinas virtuales que se utilizarán están en tres sistemas operativos diferentes: Windows, Linux y MacOS. Se analizarán versiones recientes de la aplicación, tales como:

- Zoom para Windows (versión 6.4.7 y posteriores)
- Zoom para macOS (versión 6.4.10 y posteriores)
- Zoom para Linux Ubuntu 22.0.4 (versión 6.4.3 y posteriores)

El estudio considerará diversos escenarios, tales como:

- Videollamadas realizadas y recibidas.
- Grabaciones locales y en la nube.
- Archivos temporales y registros de logs.

- Metadatos asociados a sesiones de Zoom.
- Artefactos almacenados en navegadores web.
- Información compartida entre participantes

El estudio incluirá el análisis de posibles técnicas de eliminación de datos dentro de Zoom y su impacto en la investigación forense. No se analizará la infraestructura de Zoom ni sus mecanismos de cifrado, este trabajo final está enfocado en la extracción y análisis de datos en dispositivos locales.

1.4. **Objetivos.**

1.4.1. **Objetivo general**

Establecer una metodología para la identificación, extracción y análisis de artefactos digitales generados por Zoom con el fin de contribuir a investigaciones forenses en ciberseguridad.

1.4.2. **Objetivo específico**

- Identificar los artefactos forenses generados por Zoom en sistemas Windows, Linux y macOS.
- Diseñar procedimientos de extracción garantizando la integridad de la evidencia.
- Analizar los datos recolectados y evaluar su utilidad en investigaciones cibernéticas.
- Comparar herramientas forenses para la extracción y análisis de artefactos.
- Documentar hallazgos y desarrollar recomendaciones para mejorar las investigaciones digitales.

CAPÍTULO 2

2. REVISIÓN DE LITERATURA

2.1. Estado del Arte

Según Al Barghuthi, “Las pruebas digitales obtenidas a partir de aplicaciones de videoconferencia pueden resultar útiles en las investigaciones y son utilizadas por particulares de todos los sectores. Aplicaciones como Skype, Google Video/Messaging series y Microsoft Teams se han utilizado más comúnmente en los últimos años” (Al Barghuthi, 2013). Debido a la pandemia de COVID-19, muchas escuelas, empresas y personas han recurrido a la aplicación de videoconferencia Zoom para comunicarse entre sí. Este rápido aumento del tráfico de usuarios ha llevado al escrutinio y a la sospecha respecto a las prácticas de ciberseguridad de la empresa después de que se encontraran importantes exploits dentro de sus protocolos.

Por otro lado, O’Flaherty en su publicación del 2020 menciona: “Estos problemas de seguridad han dado lugar a violaciones de la privacidad cometidas a través de Zoom Bombings” (O'Flaherty, 2020; Lorenz y Alba, 2020) y por consecuencia la explotación de protocolos básicos. Los Zoom Bombings implican interrupciones no deseadas de conferencias de cualquier tipo, incluyendo, entre otras, la proyección de imágenes ilícitas y el uso de blasfemias verbales, lo que podría constituir una forma de acoso criminal (Office, 2020; Setera, 2020).

De la misma forma, (Azab, 2012) caracterizaron el tráfico de red de la aplicación Skype y demostraron las dificultades a las que se enfrentan los expertos forenses cuando intentan interceptar o analizar este tráfico. El trabajo también identificó y analizó las diferencias descubiertas en el tráfico entre versiones antiguas y diferentes de la aplicación Skype.

Posteriormente, (Majeed, 2016) exploró el comportamiento de Skype, Facebook y Twitter dentro del entorno Windows 10. Se descubrió que Skype almacenaba en disco mensajes de chat en texto plano, así como otra información relativa a un usuario.

Los problemas de seguridad más notables aparecen en los informes de vulnerabilidades y exposiciones comunes (CVE). Zoom publicó un informe de seguridad en 2018 detallando dos CVE importantes. CVE-2018-157152 mostró cómo los actores maliciosos podían tomar el control de las pantallas de los usuarios, falsificar mensajes de chat y controlar otros aspectos de la reunión. CVE-2020-114433 detalló cómo el instalador de TI de Windows Zoom, que elimina archivos y datos antes de reinstalar Zoom, podría ser explotado para eliminar archivos que un usuario normalmente no podría eliminar. Se encontraron vulnerabilidades adicionales en la aplicación Zoom pero a la fecha Zoom ha respondido con parches para estos problemas, solucionándolos en su mayoría.

2.2. Marco Teórico

2.2.1. Plataforma de videoconferencia Zoom

La plataforma de videoconferencia Zoom, es una aplicación de video comunicaciones la cual permite realizar videollamadas, conferencias virtuales, reuniones virtuales, seminarios, compartición de archivos, mensajería y uso compartido de pantallas entre los participantes. Esta aplicación es una de las más populares a nivel mundial por su facilidad de uso para temas personales, laborales, empresariales y educacionales.

El aplicativo de videoconferencia Zoom tiene dos modalidades: gratuita y pagada; la versión gratuita tiene limitaciones en su usabilidad con respecto a la pagada, la principal limitación es el tiempo permitido para realizar videollamadas para más de dos participantes, la cual es de 40 minutos, posterior a este tiempo la videollamada automáticamente finaliza. Adicionalmente, la versión gratuita únicamente permite grabaciones locales, es decir se almacena solo en la computadora del anfitrión y no en la nube de

Zoom. La versión pagada no tiene restricciones de tiempo de uso, las grabaciones se pueden almacenar localmente o en la nube de Zoom. Un aspecto importante es que, dentro de la versión pagada de Zoom, existen diferentes tipos de licenciamiento, cada uno con su característica principal como, por ejemplo:

- Pro: Permite hasta 100 participantes simultáneos, 5 GB de almacenamiento en la nube de Zoom para grabaciones, elaboración de informes básicos.
- Business: Permite hasta 300 participantes simultáneos, 10 GB de almacenamiento en la nube de Zoom para grabaciones, elaboración de informes avanzados, dominio de correo personalizado

Debido a la popularidad que ha tenido a nivel mundial, la plataforma Zoom se ha visto obligada a implementar reglas de ciberseguridad para proteger los datos compartidos durante las videollamadas, garantizar la privacidad de las comunicaciones y a resguardar las grabaciones almacenadas en su nube.

2.2.2. **Tipos de artefactos forenses en Zoom**

Los artefactos digitales generados por Zoom incluyen:

- Logs de reuniones: Archivos almacenados en %APPDATA%\Roaming\Zoom\logs (Windows) o ~/Library/Application Support/zoom.us (macOS), que registran conexiones, participantes, fechas y horas.
- Grabaciones locales y en la nube: Archivos en formatos “.zoom” o “.mp4”, que incluyen metadatos como la duración de la reunión, el identificador del host y los permisos de grabación.
- Chats: Mensajes almacenados localmente o en la nube, que pueden contener información sensible o adjuntos.
- Metadatos: Información sobre configuraciones de la reunión, como cifrado, roles de los participantes y ajustes de seguridad.

- Archivos temporales: Datos de caché generados durante las sesiones, que pueden incluir fragmentos de audio o video.
- Registros en navegadores: Cookies y datos de sesiones iniciadas a través de la versión web de Zoom.

Estos artefactos son esenciales para reconstruir eventos, identificar accesos no autorizados o recuperar datos eliminados en investigaciones forenses.

2.2.3. Desafíos en el análisis forense de Zoom

El análisis forense de la plataforma Zoom presenta desafíos como la fragmentación de datos, la eliminación intencional de artefactos y la gestión de datos en la nube propia de la aplicación. Además, las diferencias entre sistemas operativos (Windows, Linux y macOS) y las actualizaciones frecuentes de Zoom pueden afectar la consistencia de los artefactos generados. Por lo tanto, las herramientas forenses deben ser capaces de adaptarse a estos entornos dinámicos y garantizar la integridad de la evidencia.

2.2.4. Herramientas forenses para el análisis de artefactos Zoom

2.2.4.1. Identificación de herramientas forenses

A continuación, presentamos una lista de algunas herramientas forenses que pueden ser utilizados para el análisis de los artefactos Zoom. Para cada herramienta, se proporciona una descripción y un propósito seguido de su relevancia para las investigaciones forenses.

FTK Imager: Es una utilidad que fue desarrollada por AccessData y se utiliza para adquirir imágenes de disco gratuitamente y extraer archivos. Se puede utilizar la herramienta para recuperar logs, grabaciones y configuración de Zoom, ya que la utilidad soporta el sistema de archivos NTFS y APFS. Además, esta herramienta puede generar hash MD5 / SHA-1, lo que garantiza la integridad de los artefactos.

Autopsy: Plataforma de código abierto desarrollada por Basis Technology. Permite analizar sistemas de archivos, recuperar archivos eliminados y correlacionar eventos. Es útil para identificar chats, logs y metadatos de Zoom en Windows y macOS.

X-Ways Forensics: Herramienta comercial avanzada, conocida por su velocidad y capacidad para analizar sistemas de archivos complejos. Permite reconstruir sesiones de Zoom, recuperar datos fragmentados y analizar metadatos detallados.

Log Parser Studio: Herramienta gratuita de Microsoft para analizar logs en formatos CSV, XML y JSON. Es efectiva para procesar logs de Zoom y correlacionar eventos de reuniones, como conexiones o transferencias de archivos.

Wireshark: Software de código abierto para análisis de tráfico de red. Captura paquetes relacionados con videollamadas de Zoom, proporcionando información sobre metadatos de conexión, como direcciones IP y puertos.

Magnet AXIOM: Herramienta comercial que integra análisis de discos, dispositivos móviles y datos en la nube. Es útil para recuperar grabaciones en la nube y artefactos almacenados en navegadores

EnCase: Software comercial de Guidance Software, utilizado para análisis forense integral. Soporta la extracción de artefactos de Zoom y la validación de su integridad, siendo ampliamente utilizado en entornos legales.

2.2.4.2. Relevancia en el análisis de Zoom

Estas herramientas permiten analizar una amplia gama de artefactos de Zoom, desde logs almacenados en directorios específicos hasta grabaciones y metadatos. Su capacidad para preservar la cadena de custodia, recuperar datos eliminados y adaptarse a diferentes sistemas operativos las hace esenciales para investigaciones forenses. Además, la combinación de herramientas gratuitas y comerciales ofrece flexibilidad para diferentes contextos, desde investigaciones académicas hasta casos legales complejos.

2.2.5. **Comparación de herramientas forenses**

2.2.5.1. Metodología de comparación

La evaluación se realizó en un entorno controlado con sistemas Windows 11 (64 bits), Ubuntu 24.04 y macOS Catalina (10.15.7), utilizando Zoom en windows versión 6.4.7. Se generaron artefactos estandarizados mediante:

- Videollamadas simuladas con 3 o 4 participantes durante 15 minutos.
- Grabaciones locales (.mp4) y en la nube.
- Chats con 20 mensajes, incluyendo archivos adjuntos (imágenes y documentos).
- Eliminación intencional de logs y grabaciones para probar recuperación.
- Configuraciones de Zoom modificadas para simular diferentes escenarios (cifrado habilitado/deshabilitado, roles de participante).

Durante el trabajo hemos descartado el uso de X-Ways Forensics debido su costo elevado (licencia comercial) y curva de aprendizaje limitan su accesibilidad para trabajos de investigación que no sean empresariales como este caso. Adicionalmente, también hemos descartado otras herramientas comerciales como los son Magnet AXIOM y En Case, ya que no son de fácil accesibilidad para ambientes de estudio o investigativos.

El conjunto de datos analizados fue aproximadamente de 1 GB, incluyendo logs, grabaciones, chats y configuraciones. Los criterios de evaluación fueron:

- Facilidad de uso: Interfaz, curva de aprendizaje y capacidad para generar informes.
- Precisión: Porcentaje de artefactos identificados y extraídos correctamente.
- Profundidad de análisis: Nivel de detalle en los datos recuperados y capacidad para analizar artefactos complejos.

- Tiempo de análisis: Duración del procesamiento del conjunto de datos.
- Detección de artefactos eliminados: Capacidad para recuperar datos borrados o corrompidos.
- Compatibilidad: Rendimiento en Windows, Linux y macOS.
- Cobertura de logs: Análisis de registros específicos de Zoom (reuniones, conexiones, chats).

2.2.6. **Resultados de la evaluación**

2.2.6.1. Facilidad de uso

FTK Imager: Interfaz intuitiva con un diseño centrado en la adquisición de imágenes y exploración de sistemas de archivos. Es ideal para usuarios principiantes, pero los informes generados (HTML) son básicos y requieren herramientas adicionales para personalización. Curva de aprendizaje: baja.

Autopsy: Interfaz modular con complementos para análisis avanzado. La cantidad de opciones puede ser abrumadora para nuevos usuarios, pero los informes son detallados, exportables a PDF y ofrecen visualizaciones claras. Curva de aprendizaje: moderada.

Log Parser Studio: Basada en consultas SQL, es adecuada para analistas técnicos. La configuración inicial es compleja, pero los informes son altamente personalizables. Curva de aprendizaje: moderada-alta.

2.2.6.2. Precisión

FTK Imager: Detectó casi todos los tipos de artefactos (logs, grabaciones, configuraciones), pero tuvo dificultades con metadatos fragmentados en APFS.

Autopsy: Identificó una gran cantidad de los artefactos, con limitaciones en la recuperación de chats eliminados en macOS.

Log Parser Studio: Limitada por su enfoque en logs y no en grabaciones o archivos temporales, no permite obtener todos los artefactos necesarios.

2.2.6.3. Profundidad de análisis

FTK Imager: Proporciona análisis básico de archivos y metadatos, pero no permite correlaciones avanzadas entre artefactos, como vincular chats con logs de reuniones.

Autopsy: Ofrece análisis profundo de sistemas de archivos, con capacidad para correlacionar chats, logs y metadatos de reuniones. Incluye módulos para análisis de líneas de tiempo.

Log Parser Studio: Especializada en logs, permite identificar patrones en registros de reuniones, pero no analiza grabaciones ni archivos complejos.

2.2.6.4. Tiempo de análisis

FTK Imager: 12 minutos para analizar 1 GB, con un rendimiento estable, pero sin optimización para grandes volúmenes.

Autopsy: 14 horas, con mayor tiempo en la indexación inicial de sistemas de archivos.

Log Parser Studio: No se utilizó en este estudio para analizar logs, ya que tenía las mismas funcionalidades de FTK Imager.

2.2.6.5. Detección de artefactos eliminados

FTK Imager: No tiene capacidad para detectar grabaciones corrompidas.

Autopsy: Capacidad para recuperar los datos eliminados, con soporte para archivos fragmentados en NTFS y APFS.

Log Parser Studio: No está diseñada para recuperación de datos eliminados, solo analiza logs existentes.

2.2.6.6. Compatibilidad con Windows, Linux y MacOS

FTK Imager: Excelente compatibilidad con Windows; limitada en Linux y macOS, requiere emuladores como Wine.

Autopsy: Compatible con los tres sistemas operativos, con mejor rendimiento en Windows debido a la optimización de complementos.

Log Parser Studio: Exclusiva para Windows, no compatible con Linux y macOS.

2.2.6.7. Cobertura de logs

FTK Imager: Detecta logs de Zoom y configuraciones, pero no ofrece correlación avanzada de eventos.

Autopsy: Analiza logs, chats y metadatos, con capacidad para vincular eventos de reuniones en una línea de tiempo.

Log Parser Studio: Especializada en logs, con análisis detallado de registros de reuniones y conexiones.

2.2.6.8. Análisis de limitaciones

FTK Imager: Limitado en el análisis de datos en la nube y correlaciones avanzadas. No soporta análisis de tráfico de red.

Autopsy: Puede ser lento en sistemas con grandes volúmenes de datos y requiere complementos para análisis avanzado.

X-Ways Forensics: Su costo elevado (licencia comercial) y curva de aprendizaje limitan su accesibilidad para equipos con recursos limitados.

Log Parser Studio: No analiza grabaciones ni datos eliminados, restringiendo su utilidad a logs.

2.2.7. Errores encontrados

Durante las pruebas, pudimos identificar algunos errores entre los que podemos listar:

FTK Imager: Fallos ocasionales al leer metadatos en sistemas de macOS generan que la aplicación se cierre espontáneamente sin permitir facilidad el análisis.

Log Parser Studio: Errores en el procesamiento de algunos logs con formatos no estándares, que requerían reprocesamiento manual.

2.2.8. Resultados y análisis

2.2.8.1. Tabla comparativa

Tabla 1

Comparativa de los resultados

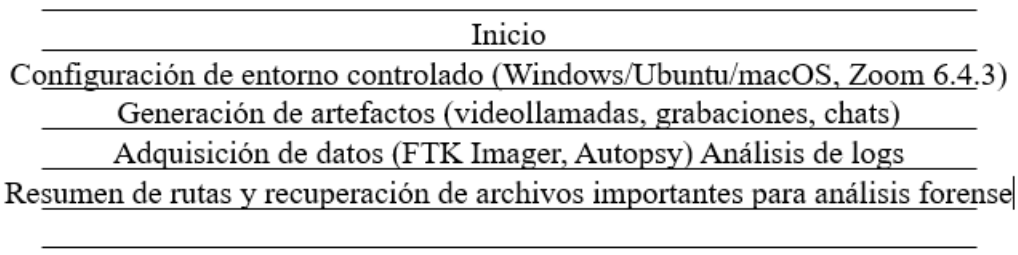
Criterio	FTK Imager	Autopsy	Log Parser Studio
Costo	Gratuito	Gratuito	Gratuito
Facilidad de uso	Alta	Media	Media
Precisión	Muy Alta	Muy Alta	Alta
Profundidad de análisis	Básica	Alta	Media
Tiempo de análisis (1 GB)	10 min	14 horas	No analizado
Detección de datos eliminados	Alta	Muy Alta	Muy Baja
Compatibilidad	Windows/Ubuntu	Windows/macOS /Ubuntu	Windows/macOS
Cobertura de logs	Media	Alta	Alta

Nota. En la Tabla 1 se puede observar la comparativa de las diferentes herramientas utilizadas para el análisis forense realizado.

2.2.8.2. Diagrama de flujo del proceso de análisis

Figura 1

Diagrama de flujo



Nota. Se observa el flujo utilizado para el proyecto final

2.2.9. Recomendaciones prácticas

Investigaciones corporativas: X-Ways Forensics es ideal debido a su alta precisión y capacidad para recuperar datos eliminados, especialmente en entornos Windows. Es adecuada para casos que requieren análisis exhaustivo y evidencia admisible en tribunales.

Respuesta a incidentes: Autopsy es recomendada por su compatibilidad con Windows y macOS, facilidad para generar informes detallados y soporte para análisis de líneas de tiempo, ideal para equipos con experiencia moderada.

Análisis académico: FTK Imager es la mejor opción por su costo nulo y facilidad de uso, adecuada para proyectos académicos con recursos limitados.

Análisis de logs: Log Parser Studio es la herramienta preferida para analizar logs de Zoom en Windows, especialmente para correlacionar eventos de reuniones y conexiones.

2.2.10. Consideraciones éticas y legales

El análisis forense de artefactos de Zoom debe cumplir con normativas de privacidad, como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley de Protección de Datos Personales en Ecuador. Las herramientas seleccionadas deben garantizar la cadena de custodia y la integridad de la evidencia para ser admisibles en procesos judiciales. Además, los investigadores deben obtener consentimiento o autorización legal para acceder a datos sensibles, como grabaciones o chats, para evitar violaciones de privacidad.

CAPÍTULO 3

3. DESARROLLO

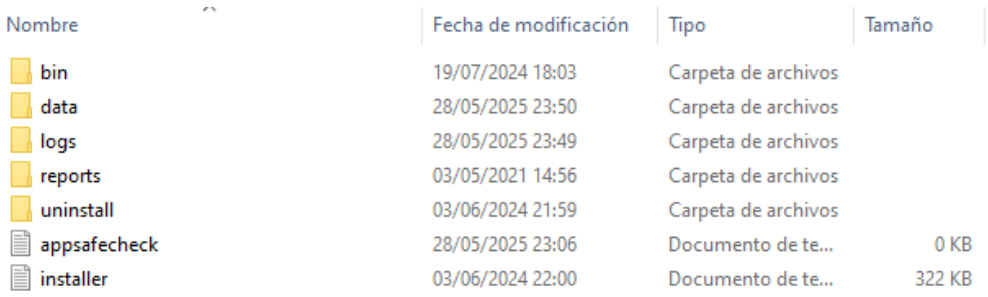
3.1. Desarrollo del trabajo

3.1.1. Instalar versiones específicas de Zoom en Windows, Ubuntu y macOS Catalina

Entorno Windows 10:

Una vez terminada la instalación de Zoom en Windows 10 se genera en la ruta "C:\Users\[Usuario]\AppData\Roaming\Zoom", varios archivos que deja la instalación como se puede ver en la Figura 2.

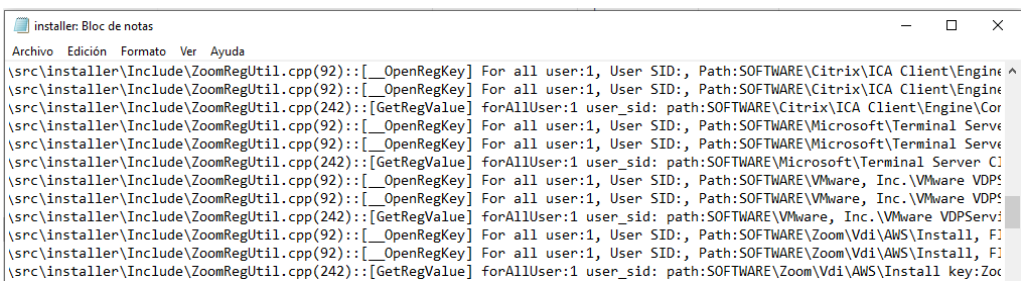
Figura 2
Archivos instalados de Zoom en Windows 10



Nota. Al finalizar la instalación de Zoom, se genera un directorio en el cual se almacena toda la información que genera el aplicativo

El archivo "installer.txt" revela información acerca de la instalación, aquí podemos encontrar información de los procesos que se generaron, en la Figura 3 se puede visualizar que se ingresó al registro de Windows y se añadieron algunas claves.

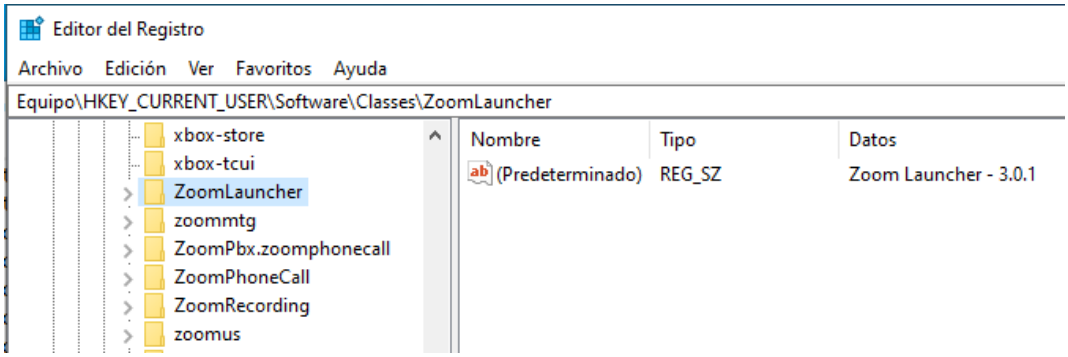
Figura 3
Información archivo "installer.txt"



Nota. Se visualiza la información almacenada en el archivo “installer.txt” del aplicativo Zoom

En el directorio “ZoomLauncher”, como se puede visualizar en la Figura 4, se modifica el registro de Windows y se añaden varias claves en el mismo que servirán para la ejecución de Zoom

Figura 4
Modificación registro Windows

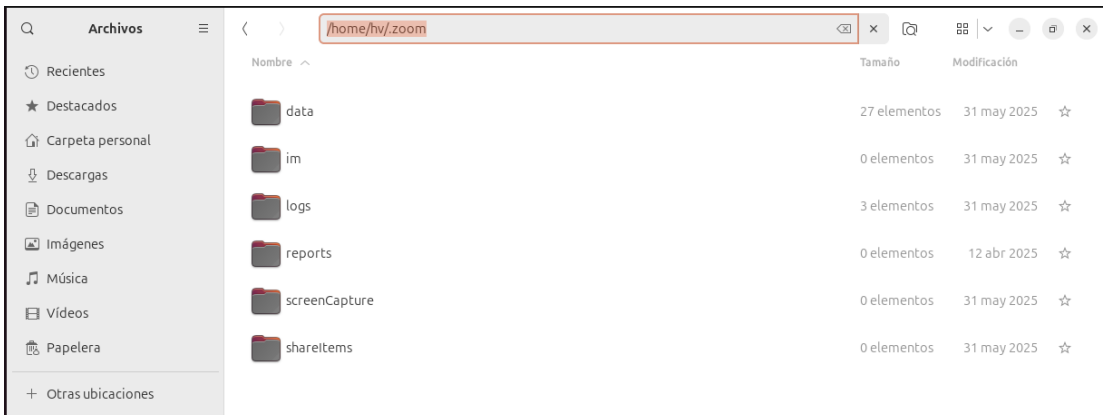


Nota. En el directorio “ZoomLauncher” se almacenan las claves que serán usadas para el funcionamiento del aplicativo Zoom

Entorno Linux (Ubuntu):

Una vez terminada la instalación de Zoom en Ubuntu se genera en la ruta “/home/[Usuario] /.zoom”, varios archivos que deja la instalación como se puede ver en la Figura 5.

Figura 5
Archivos instalados de Zoom en Ubuntu



Nota. Al finalizar la instalación de Zoom, se genera un directorio en el cual se almacena toda la información que genera el aplicativo

El archivo “history.log” revela información acerca de la instalación, aquí podemos encontrar la fecha de inicio y fin de la instalación, en la Figura 6 se puede observar esta información.

Figura 6

Información archivo “history.log”

Nota. Se visualiza la información almacenada en el archivo “history.log” del aplicativo Zoom

Entorno macOS:

Para levantar la máquina es necesario ejecutar una sección de código el cual permitirá configurar adecuadamente la máquina virtual para proceder con la instalación. Desde la máquina anfitriona Windows, en la terminal ejecutaremos como administrador las siguientes líneas que se pueden ver en la Figura 7:

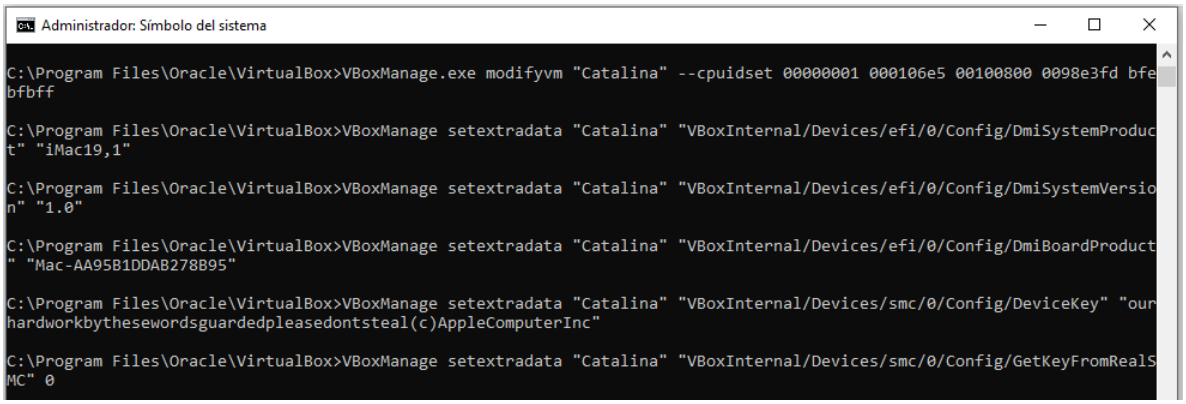
- cd "C:\Program Files\Oracle\VirtualBox\"
- VBoxManage setextradata "Catalina" "VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 0
- VBoxManage.exe modifyvm "Catalina" --cpuidset 00000001 000106e5 00100800 0098e3fd bfebfbff
- VBoxManage setextradata "Catalina" "VBoxInternal/Devices/efi/0/Config/DmiSystemProduct" "iMac19,1"
- VBoxManage setextradata "Catalina" "VBoxInternal/Devices/efi/0/Config/DmiSystemVersion" "1.0"
- VBoxManage setextradata "Catalina" "VBoxInternal/Devices/efi/0/Config/DmiBoardProduct" "Mac-AA95B1DDAB278B95"
- VBoxManage setextradata "Catalina" "VBoxInternal/Devices/smc/0/Config/DeviceKey" "ourhardworkbythesewordsguardedpleasedontsteal(c)AppleComputerInc"

- VBoxManage setextradata "Catalina"

  "VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 0

- VBoxManage setextradata "Catalina" VBoxInternal2/EfiGraphicsResolution 1280x720

Figura 7
Ejecución de comandos en Windows



Nota. Es necesario ejecutar los comandos detallados para poder iniciar la máquina virtual en sistema operativo macOS.

Con los comandos ejecutados se puede instalar el sistema operativo macOS como se visualiza en la Figura 8.

Figura 8
Instalación macOS Catalina

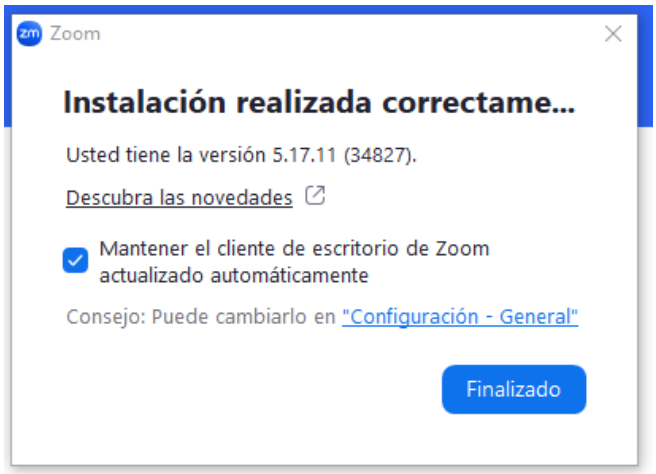
Nota. Se instaló la máquina virtual con sistema operativo macOS Catalina

3.1.2. Configuración entornos controlados para pruebas (máquinas virtuales o físicas)

Instalación de Zoom en Windows:

Inicialmente, el asistente define la ruta donde se va a instalar en el sistema operativo y a continuación se finaliza la instalación como se puede ver en la Figura 9.

Figura 9
Instalación Zoom Windows 10



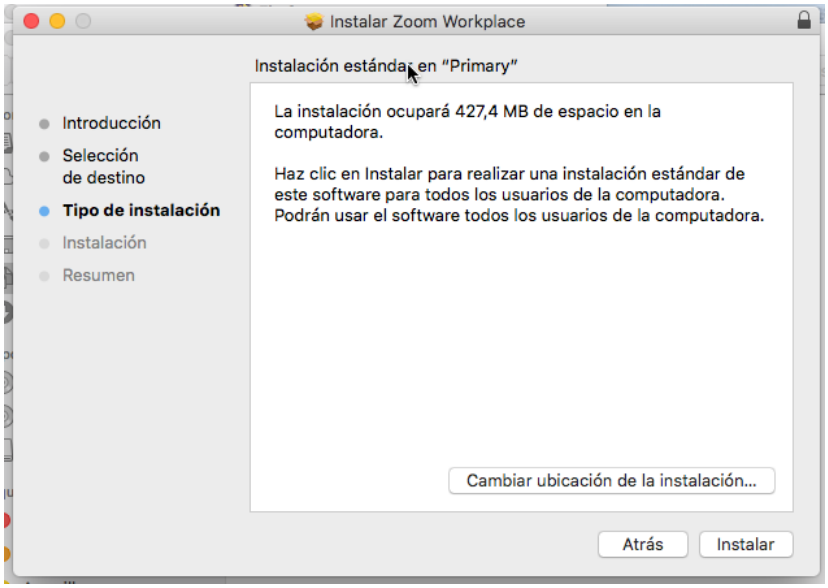
Nota. La versión de Zoom instalada en el equipo es la 5.17.11

Instalación de Zoom en macOS:

La instalación automáticamente escoge la ruta predeterminada, pero al final se puede modificar la ruta como se puede ver en la Figura 10 y finaliza la instalación como se visualiza en Figura 11.

Figura 10

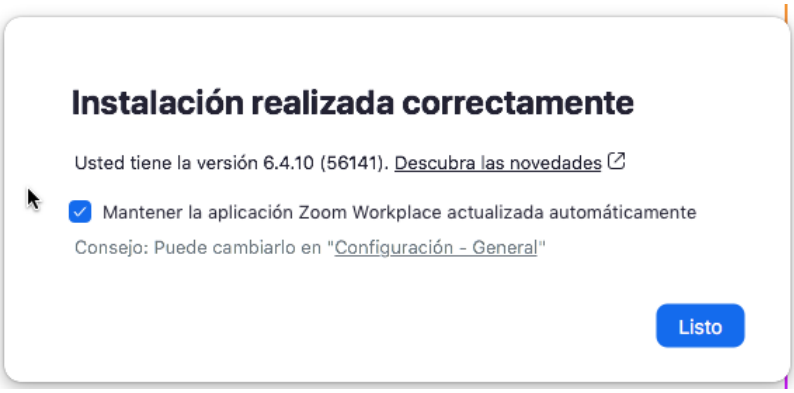
Instalación Zoom en macOS Catalina



Nota. Si se desea, se puede cambiar la ruta de instalación en macOS Catalina.

Figura 11

Finalización de la instalación Zoom en macOS Catalina

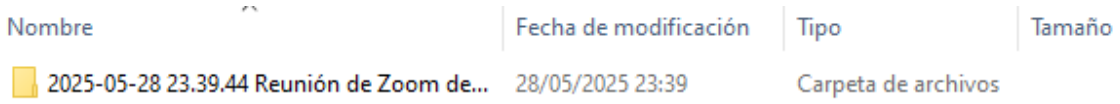


Nota. En macOS Catalina se instala la versión 6.4.10 de Zoom.

3.1.3. Ejecución plataforma Zoom en diferentes escenarios de uso (videollamadas, grabaciones y chat)

Al iniciar una grabación en Windows, y posteriormente finalizar la reunión, se genera un archivo en la ruta "C:\Users\[Usuario]\Documents\Zoom" con la fecha, hora y tema de la reunión de Zoom como se puede ver en la Figura 12.

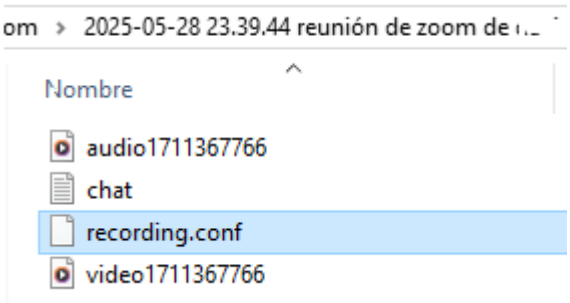
Figura 12
Creación directorio de reunión Zoom



Nota. Se crea un directorio para cada videoconferencia Zoom que se realiza

Una vez finalizada la sesión de Zoom, al ingresar en el directorio que se generó, nos encontraremos con varios archivos que se crearon, entre ellos está el audio, el video, archivos de chat en caso de interacción por el chat durante la grabación y un archivo de configuración como se puede ver en la Figura 13.

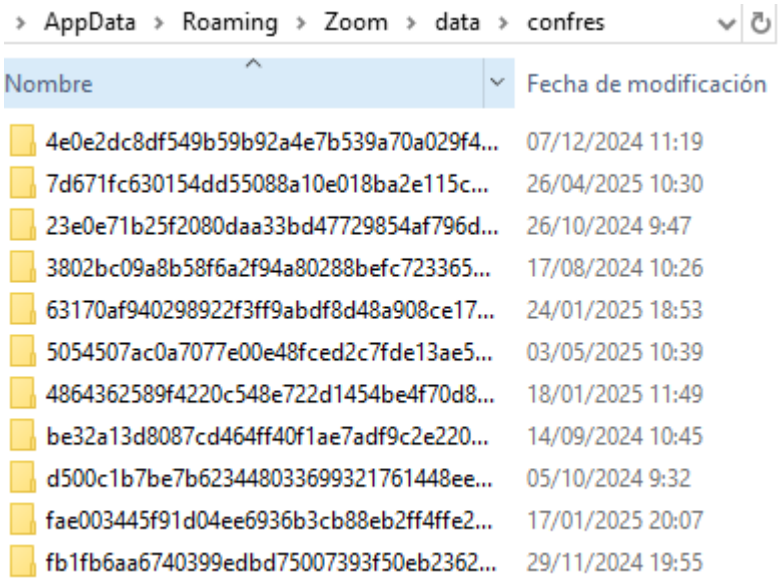
Figura 13
Información almacenada en directorio Zoom



Nota. Zoom crea automáticamente archivos con la información generada en cada videoconferencia Zoom que se realiza

Adicionalmente, se pueden obtener las imágenes que se envían a través del chat de cada sesión, estas imágenes se guardan en el directorio “C:\Users\[Usuario]\AppData\Roaming\Zoom\data\confres” como se puede ver en la Figura 14. Por cada sesión se genera un directorio y dentro del mismo se guardan las imágenes que se enviaron por el chat durante la reunión.

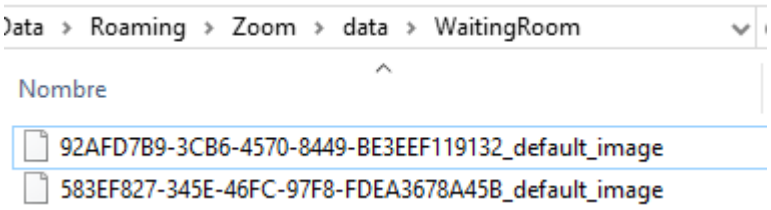
Figura 14
Directorio Zoom de imágenes de chat



Nota. Hay que tomar en cuenta que solamente se van a guardar si la sesión es grabada.

Al iniciar una nueva reunión, en el directorio "C:\Users\[Usuario]\AppData\Roaming\Zoom\data\WaitingRoom" se genera un archivo, el cual, al momento de analizarlo, se trataría de una imagen como se puede ver en la Figura 15.

Figura 15
Imagen de Zoom creada

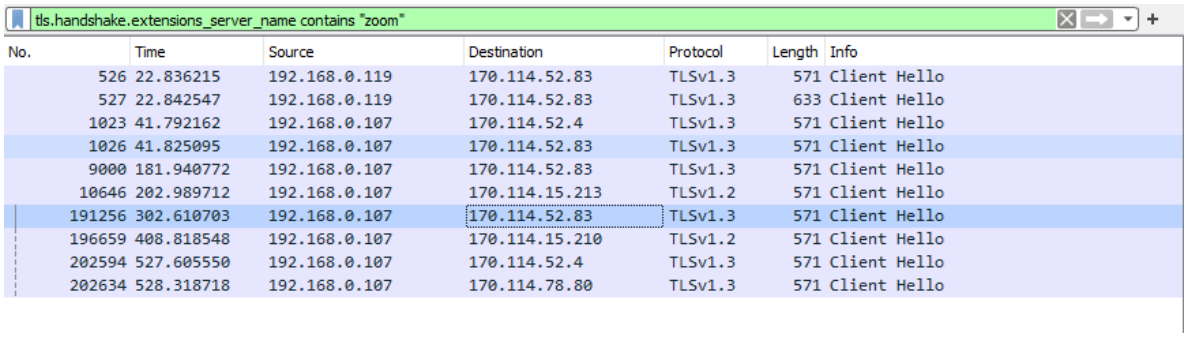


Nota. Zoom crea automáticamente una imagen cuando se inicia una videoconferencia.

3.1.4. Tráfico de red generado durante videoconferencia con Zoom

Al capturar el tráfico que se genera durante una sesión de Zoom, podemos observar que se realizan peticiones hacia los servidores de Zoom, como se puede ver en la Figura 16.

Figura 16
Captura de tráfico de red

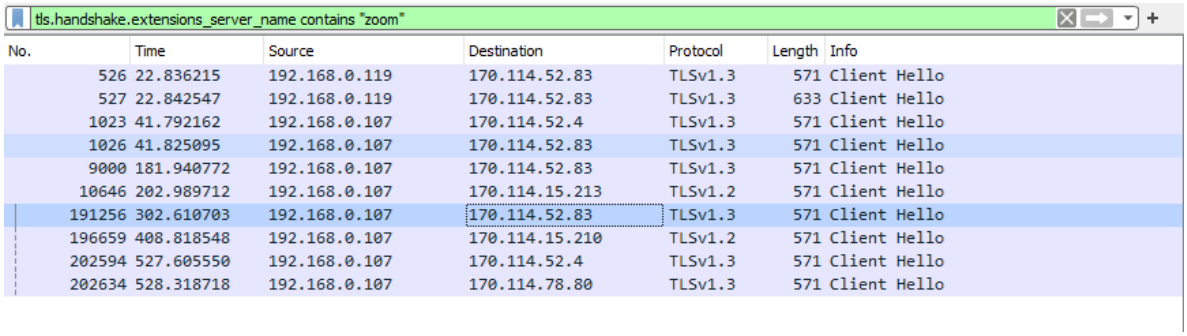


No.	Time	Source	Destination	Protocol	Length	Info
526	22.836215	192.168.0.119	170.114.52.83	TLSv1.3	571	Client Hello
527	22.842547	192.168.0.119	170.114.52.83	TLSv1.3	633	Client Hello
1023	41.792162	192.168.0.107	170.114.52.4	TLSv1.3	571	Client Hello
1026	41.825095	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
9000	181.940772	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
10646	202.989712	192.168.0.107	170.114.15.213	TLSv1.2	571	Client Hello
191256	302.610703	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
196659	408.818548	192.168.0.107	170.114.15.210	TLSv1.2	571	Client Hello
202594	527.605550	192.168.0.107	170.114.52.4	TLSv1.3	571	Client Hello
202634	528.318718	192.168.0.107	170.114.78.80	TLSv1.3	571	Client Hello

Nota. Para la captura de tráfico se utilizó la herramienta Wireshark.

En los primeros registros que se muestran en el tráfico de red podemos apreciar la frase “Client Hello”, esto quiere decir que al iniciar la sesión de Zoom el cliente realiza una petición. Este es el primer mensaje del proceso de establecimiento de una sesión segura TLS. Es enviado por el cliente ya sea el navegador o la aplicación al servidor para iniciar la comunicación segura como se puede ver en la Figura 17.

Figura 17
Primeros registros de Zoom al iniciar videoconferencia

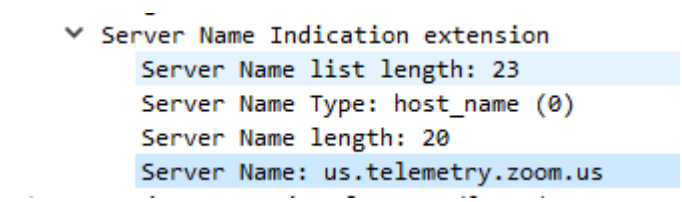


No.	Time	Source	Destination	Protocol	Length	Info
526	22.836215	192.168.0.119	170.114.52.83	TLSv1.3	571	Client Hello
527	22.842547	192.168.0.119	170.114.52.83	TLSv1.3	633	Client Hello
1023	41.792162	192.168.0.107	170.114.52.4	TLSv1.3	571	Client Hello
1026	41.825095	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
9000	181.940772	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
10646	202.989712	192.168.0.107	170.114.15.213	TLSv1.2	571	Client Hello
191256	302.610703	192.168.0.107	170.114.52.83	TLSv1.3	571	Client Hello
196659	408.818548	192.168.0.107	170.114.15.210	TLSv1.2	571	Client Hello
202594	527.605550	192.168.0.107	170.114.52.4	TLSv1.3	571	Client Hello
202634	528.318718	192.168.0.107	170.114.78.80	TLSv1.3	571	Client Hello

Nota. El primer mensaje para el establecimiento de una sesión segura TLS es la frase “Client Hello”

Al analizar uno de los registros y verificar la sección: “Transport Layer Security → Handshake Protocol → Extension: server name → Server Name Indication extensión → Server Name”, se puede visualizar al servidor hacia donde se está estableciendo la conexión como se puede ver en la Figura 18.

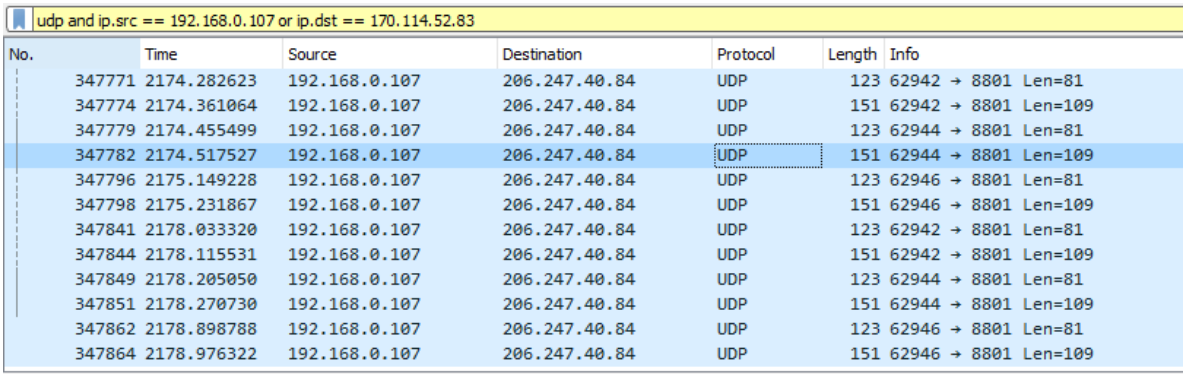
Figura 18
Registros de conexión de Zoom



Nota. Ese puede ver que el registro al cual está realizando la conexión de Zoom, que en el ejercicio es en los Estados Unidos.

Podemos buscar a que IP está enmascarando ese DNS para lo cual hacemos un nslookup a "us.telemetry.zoom.us". Luego aplicamos un filtro en Wireshark para visualizar el tráfico de Audio y Video que se está generando como se puede ver en la Figura 19.

Figura 19
Tráfico de audio y video de Zoom



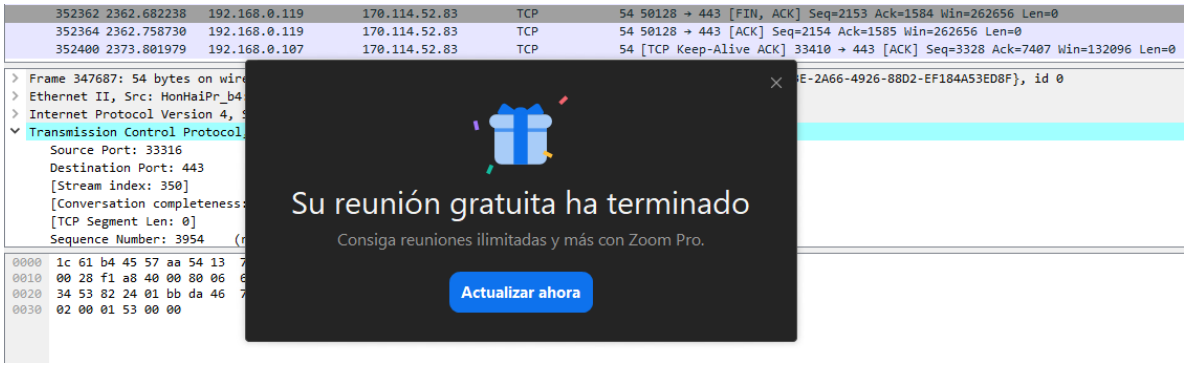
No.	Time	Source	Destination	Protocol	Length	Info
347771	2174.282623	192.168.0.107	206.247.40.84	UDP	123	62942 → 8801 Len=81
347774	2174.361064	192.168.0.107	206.247.40.84	UDP	151	62942 → 8801 Len=109
347779	2174.455499	192.168.0.107	206.247.40.84	UDP	123	62944 → 8801 Len=81
347782	2174.517527	192.168.0.107	206.247.40.84	UDP	151	62944 → 8801 Len=109
347796	2175.149228	192.168.0.107	206.247.40.84	UDP	123	62946 → 8801 Len=81
347798	2175.231867	192.168.0.107	206.247.40.84	UDP	151	62946 → 8801 Len=109
347841	2178.033320	192.168.0.107	206.247.40.84	UDP	123	62942 → 8801 Len=81
347844	2178.115531	192.168.0.107	206.247.40.84	UDP	151	62942 → 8801 Len=109
347849	2178.205050	192.168.0.107	206.247.40.84	UDP	123	62944 → 8801 Len=81
347851	2178.270730	192.168.0.107	206.247.40.84	UDP	151	62944 → 8801 Len=109
347862	2178.898788	192.168.0.107	206.247.40.84	UDP	123	62946 → 8801 Len=81
347864	2178.976322	192.168.0.107	206.247.40.84	UDP	151	62946 → 8801 Len=109

Nota. Se puede establecer cuál es el tráfico generado en el audio y video de una videollamada con Zoom.

Adicionalmente, podemos capturar la trama cuando finaliza la sesión de Zoom como se puede ver en las Figuras 20 y 21.

Figura 20

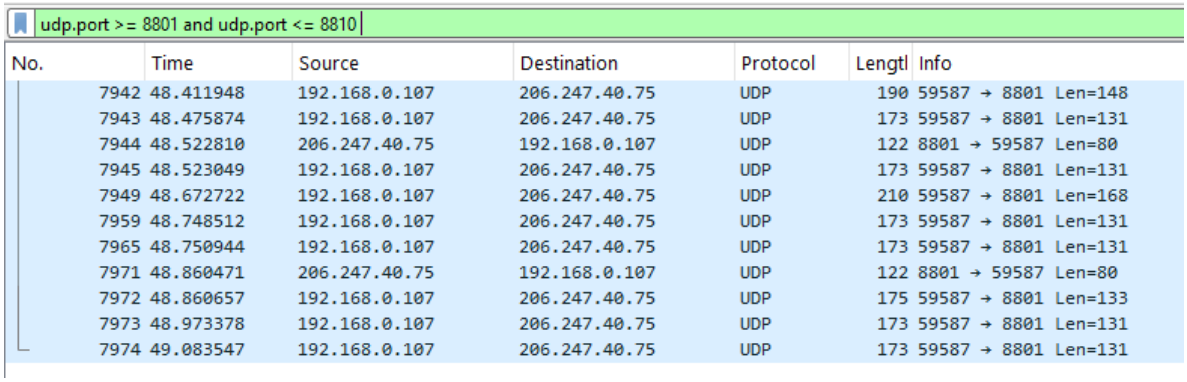
Finalización de video conferencia Zoom



Nota. En este caso se utiliza la versión gratuita, que permite solamente 40 minutos de reunión.

Figura 21

Tráfico de red generado al finalizar videoconferencia Zoom

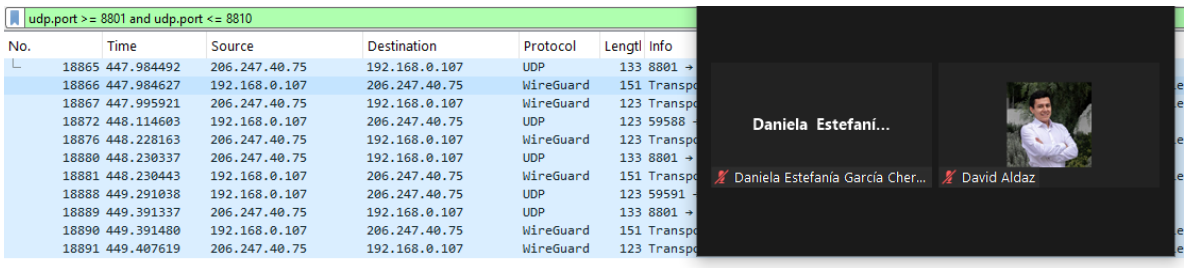


Nota. Con la herramienta Wireshark se puede obtener todo el tráfico que genera Zoom

En la Figura 22 se puede visualizar cuando no está activo el micrófono o la cámara no existe la afluencia de tráfico UDP

Figura 22

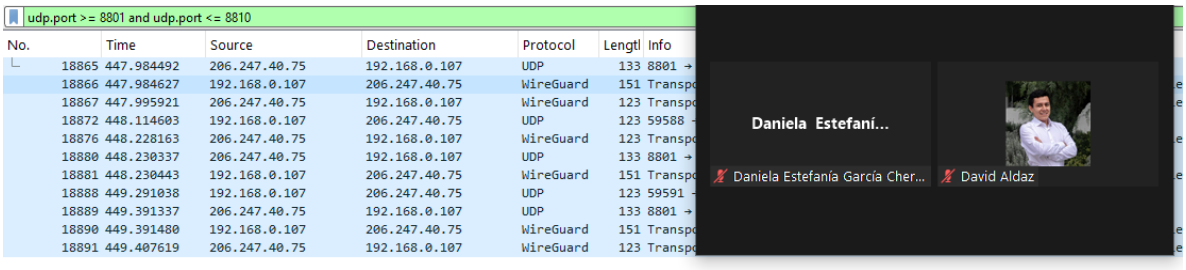
Tráfico de red generado sin micrófono o cámara



Nota. Se puede determinar la diferencia a nivel de tráfico de red cuando no se está usando el micrófono o cámara durante una videoconferencia Zoom.

Al momento de iniciar la cámara empieza a enviarse por la red, los paquetes UDP de video, así como de audio en el caso que se activó el micrófono y la cámara, como se puede ver en la Figura 23.

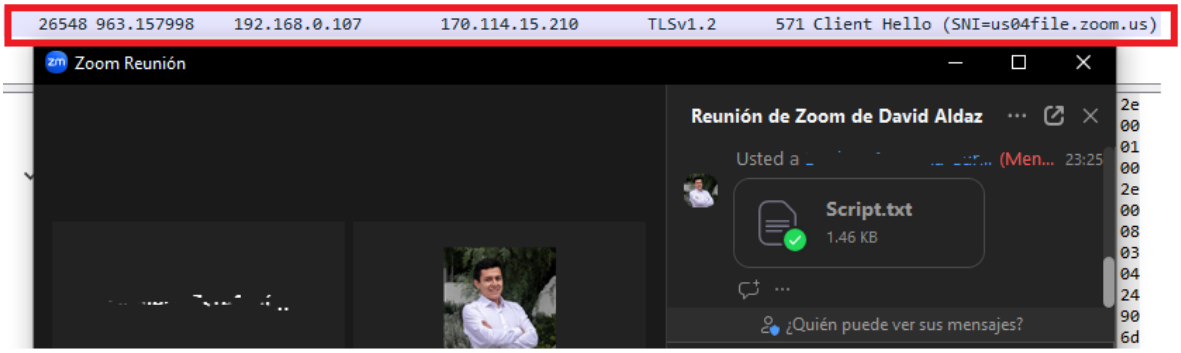
Figura 23
Tráfico de red generado con cámara activada



Nota. Se puede determinar cómo es el tráfico UDP con la cámara activada

Al enviar un archivo al chat, se logró capturar el paquete al cual se generó al momento de enviarlo. Como se puede ver en la Figura 24, se realiza una conexión hacia el servidor “us04file.zoom.us”

Figura 24
Tráfico de red generado al enviar un archivo en el chat



Nota. Se genera una conexión UDP cuando se envía un archivo utilizando el chat de la videoconferencia Zoom.

3.1.5. Uso de mecanismo para generar imágenes forenses de los discos

La clonación en este caso la vamos a realizar directo desde virtualbox utilizando los comandos propios de VirtualBox. Lo primero que hacemos es abrir una terminal CMD como administrador y

dirigirnos a la ruta donde está instalado VirtualBox, en nuestro caso con el comando “cd C:\Program Files\Oracle\VirtualBox”

Una vez en esta ruta ejecutamos el siguiente comando para cada uno de los sistemas operativos que queremos clonar

Comando clonado Windows: “VBoxManage.exe clonehd "C:\Users\Hector\VirtualBox VMs\TFM-W10\TFM-W10.vdi" "C:\Users\Hector\Desktop\w10.img" --format raw”

Comando clonado Ubuntu: “VBoxManage.exe clonehd "C:\Users\Hector\VirtualBox VMs\TFM-ubuntu\TFM-ubuntu.vdi" "C:\Users\Hector\Desktop\ubuntu.img" --format raw”

Comando clonado macOS: “VBoxManage.exe clonehd "C:\Users\Hector\VirtualBox VMs\TFM-MAC1\TFM-MAC1-disk001.vdi" "C:\Users\Hector\Desktop\mac.img" --format raw”. Posteriormente “VBoxManage.exe clonehd "C:\Users\Hector\VirtualBox VMs\Catalina\Catalina.vdi" "C:\Windows\Temp\mac-Tfm-Fin.img" --format raw”

3.1.6. Establecer un protocolo de recolección sin alterar los artefactos

Protocolo para la recolección de artefactos forenses:

Equipo físico:

a) Si el dispositivo se encuentra encendido:

- Aislar el equipo de las redes y conexiones entrantes/salientes, es decir se desconectará el equipo de cualquier red cableada o Wifi a la que se encuentre conectada.
- Si el monitor está encendido registrar a través de la toma fotográfica la pantalla y documentar la información que se observa, hacer énfasis en el Sistema Operativo y la fecha y hora del mismo.
- Si el equipo se encuentra con protector de pantalla, desplazar el mouse ligeramente, sin teclear ningún botón.

- De encontrarse el dispositivo con la pantalla apagada, registrar con una fotografía encenderla, si se encuentra bloqueado, registrar la respectiva fotografía.
- Definir la adquisición de los artefactos a recopilar: memoria RAM, imagen forense o descarga de información.
- Identificar y registrar sus características más relevantes: marca, modelo, serie, estado, etc.
- Finalmente, embalar el equipo, restringiendo los puertos por donde se pueda insertar dispositivos de extracción de la información y su rotulación respectiva. (Ministerio de Seguridad de la Nación, 2023)

b) Si el dispositivo se encuentra apagado

- Se desconecta el equipo de la red eléctrica y extrayendo su batería de ser el caso.
- Documentar el equipo describiendo sus características: marca, modelo, número de serie, estado.
- Finalmente, embalar el equipo, restringiendo los puertos por donde se pueda insertar dispositivos de extracción de la información y su respectiva rotulación. (Ministerio de Seguridad de la Nación, 2023)

Evidencia digital:

a) Preparación:

- Obtener una autorización o mandato judicial (de ser necesario).
- Evaluar los artefactos a recolectar: discos, logs, RAM, etc.
- Preparar dispositivos de almacenamiento seguro.
- Validar el ambiente del dispositivo donde se va a trabajar:

- **Activo/Encendido**
- **Inactivo/Apagado**

b) Identificación y preservación:

- Registrar el estado de los dispositivos a través de las fotografías necesarias de los periféricos.
- Etiquetar los dispositivos.
- Aislar el dispositivo de las conexiones ya sea de alimentación eléctrica, así como de las conexiones de red.
- Documentar puertos periféricos conectados y conexiones físicas. (NIST, 2014).

c) Adquisición:

- Utilizar un bloqueador de escritura al momento de realizar la imagen forense, mediante una herramienta especializada para este tipo de procedimientos.
- Se generará la debida firma de HASH de la imagen recolectada.
- La imagen será almacenada en dispositivos externos físicos, de forma que no se altere la cadena de custodia.
- Registrar comandos, herramientas utilizadas en el proceso. (SWGDE, 2022).

d) Documentación:

- Se debe registrar en un formulario debidamente estructurado la siguiente información:
  - Fecha y hora de recolección
  - Responsable
  - Descripción del artefacto

- Método de extracción
- Herramientas usadas
- Hash generado

e) Cadena de custodia (para casos específicos):

- Se utiliza el formulario de cadena de custodia establecido por las entidades.
- Consignar las respectivas firmas de cada responsable que recibe y transfiere la evidencia.
- Entrega de dispositivos seguros de almacenamiento. (ACPO, 2012).

f) Formato de documentación

Tabla 2

Formato de documentación

Artefacto	Tipo	Fecha/Hora	Responsable	Método	Hash	Obs.

Nota. Se detallan los parámetros que deben estar presentes para la documentación

Almacenamiento de las imágenes generadas desde VirtualBox:

Para este caso en específico se utilizará, por cuestiones prácticas, una cuenta de MEGA la cual permite almacenar archivos en la nube, originalmente en una situación real, las imágenes se almacenarían en discos físicos seguros.

3.1.7. **Validar la integridad de los artefactos mediante hashes (MD5/SHA1).**

Se comprueba la integridad de los artefactos generados, mediante la comprobación de las claves SHA 256 que fueron generadas en el caso anterior. Para ello se utiliza la herramienta HashMyFiles.

CAPÍTULO 4

4. ANÁLISIS DE RESULTADOS

4.1. Análisis de imágenes con herramientas como Autopsy y FTK

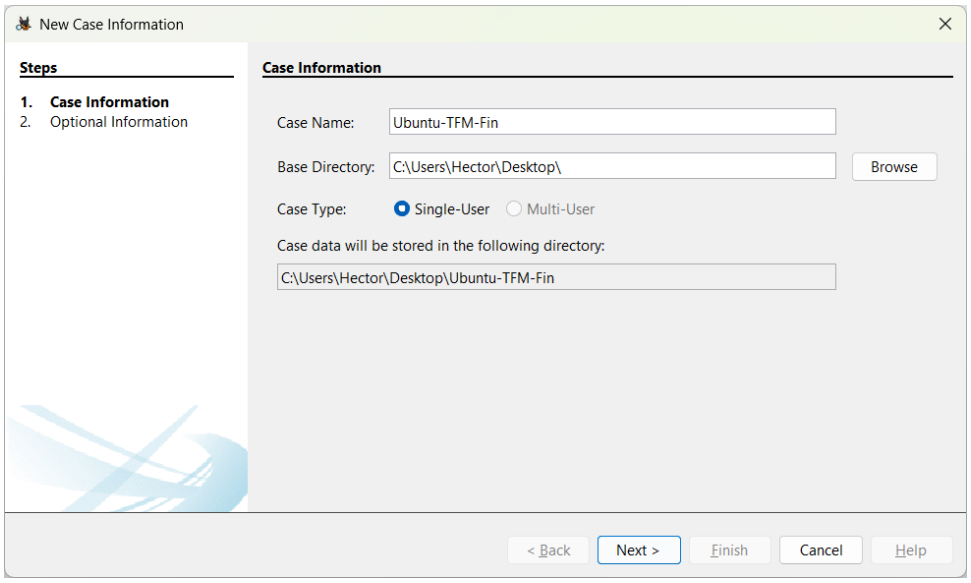
Con base en las imágenes creadas en los puntos anteriores, se utilizó Autopsy y FTK para poder abrirlas y de esta forma poder analizar su contenido en busca de información relevante de Zoom.

En Autopsy dependiendo de cómo configuremos cada caso va a tomar un tiempo considerable su análisis, en FTK el tiempo que toma para cargar una imagen es mucho menor, pero no nos brinda información relevante como lo hace Autopsy, por este motivo nuestra recomendación si tenemos tiempo para realizar el análisis forense es utilizar Autopsy, si el tiempo es corto la mejor opción será FTK.

4.1.1. Proceso para montar la imagen en Autopsy

Creamos un nuevo caso y colocamos su nombre como se puede observar en la Figura 25

Figura 25
Creación de un nuevo caso en Autopsy

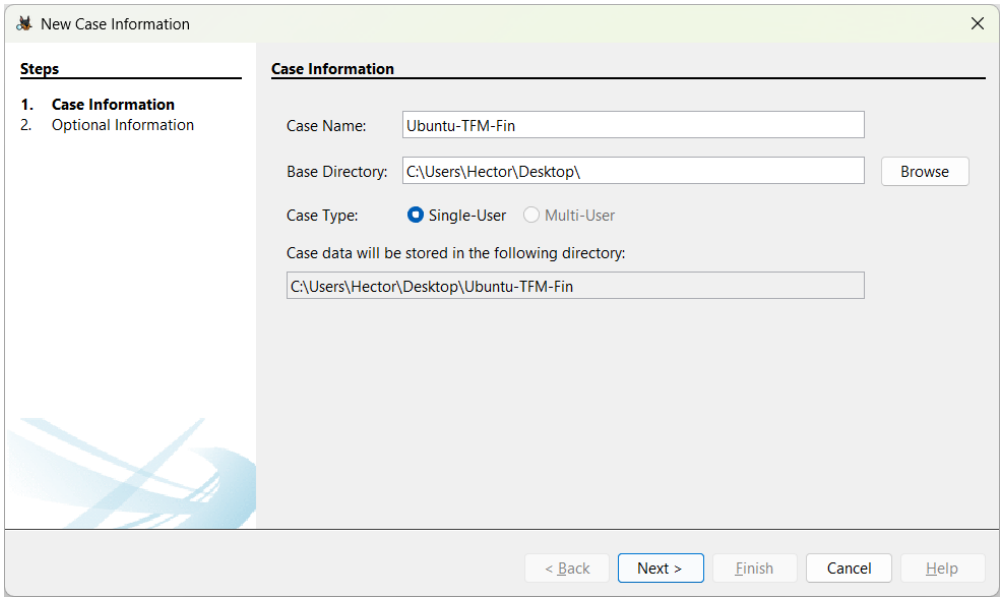


Nota. Se crea un nuevo caso utilizando la herramienta forense “Autopsy”

Colocamos información adicional al caso como se indica en la Figura 26

Figura 26

Ingreso de información adicional al caso en "Autopsy"

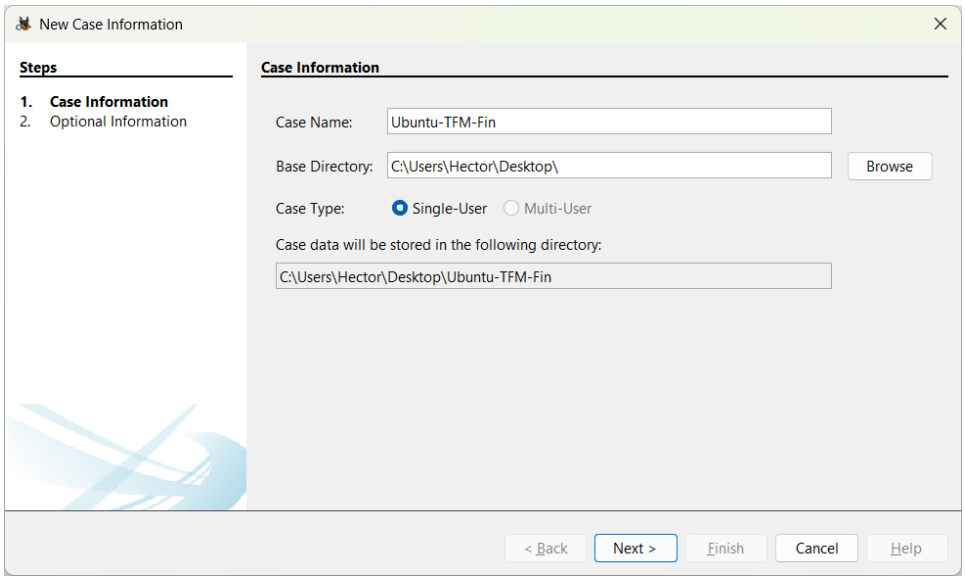


Nota. Se agrega más información al caso en Autopsy

Agregamos el origen de datos, para esto seleccionamos la primera opción como vemos en la Figura 27

Figura 27

Primer paso para agregar el origen de datos en Autopsy

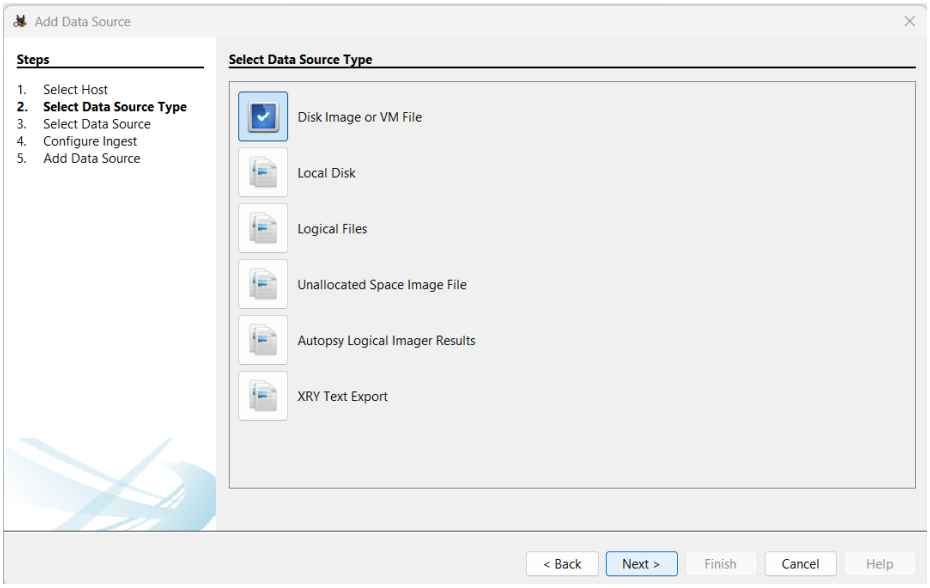


Nota. Se selecciona el host

Seleccionamos el tipo de origen de datos que vamos a utilizar, en nuestro caso imagen de Disco como se puede observar en la Figura 28

Figura 28

Segundo paso para agregar el origen de datos en Autopsy

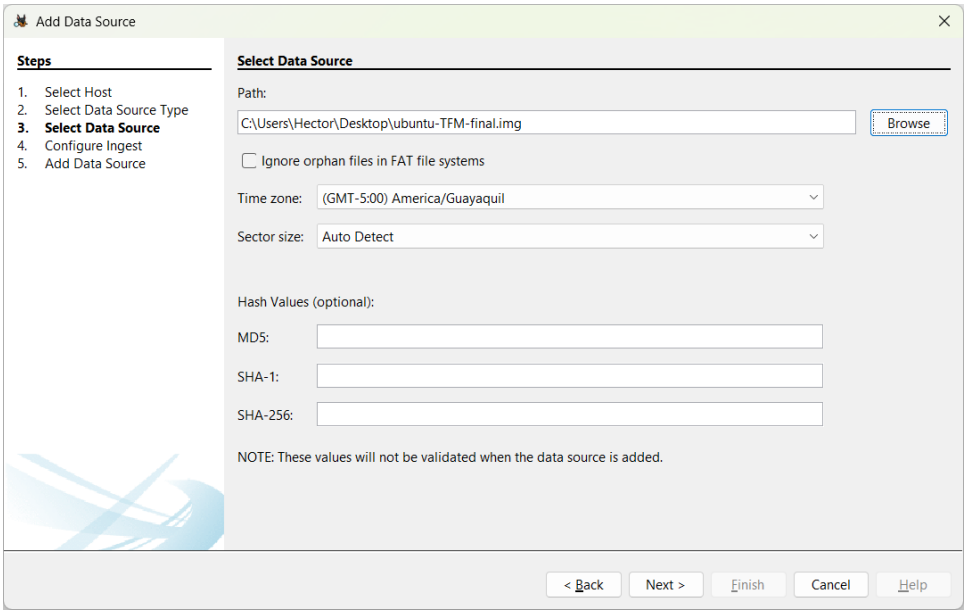


Nota. Se selecciona el tipo de origen

Escogemos la ruta donde se encuentra la imagen del disco que generamos en puntos anteriores como se muestra en la Figura 29

Figura 29

Tercer paso para agregar el origen de datos en Autopsy

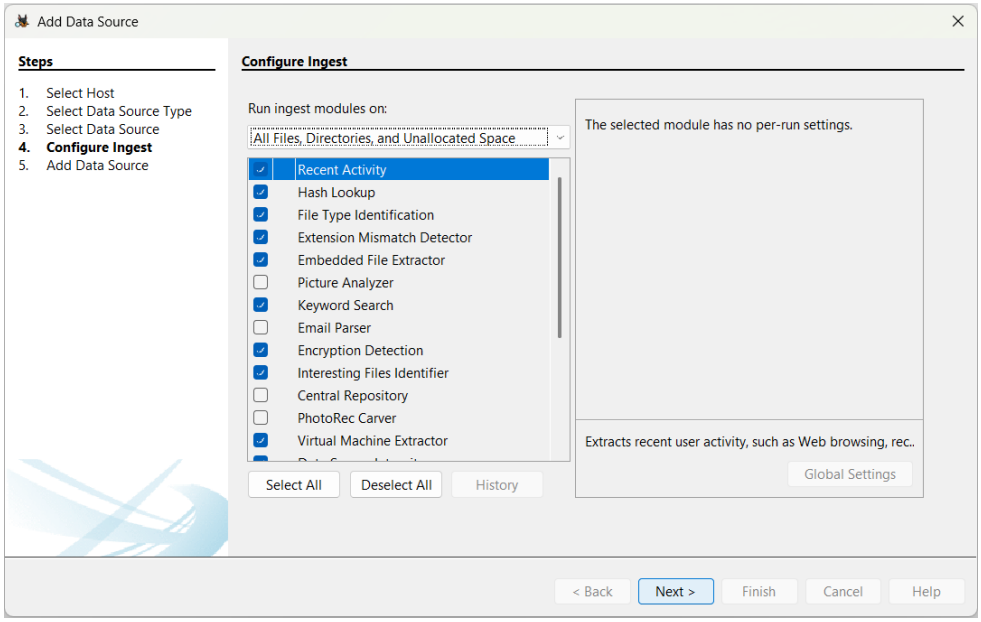


Nota. Se selecciona la imagen del Disco

Configuramos los módulos de ingesta que vamos a necesitar como podemos observar en la figura 30.

Figura 30

Cuarto paso para agregar el origen de datos en Autopsy

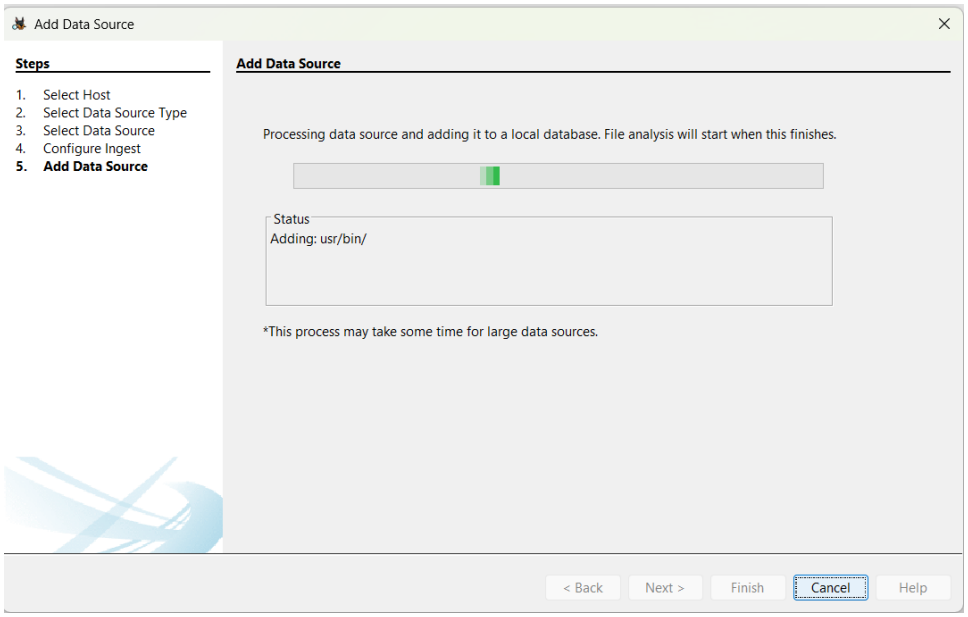


Nota. Se seleccionan los módulos de ingesta

En la Figura 31 se puede observar cómo procesa los datos del origen que seleccionamos

Figura 31

Quinto paso para agregar el origen de datos en Autopsy

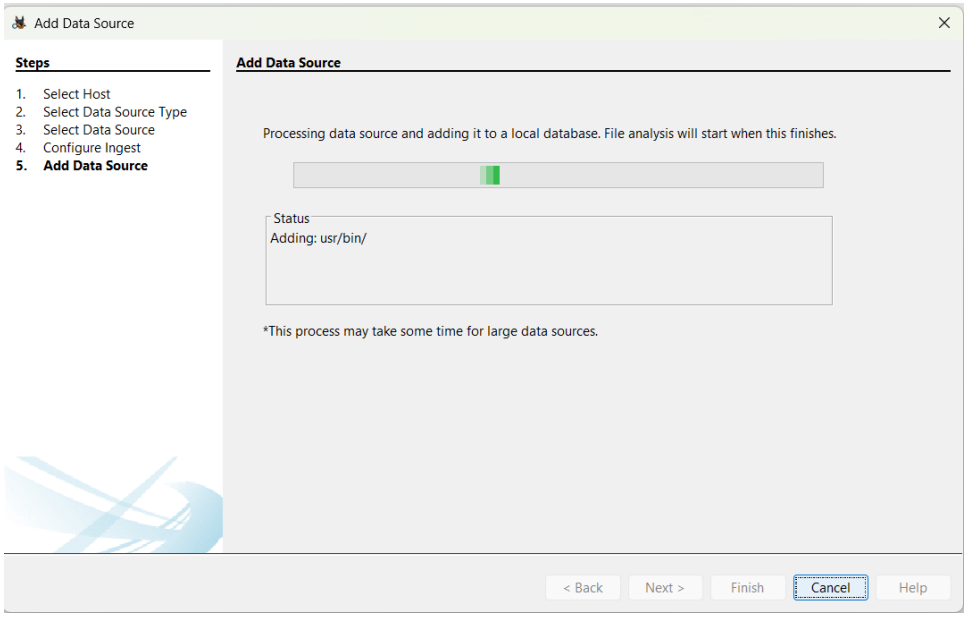


Nota. Autopsy realiza el proceso de importación de los datos.

Terminamos el proceso como se muestra en la Figura 32

Figura 32

Quinto paso para agregar el origen de datos en Autopsy

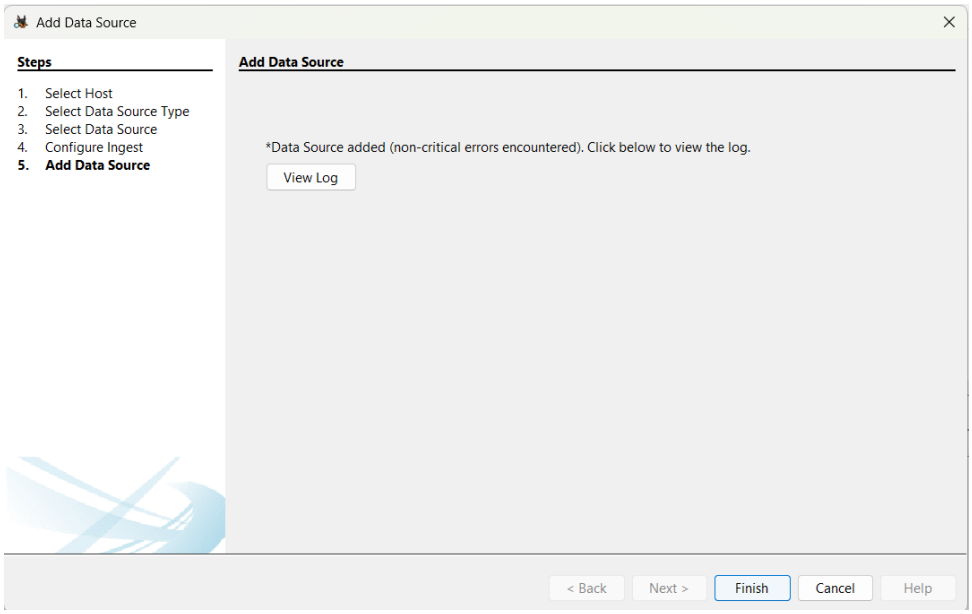


Nota. Autopsy realiza el proceso de importación de los datos.

Terminamos el proceso como se muestra en la Figura 33

Figura 33

Finalización del proceso de cargar origen de datos en Autopsy



Nota. Los datos se han agregado correctamente al programa Autopsy.

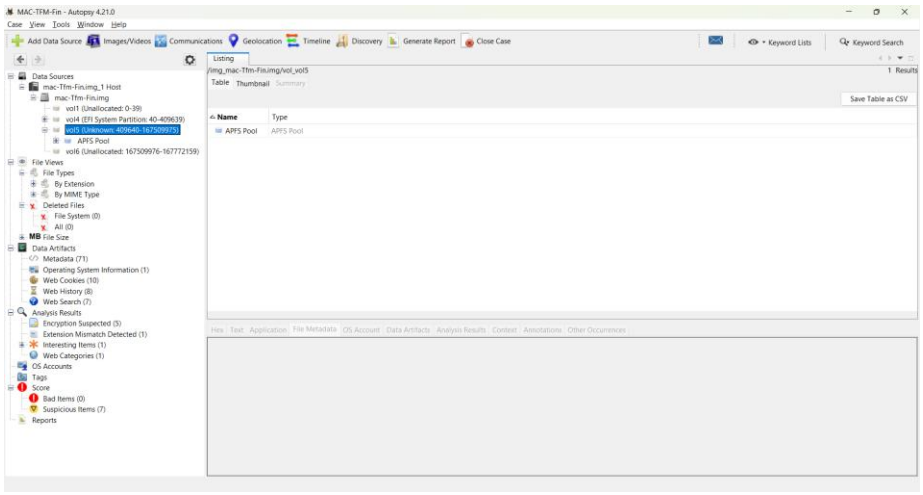
4.1.2. **Análisis de imagen en Autopsy**

macOS Catalina:

En la Figura 34, vamos a poder observar la Imagen de MAC analizada con autopsy.

Figura 34

Caso de Autopsy con la imagen de Disco de macOS Catalina



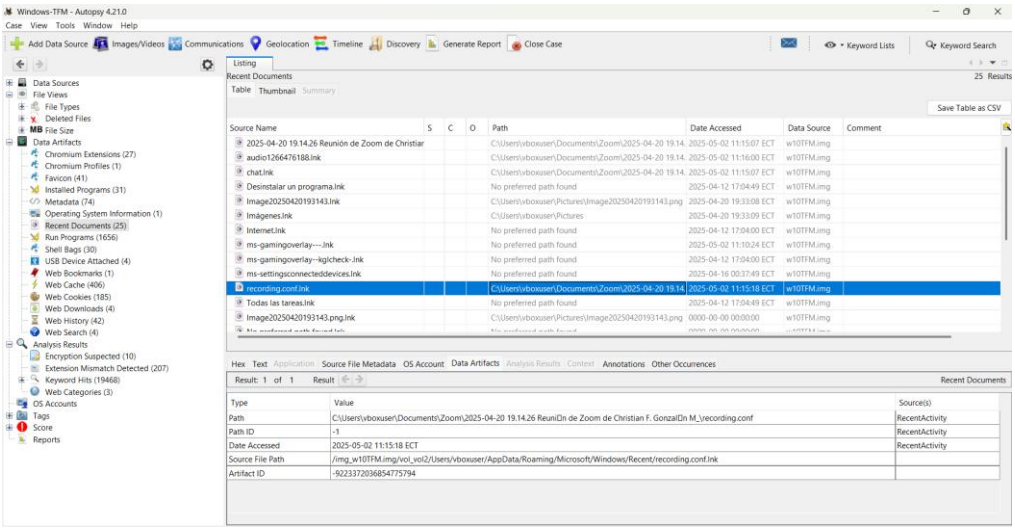
Nota. Pantalla que muestra los datos de la imagen de macOS Catalina obtenidos por Autopsy

Windows:

En la Figura 35, vamos a poder observar la Imagen de Windows analizada con Autopsy

Figura 35

Caso de Autopsy con la imagen de Disco de Windows



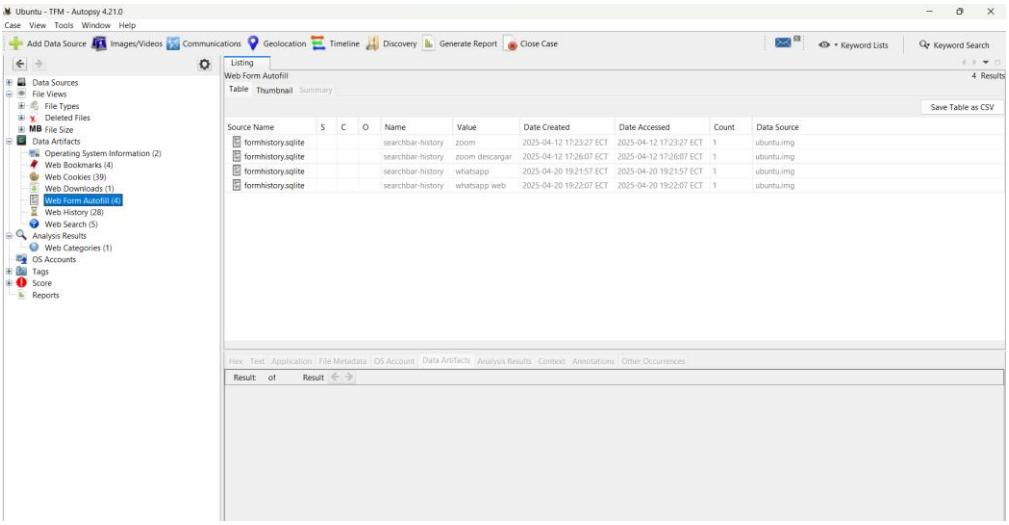
Nota. Pantalla que muestra los datos de la imagen de Windows obtenidos por Autopsy

Linux Ubuntu:

En la Figura 36, vamos a poder observar la Imagen de Ubuntu analizada con Autopsy.

Figura 36

Caso de Autopsy con la imagen de Disco de Linux Ubuntu

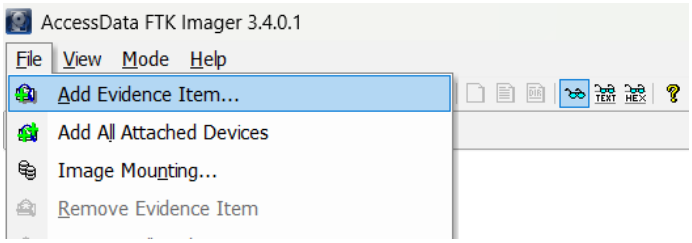


Nota. Pantalla que muestra los datos de la imagen de Linux Ubuntu obtenidos por Autopsy

El proceso para montar la imagen en FTK es el mismo en los tres sistemas operativos (Windows, macOS Catalina y Linux Ubuntu), para ello realizamos los siguientes pasos:

Ejecutamos el programa, vamos a File y escogemos Add Evidence Item como se observa en la Figura 37

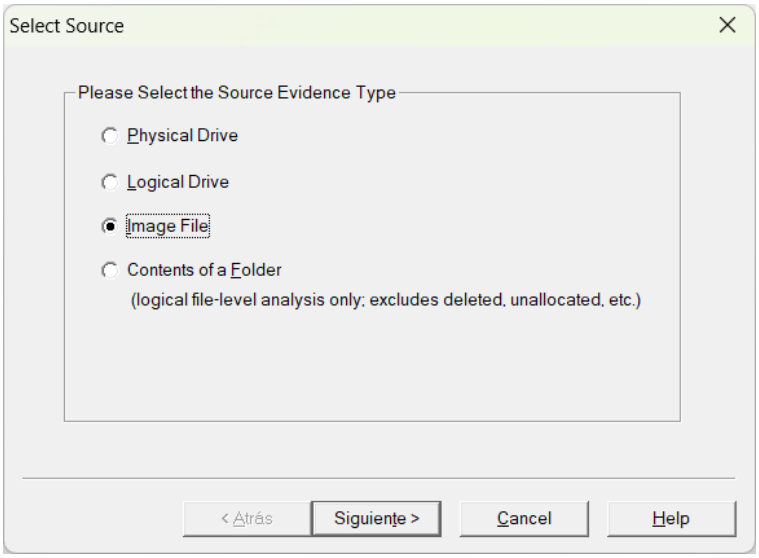
Figura 37
Proceso para montar imagen en FTK



Nota. Muestra la opción para agregar evidencia

Seleccionamos el tipo de origen que vamos a cargar, para nuestro caso será: Image File como vemos en la Figura 38

Figura 38
Opción para seleccionar el tipo de evidencia en FTK

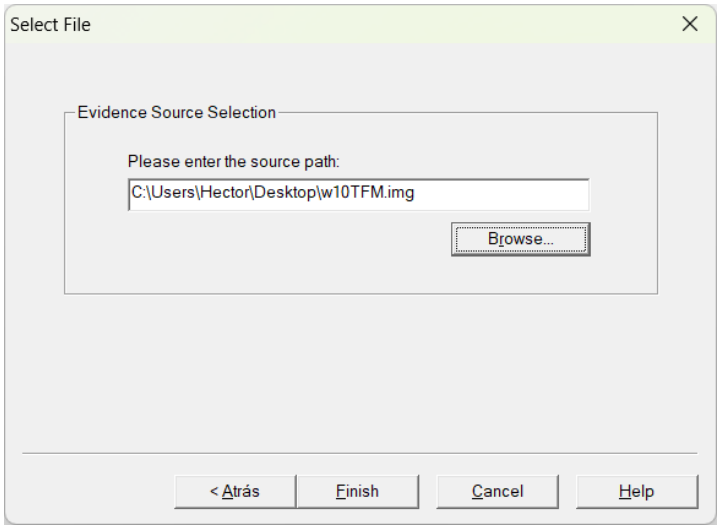


Nota. Pantalla para seleccionar el tipo de origen de evidencia

Seleccionamos la imagen que necesitamos y colocamos finalizar, esto se observa en la Figura 39:

Figura 39

Directorio donde tenemos nuestra imagen de disco

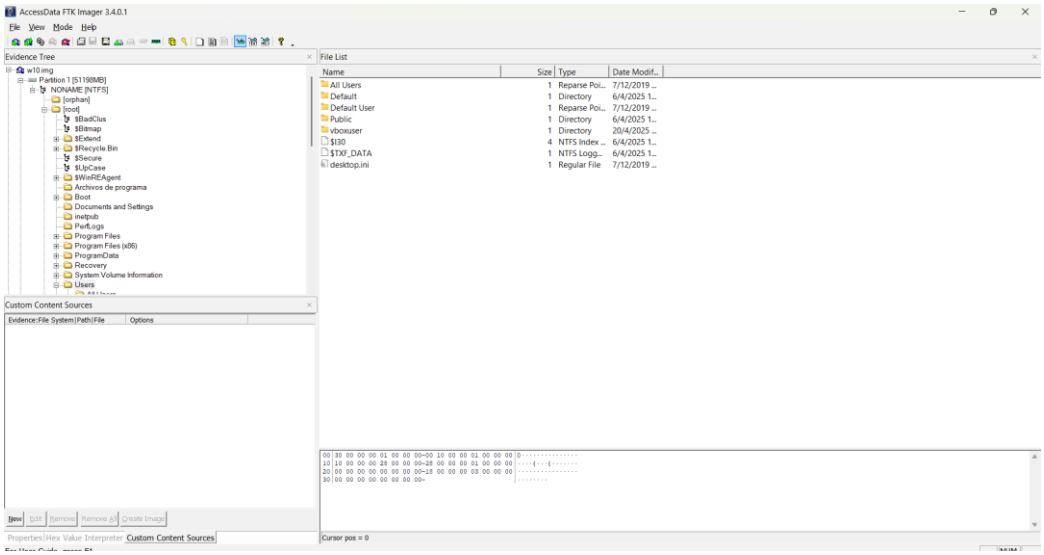


Nota. Pantalla para indicar el directorio de nuestra imagen a ser utilizada

Una vez montada la imagen del disco de la máquina virtual windows en FTK se presentará una pantalla similar a la que se muestra en la Figura 40, esto nos permitirá explorar en los diferentes directorios del sistema operativo.

Figura 40

Pantalla inicial imagen Windows en FTK

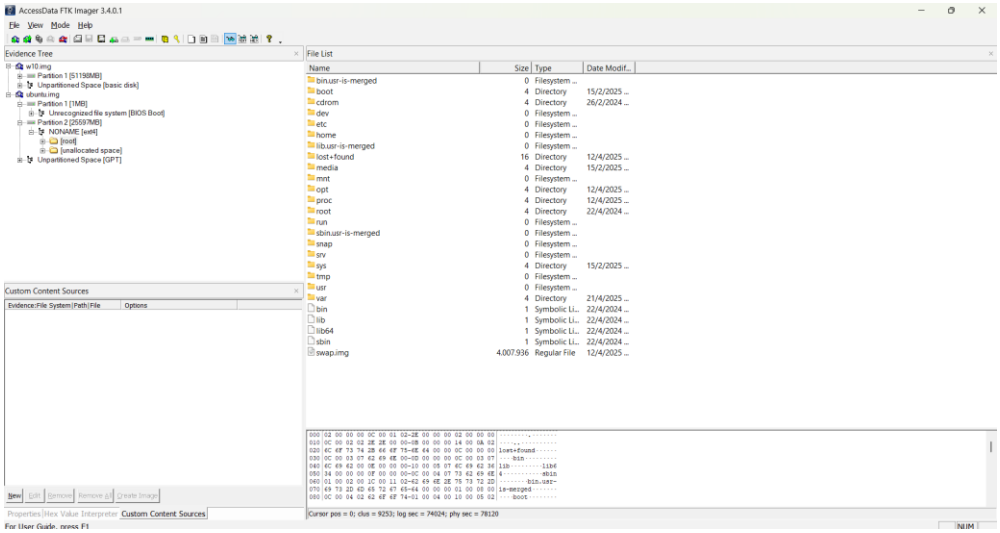


Nota. Imagen Windows montada en FTK

Una vez montada la imagen del disco de la máquina virtual ubuntu en FTK se presentará una pantalla similar a la que se muestra en la Figura 41.

Figura 41

Pantalla inicial imagen Ubuntu en FTK



Nota. Imagen Ubuntu montada en FTK

Imagen de macOS Catalina montada en FTK. Para este caso, FTK no pudo reconocer los archivos, por lo que fue necesario realizar el análisis con Autopsy.

4.1.3. **Identificación de artefactos relevantes: logs, metadatos y archivos temporales**

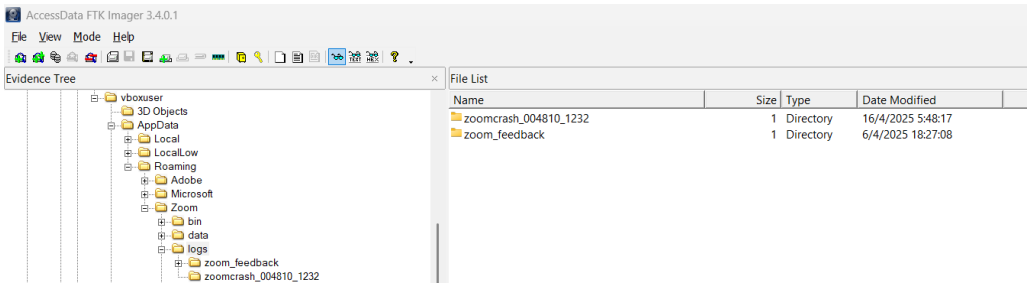
Zoom guarda registros (logs) en diferentes ubicaciones del sistema operativo que se está utilizando, las rutas que pudimos identificar son:

Logs de la aplicación Zoom en Windows:

Zoom almacena los logs en la ruta “C:\Users\[Usuario]\AppData\Roaming\Zoom\logs” que se puede observar en la Figura 42

Figura 42

Directorio de logs Zoom en Windows



Nota. Pantalla que muestra los logs de Zoom en un sistema Windows

En esta ruta se pudo identificar la siguiente información:

Se crea una carpeta de las sesiones que tuvieron algún inconveniente siguiendo el formato de nombre (zoomcrash_xxxxxx_xxxx) y existe una carpeta “zoom_feedback” que guarda información de forma cifrada y no se cuenta con una herramienta para validar el contenido de estos archivos ya que según se investigó son usados por Zoom de forma interna, los archivos cifrados tienen en su nombre la fecha en la que se realizó la reunión lo que nos puede ayudar a identificar una línea de tiempo.

La carpeta “zoomcrash_xxxxxx_xxxx” contiene por lo general dos archivos, uno en formato dmp y un xml. En esta carpeta se almacena información de errores generados por Zoom.

El documento XML contiene información que nos podría ser útil en un análisis forense, hay datos importantes relacionados con las capacidades y características del computador como por ejemplo el consumo de memoria, versión de sistema operativo, memoria disponible, fecha de inicio de la reunión, fecha de logueo en la reunión, la versión de Zoom, en ocasiones el ID de la reunión, entre otros datos como se observa en la Figura 43.

El archivo dmp es un dump de memoria que contiene información del error presentado.

Figura 43
Información del archivo crashrpt.xml

Nota. Pantalla que muestra el tipo de información que contiene el archivo crashrpt.xml

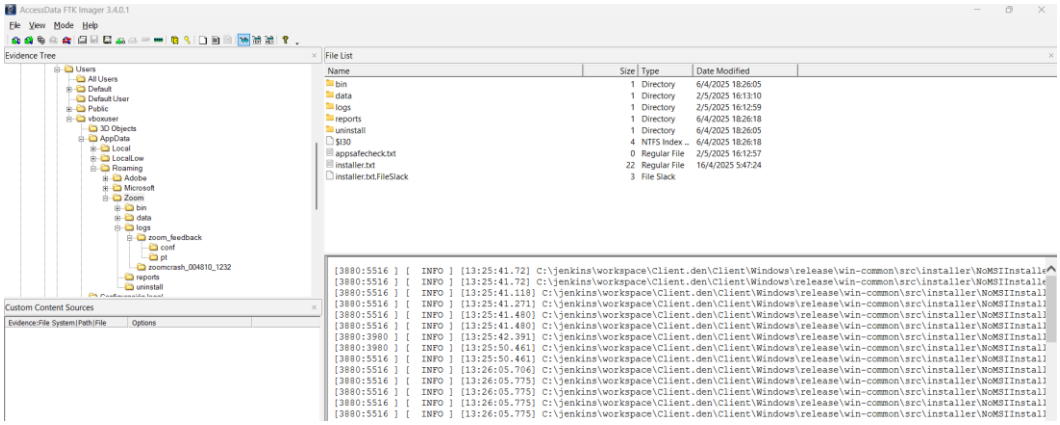
Dentro de la carpeta zoom_feedback existen dos carpetas adicionales conf y pt, estas carpetas contienen información importante de las sesiones, pero se encuentran cifradas, según se investigó en la carpeta conf se almacena información sobre la configuración del usuario y el estado de la aplicación, en la carpeta pt se almacena información detallada sobre actividades de la aplicación como eventos del usuario, errores y otros eventos importantes.

Logs de instalación de Zoom en Windows:

En la ruta “C:\Users\[Usuario]\AppData\Roaming\Zoom\installer.txt” como se aprecia en la Figura 44 encontramos el archivo installer.txt que es el que contiene información detallada del proceso de instalación, actualizaciones y desinstalación.

Figura 44

Ruta de logs de instalación de Zoom en Windows



Nota. Pantalla que muestra los logs de instalación de Zoom en un sistema Windows

El archivo contiene información importante como la fecha y hora de instalación de la aplicación Zoom (6 de abril de 2025 desde las 13:25:41 hasta las 13:26:14), el directorio donde se instaló (C:\Users\[Usuario]\AppData\Roaming\Zoom\), la hora de inicio de la instalación, la versión de Zoom (6.4.3.63669), el usuario con el que se instaló (vboxuser), etc., como se muestra en la Figura 45.

Figura 45

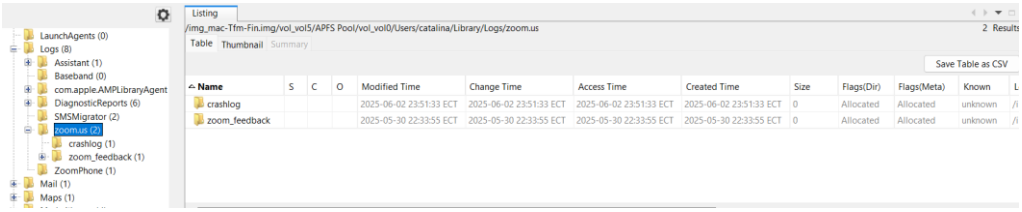
Archivo installer.txt de Zoom

Nota. Pantalla que muestra la información que contiene el log de instalación de Zoom.

Logs de la aplicación Zoom en macOS Catalina:

Zoom almacena los logs en la ruta “/Users/[Usuario]/Library/Logs/Zoom.us/” que se puede observar en la Figura 46

Figura 46
Ruta de logs en MAC

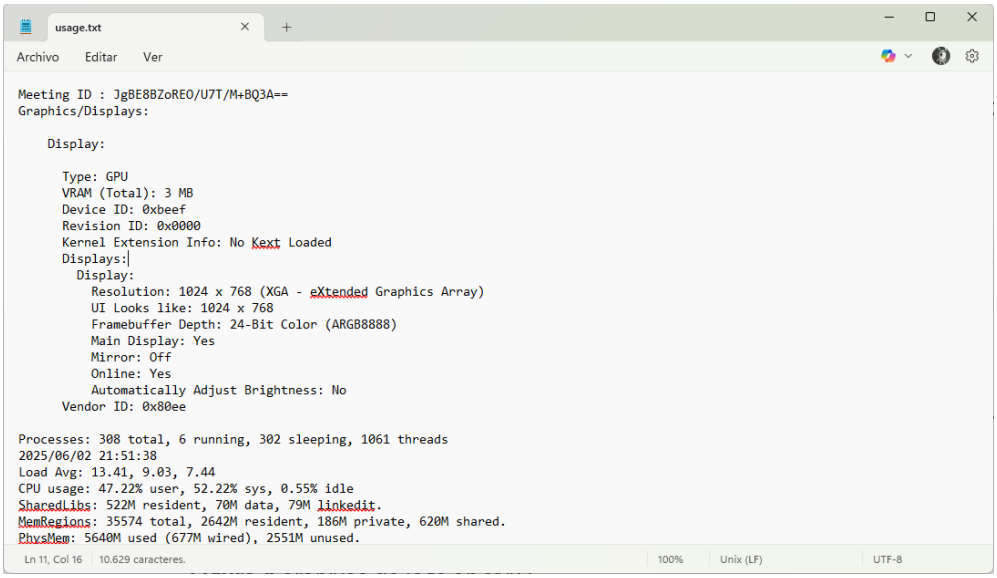


Nota. Pantalla que muestra los logs de Zoom en un sistema macOS Catalina

En este directorio se encuentran varios directorios y archivos de Zoom, pero en su mayoría cifrados, lo que no nos permite analizarlos y usarlos para vincularlos con otras evidencias.

En la carpeta crashlog se encuentra el archivo “usage.txt” que, si contiene información importante, ya que registra información detallada sobre errores que ocurren en Zoom, dentro de la información almacenada se encuentra el ID de la reunión e información relacionada con el consumo de recursos como se observa en la Figura 47.

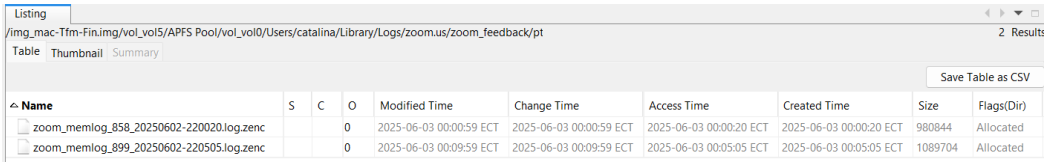
Figura 47
Archivos “usage.txt” de macOS Catalina



Nota. Pantalla que muestra los datos que contiene el archivo usage.txt

En la carpeta zoom_feedback se encontró archivos cifrados de los cuales solo podríamos tomar fechas de creación y modificación, pero no ver su contenido como se aprecia en la Figura 48.

Figura 48
Archivos de logs en MAC



Nota. Pantalla que muestra los archivos almacenados dentro de las carpetas de logs

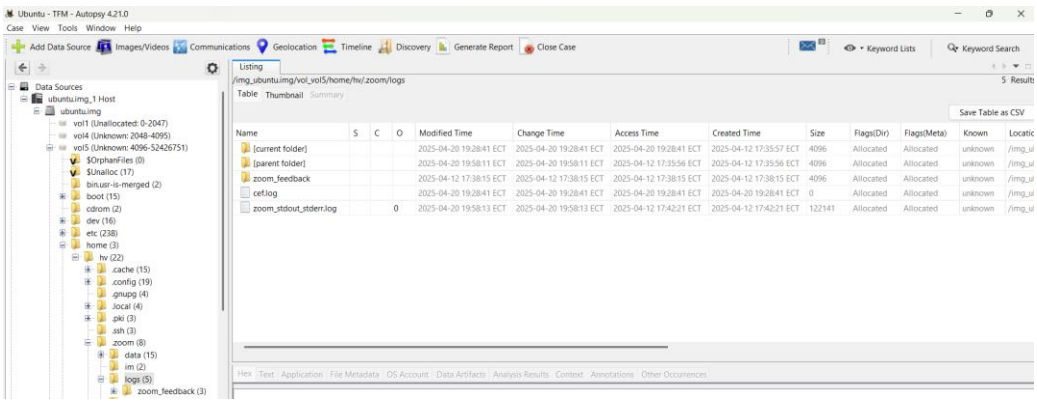
Logs de la aplicación Zoom en Linux Ubuntu:

Zoom almacena los logs en la ruta "/home/[Usuario]/.zoom/logs". Revisando la información que se encuentra en este directorio, cuya estructura se observa en la figura 49, se pudo identificar que en la carpeta zoom_feedback existe otra carpeta llamada pt la cual solamente contiene archivo de Zoom cifrados, de los cuales no es posible validar sus datos.

Existe otro archivo llamado zoom_stdout_stderr.log el cual contiene información sobre el inicio, configuración y ejecución de Zoom, información sobre configuraciones como el entorno gráfico, librerías, procesos relacionados y funcionalidades de la aplicación, también errores del sistema.

El archivo cef.log se encuentra vacío.

Figura 49
Ruta de logs en Ubuntu



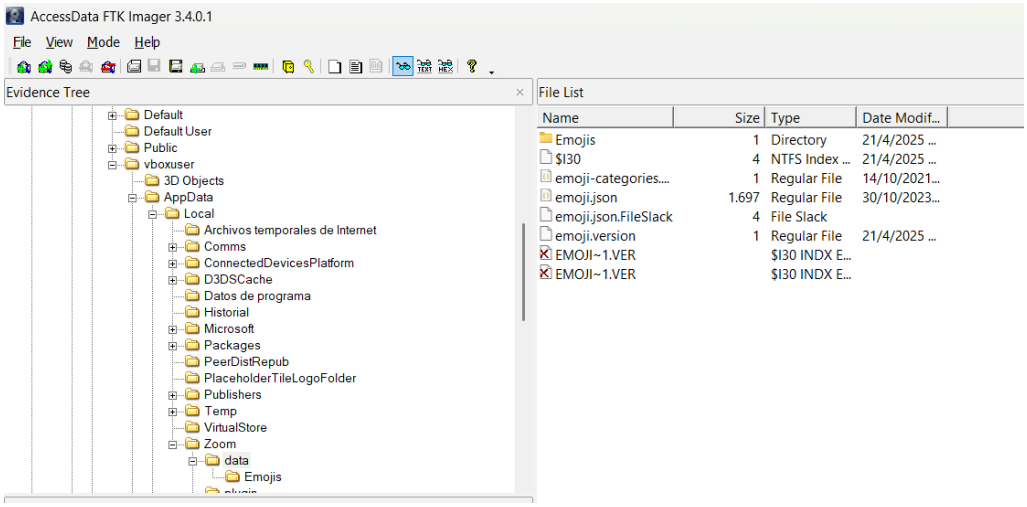
Nota. Pantalla que muestra los logs de Zoom en un sistema Ubuntu

Zoom guarda los archivos temporales en diferentes ubicaciones del sistema operativo y va a depender mucho de la versión de este. Las rutas identificadas para estos archivos temporales son:

Archivos temporales de Windows:

Los archivos temporales en Windows se guardan en la ruta "C:\Users\[Usuario]\AppData\Local\Zoom\" como se puede ver en la Figura 50.

Figura 50
Ruta de archivos temporales de Zoom en Windows



Nota. Pantalla que muestra los archivos temporales en Windows

En esta ruta no se encontró información relevante para nuestro análisis, de lo validado contiene emojis que utiliza la aplicación.

Archivos temporales de grabaciones en Windows

La ruta en la cual se almacenan los archivos temporales de las grabaciones en Windows es "C:\Users\[Usuario]\Documents\Zoom\"

En esta ruta, como se observa en la Figura 51, si se pudo identificar información relevante para nuestro análisis, ya que si la reunión fue grabada vamos a encontrar la grabación, el audio, la información que se colocó en el chat de la reunión, entre otros. Zoom va a crear un directorio para cada reunión que se grabe.

El archivo de audio es almacenado en formato m4a y el de video en formato mp4, en ambos casos dentro de su nombre tienen el ID de la sesión de Zoom, para nuestro caso de estudio “266476188”, como sugerencia en un análisis forense podemos realizar una búsqueda de este tipo de archivos en todo el equipo ya que los archivos pueden haber sido movidos a directorios diferentes a los que utiliza Zoom por defecto.

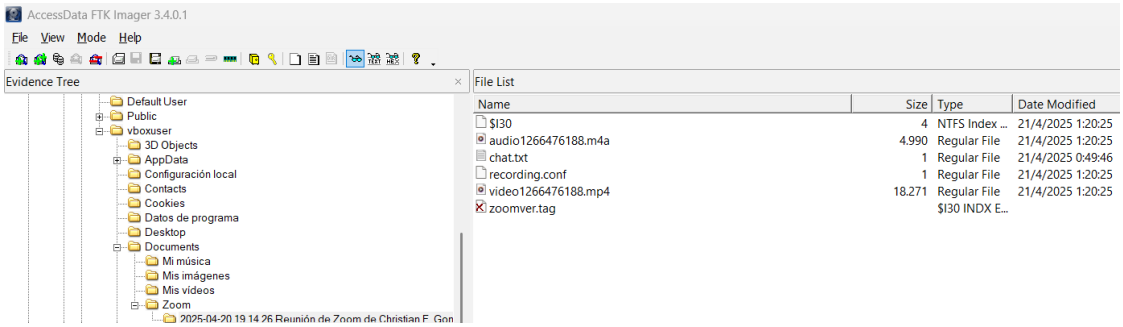
A través de las grabaciones podríamos identificar la fecha de la reunión, su duración y es muy probable que podamos ver los participantes de la misma, así como también la información que compartieron.

El archivo recording.conf contiene los nombres del archivo de audio, de video y el ID que va a colocar como parte del nombre de los archivos, esta información es super valiosa, ya que conoceríamos los nombres de los archivos generados y podríamos buscarlos en todo el PC o dispositivo.

En el archivo chat.txt se encuentra el detalle de la hora en el que los participantes interactuaron y quienes fueron.

Figura 51

Ruta de archivos temporales de grabaciones de Zoom en Windows



Nota. Pantalla que muestra los archivos temporales de grabaciones en Windows

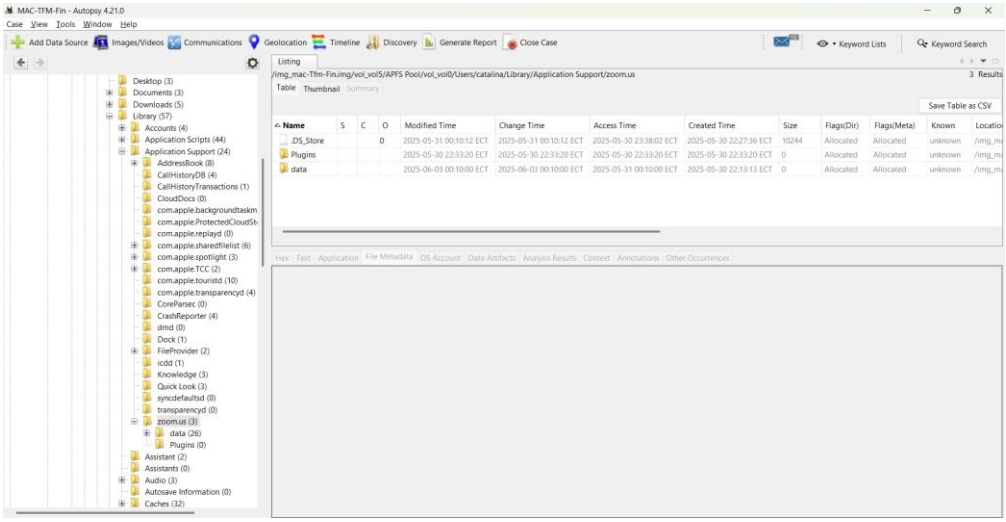
Archivos temporales de Zoom en macOS Catalina:

En el directorio “/Users/[Usuario]/Library/Application Support/Zoom.us/” hay varios subdirectorios, como se observa en la Figura 52, pero en ninguno se encontró información relevante, en su mayoría son archivos que se encuentran cifrados y cuya data no es legible.

Se identificó una carpeta llamada “confres” que contiene información de las capturas o imágenes colocadas en el chat de la reunión, que si pudiese ser información relevante en un análisis forense como se ve en la Figura 53.

Figura 52

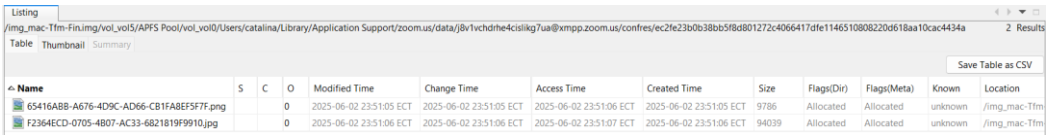
Ruta de archivos temporales de Zoom en macOS Catalina



Nota. Pantalla que muestra los archivos temporales en macOS Catalina

Figura 53

Archivos dentro de la carpeta confres



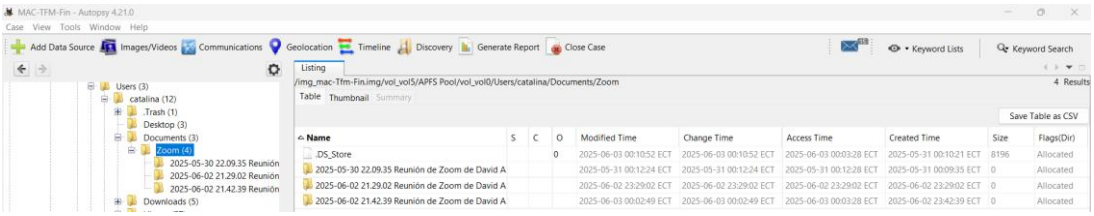
Nota. Pantalla que muestra los archivos dentro de las subcarpetas de la carpeta “confres”

Archivos temporales de grabaciones en macOS Catalina:

Si la reunión fue grabada en esta ruta “/Users/[Usuario]/Documents/Zoom/”se crea una carpeta por cada reunión en la cual se almacena el audio, video, chat de la reunión y el archivo de configuración el cual contiene un ID específico que identifica a los archivos de audio y video generados en esa reunión como se puede ver en las Figuras 54 y 55.

Figura 54

Ruta de archivos temporales de grabaciones de Zoom en MAC



Nota. Pantalla que muestra los archivos temporales de grabaciones en MAC

Figura 55

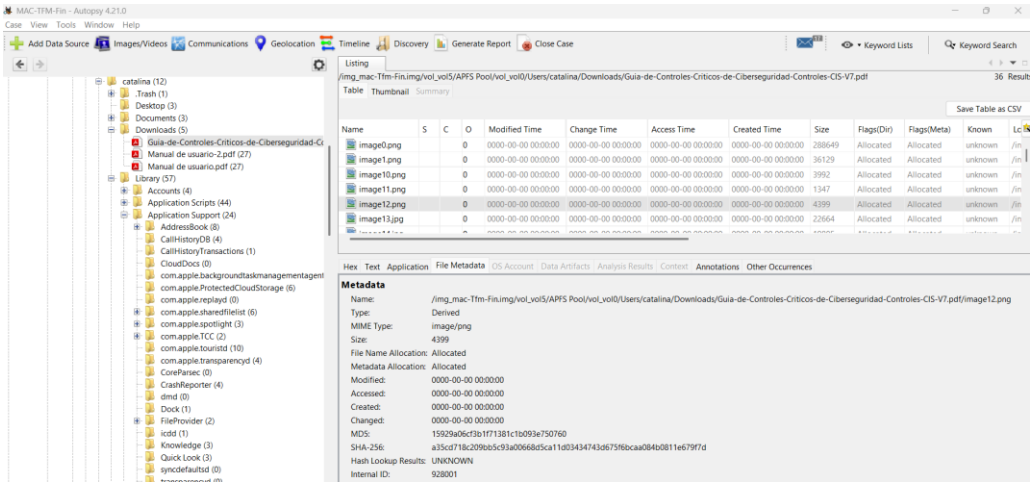
Contenido del archivo recording.conf

Nota. Pantalla que muestra el contenido del archivo recording.conf

Los archivos compartidos durante las reuniones no se encuentran en ninguno de los directorios ya nombrados como se muestra en la Figura 56, estos datos se almacenan en la carpeta de descargas y a nivel de metadatos no hay ninguno que nos indique que son documentos que se compartieron en una reunión, la única evidencia es la grabación de la reunión.

Figura 56

Contenido de la carpeta Downloads



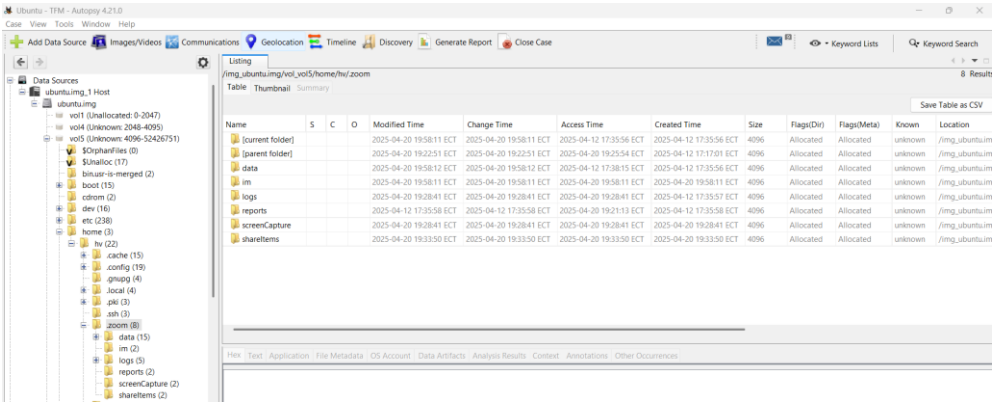
Nota. Pantalla que muestra el contenido de la carpeta Downloads

Archivos temporales de Zoom en Linux Ubuntu:

En el directorio "/home/[Usuario]/.zoom/" hay varios subdirectorios, en su mayoría son archivos que se encuentran cifrados y cuya data no es legible como se puede ver en la Figura 57.

Figura 57

Ruta de archivos temporales de Zoom en Ubuntu



Nota. Pantalla que muestra los archivos temporales en Ubuntu

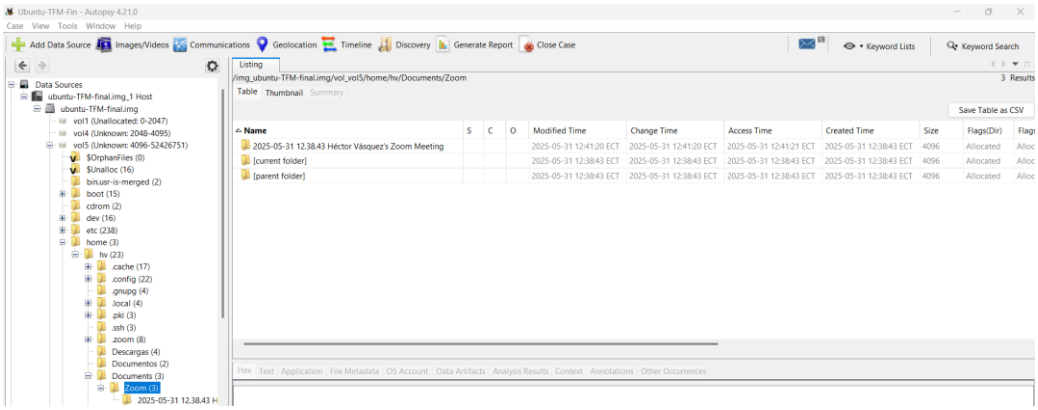
Uno de los subdirectorios llamado confres posee las imágenes que fueron compartidas en la reunión si esta fue grabada, esta información si pudiese ser relevante en un análisis forense

Archivos temporales de grabaciones en Zoom en Linux Ubuntu:

Si la reunión fue grabada en este directorio "/home/[Usuario]/Documents/Zoom/" se crea una carpeta por cada reunión en la cual se almacena el audio, video, chat de la reunión y el archivo de configuración el cual contiene el ID que forma parte de los nombres de los archivos de audio y video generados en esa reunión como se observa en la Figura 58.

Figura 58

Ruta de archivos temporales de grabaciones de Zoom en Ubuntu



Nota. Pantalla que muestra los archivos temporales de grabaciones en Ubuntu

Los metadatos de Zoom, que pueden incluir información sobre las reuniones, como detalles de los participantes, grabaciones, y otros datos relacionados, generalmente se almacenan en las siguientes ubicaciones, dependiendo del sistema operativo. Sin embargo, es importante destacar que los metadatos relacionados con la cuenta de Zoom y las reuniones (como los detalles de la reunión, el historial de chats, etc.) también pueden ser almacenados en los servidores de Zoom, especialmente si se tiene una cuenta registrada y en la nube.

Metadatos en Windows:

Metadatos locales de las reuniones y grabaciones:

- Ruta de los archivos de grabación: C:\Users\[Usuario]\Documents\Zoom\
- Los metadatos de las grabaciones locales suelen estar junto a los archivos de grabación, en un archivo de formato ".conf" que contiene información sobre la reunión, como el ID de la reunión, y el archivo de audio y video generados.

Metadatos de la aplicación:

- Se pueden guardar en los archivos de configuración de Zoom en: "C:\Users\[Usuario]\AppData\Roaming\Zoom\" y

"C:\Users\[Usuario]\AppData\Local\Zoom\."

- Directorio: C:\Users\[Usuario]\AppData\Roaming\Zoom\, en este directorio se identificó información relevante en el directorio \data\confres, en esta ruta se almacenan las capturas y gráficos enviados por el chat de las reuniones.
- Dentro del mismo directorio tenemos data\net_records, este archivo guarda información relevante para nuestro análisis, ya que contiene información de las solicitudes HTTP realizadas por la aplicación cuando se encuentra en funcionamiento. El archivo está en formato json el cual contiene detalles de las interacciones de Zoom con sus servidores, hay campos importantes como http_code para saber si fallo o fue exitoso, el campo url que es la url del servidor de Zoom contactado. Las marcas de tiempo que se muestran en este log pueden ser correlacionadas con el resto de los eventos de reuniones o sesiones específicas.
- Hay mucha más información dentro de este directorio per o se encuentra cifrada o no es relevante para un análisis forense.

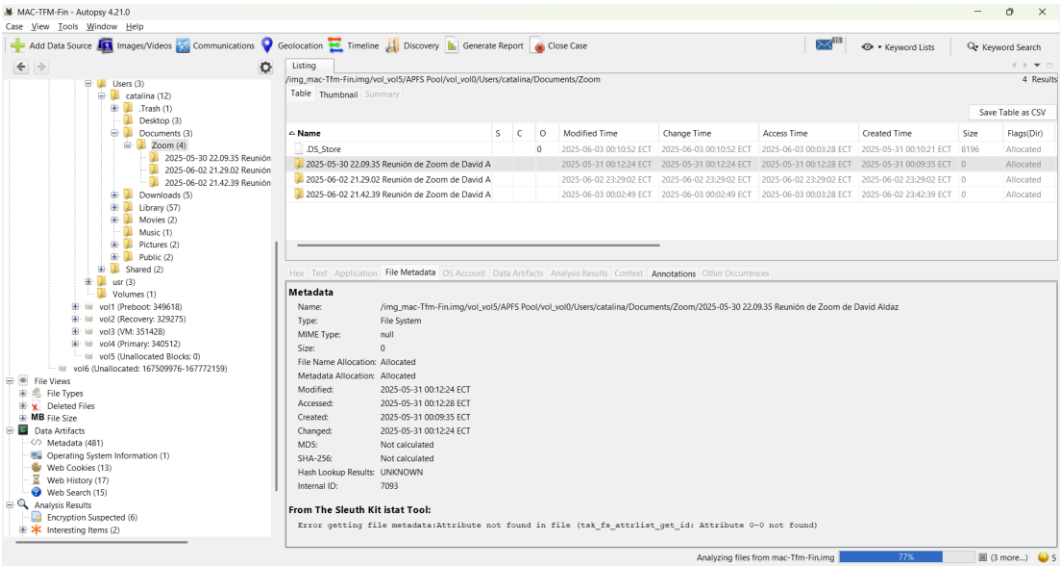
Metadatos en macOS Catalina:

Metadatos locales (de las reuniones y grabaciones)

La Ruta de los archivos de grabación "/Users/[Usuario]/Documents/Zoom/". Los archivos identificados en este directorio son los mismos que habíamos mencionado en un punto anterior, es decir, solamente encontramos los registros de chats, video y audio de la reunión. Por el path donde se encuentran podemos identificar que son registros de Zoom y, ya que los metadatos de los archivos no brindan información relevante, la única información importante son las fechas como se observa en la Figura 59.

Figura 59

Metadatos locales en macOS Catalina



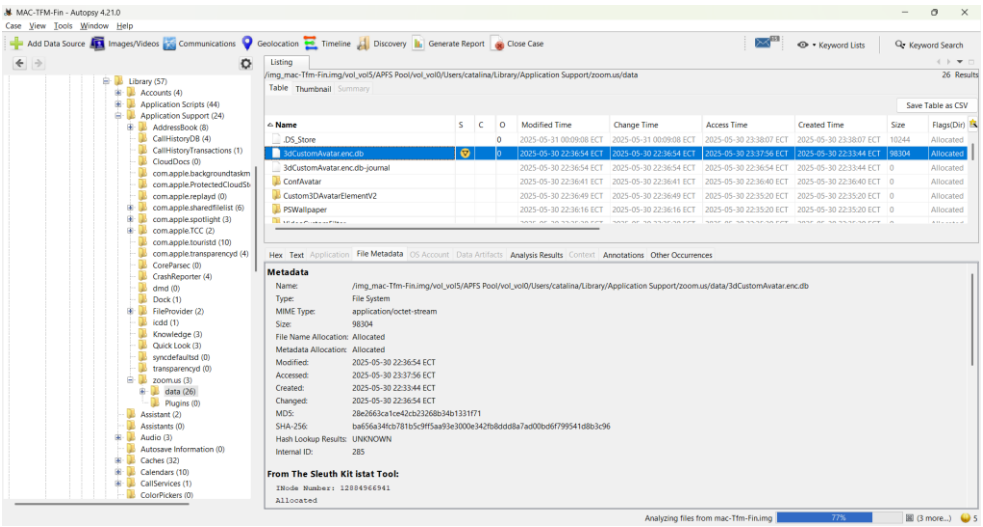
Nota. Pantalla que muestra el directorio de metadatos locales de MAC

Metadatos de la aplicación en macOS Catalina:

Se almacenan en "/Users/[Usuario]/Library/Application Support/Zoom.us/." La mayoría de la información que se encuentra en la ruta está cifrada, no se identificó información que pueda ser relevante. Se sabe que los archivos son de Zoom por la ruta donde se almacena, la metadata solo contiene como información importante fechas de creación, modificación, acceso, etc como se observa en la Figura 60.

Figura 60

Metadatos de aplicación en macOS Catalina



Nota. Pantalla que muestra el directorio de metadatos de la aplicación en macOS Catalina

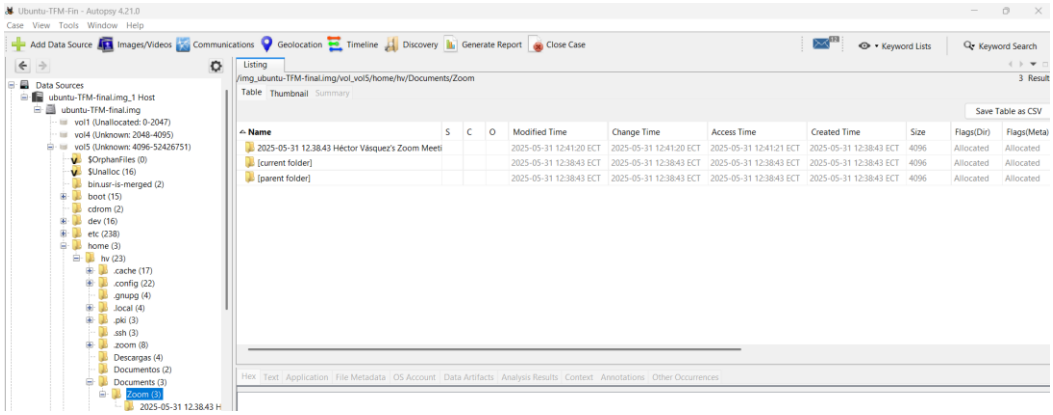
Metadatos en Linux Ubuntu

Metadatos locales

La ruta de los archivos de grabación se almacena en “/home/[Usuario]/Documents/Zoom/”

Los metadatos importantes de los archivos que se encuentran en estas rutas son las fechas de creación, modificación, etc. Como se puede ver en la Figura 61.

Figura 61
Directorio Documents/zoom

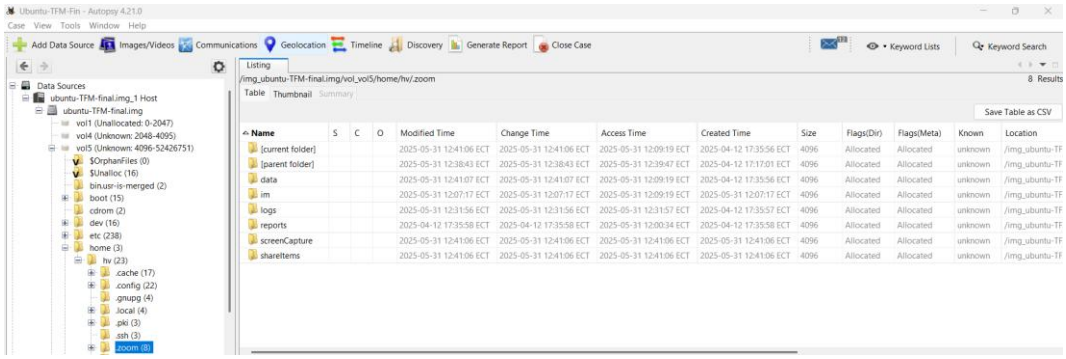


Nota. Pantalla que muestra los metadatos de los archivos de Zoom

Metadatos de aplicación:

Los metadatos de la aplicación se almacenan en la ruta “/home/[Usuario]/.zoom/”. Al igual que en el punto anterior, los puntos más relevantes son temas de fechas como se puede ver en la Figura 62.

Figura 62
Metadatos de Zoom en Linux Ubuntu



Nota. Pantalla que muestra los metadatos que almacena Zoom en Ubuntu

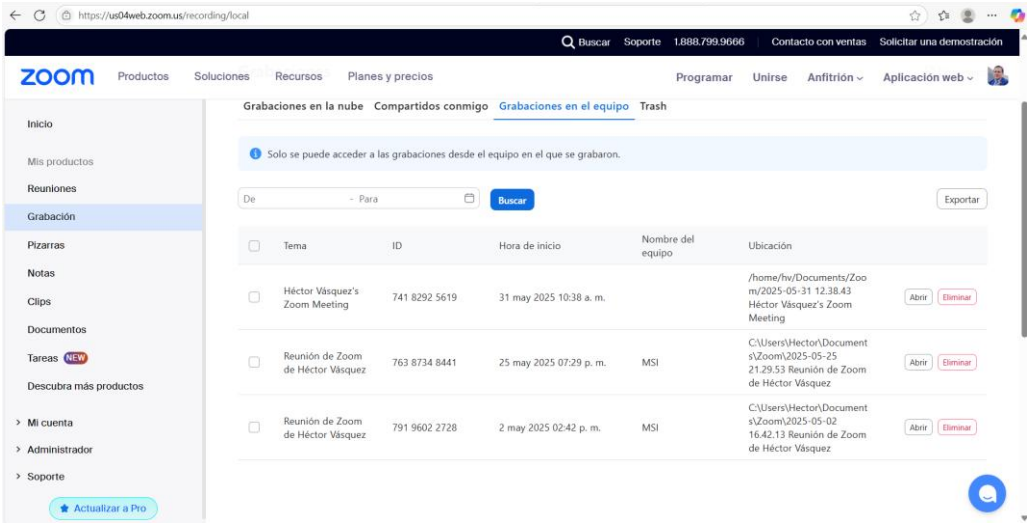
Metadatos en la nube de Zoom:

Si se utiliza Zoom en la nube con una cuenta registrada, muchos de los metadatos relacionados con las reuniones y grabaciones, como el historial de chat, detalles de los participantes y las grabaciones en la nube, se almacenan en los servidores de Zoom. Estos metadatos no son accesibles directamente desde el computador, pero se pueden ver accediendo a la cuenta de Zoom en la web (https://zoom.us), para validar datos en nube deberíamos tener acceso a las credenciales de Zoom como se puede ver en las Figuras 63, 64 y 65.

Los metadatos de la nube pueden incluir:

- Información sobre las reuniones programadas y pasadas.
- Detalles sobre los participantes y sus interacciones (como el tiempo de entrada y salida).
- Archivos de chat y grabaciones almacenadas en la nube.

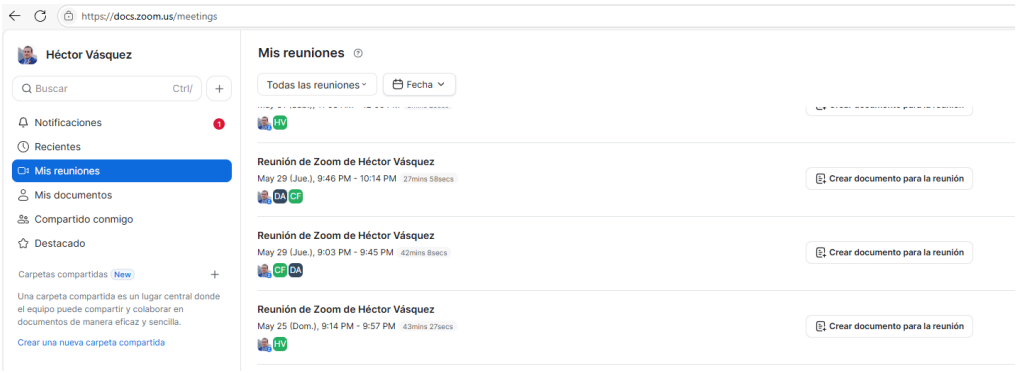
Figura 63
Grabaciones de reuniones vistas en la interfaz web del dueño de la cuenta



Nota. Pantalla que muestra las grabaciones realizadas y su ubicación

Figura 64

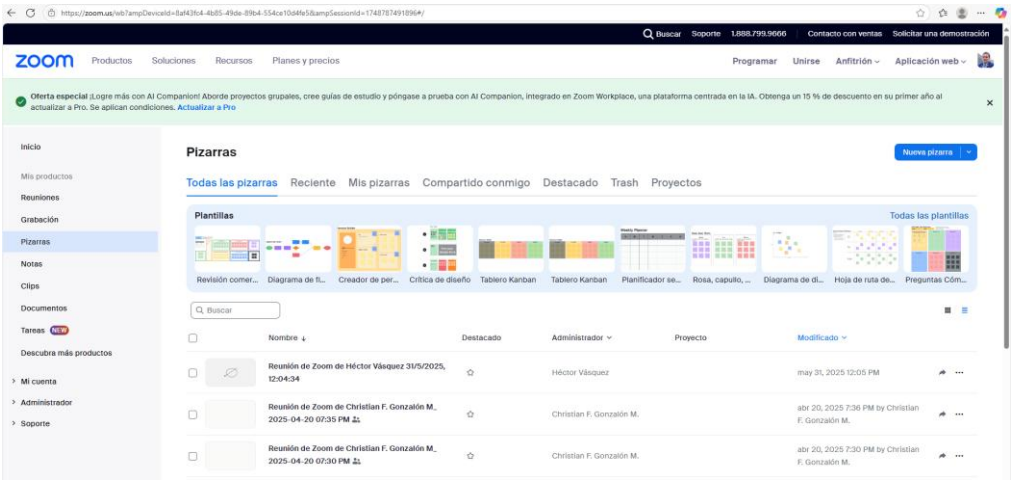
Lista de reuniones realizadas y sus participantes



Nota. Pantalla que muestra las reuniones realizadas con los participantes

Figura 65

Pizarras que se mostraron en las reuniones



Nota. Pantalla que muestra las pizarras realizadas en las reuniones

4.1.4. Clasificación los artefactos según su origen (sistema, aplicación, navegador).

Zoom no guarda registros directamente en el navegador como lo haría una aplicación web convencional, pero la información relacionada con la cuenta y actividad de Zoom podría almacenarse en el navegador a través de cookies y caché.

Estos son los detalles sobre cómo podría almacenarse la información en tu navegador:

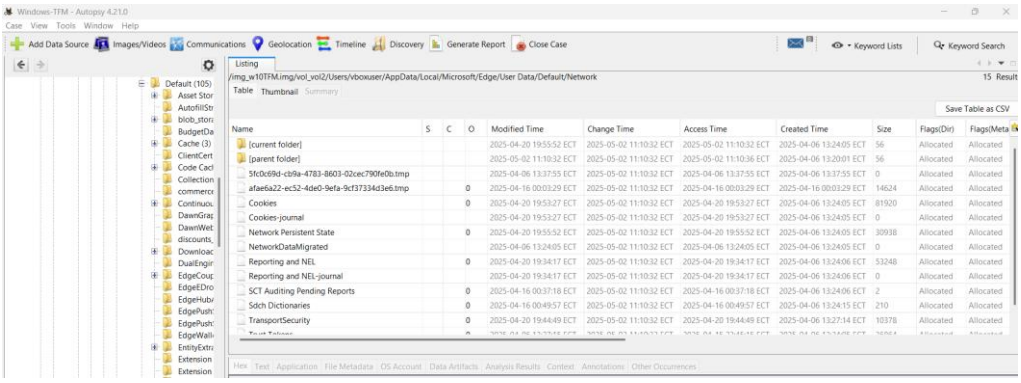
Cookies:

Cuando se inicia sesión en Zoom a través de su página web (https://zoom.us), el navegador puede guardar cookies que contienen información sobre la sesión, preferencias y autenticación, como se puede ver en las Figuras 66 y 67. Estas cookies pueden almacenar:

- La sesión iniciada para que no se tenga que iniciar sesión cada vez.
- Preferencias de configuración de la cuenta.
- Información relacionada con las configuraciones de la reunión o de la cuenta.
- El navegador Microsoft Edge almacena cookies en Windows 11/10 en el directorio "%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Network"

Figura 66

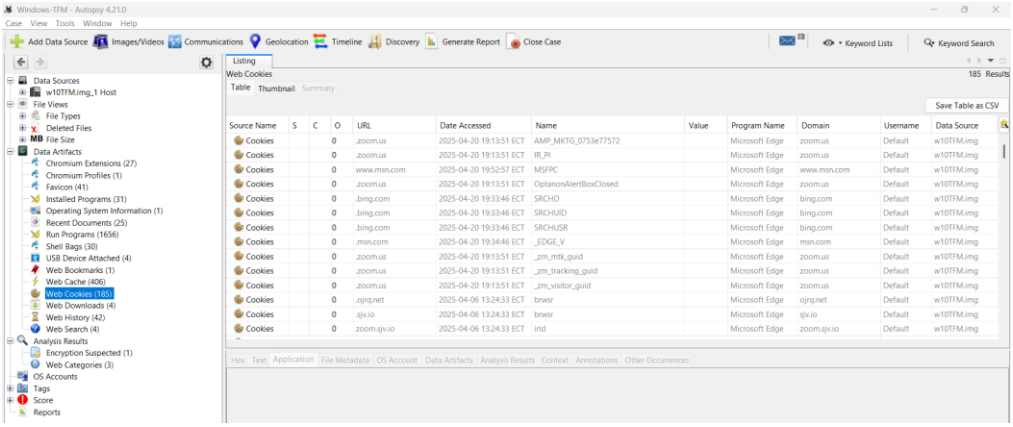
Ruta donde se almacenan cookies que guarda Edge en Windows 10



Nota. Pantalla que muestra las cookies de Edge en Windows 10

Figura 67

Cookies Web que muestra Autopsy



Nota. Pantalla que muestra las cookies en Windows 10

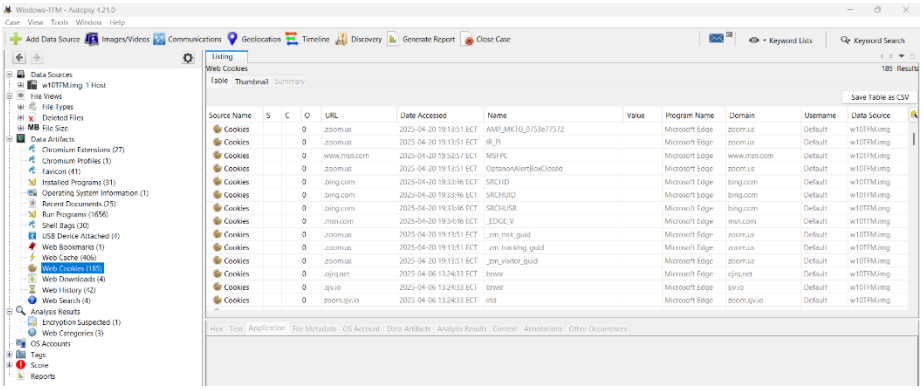
Se analizaron las cookies, pero no se identificó información relevante que nos pueda servir para un análisis forense.

Caché del navegador:

Al usar Zoom en el navegador, sobre todo si se usa la versión web y no la aplicación de escritorio, el navegador puede almacenar ciertos archivos en su caché como se puede ver en la Figura 68. Esto puede incluir:

- Archivos como imágenes, audios o videos que se utilizan en las páginas de Zoom.
- Scripts y otros archivos necesarios para la ejecución de la interfaz web.

Figura 68
Cache del navegador en Windows



Nota. Pantalla que muestra el caché del navegador

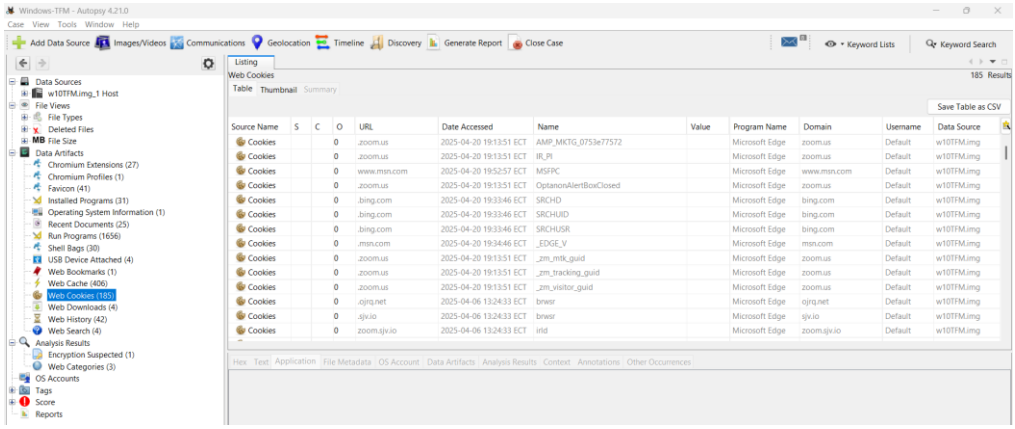
En los registros de Web Cache si se encuentra información referente a Zoom, pero los datos identificados no son tan claros, se identifica fechas de accesos al sitio web de Zoom, esto se podría correlacionar con el resto de los datos recolectados.

Historial del navegador:

Si se accede al portal de Zoom desde el navegador, es posible que se guarde un registro de las páginas web visitadas en el historial del navegador. Esto incluye la página principal de Zoom, las páginas de las reuniones a las que se unieron o incluso las páginas de configuración de la cuenta. Con los datos obtenidos con Autopsy se pudo identificar incluso registros de inicio de reuniones por zoom, accesos al

sitio para descarga de la aplicación, fechas en las que se inició la reunión como se puede ver en la Figura 69.

Figura 69
Cache del historial del navegador

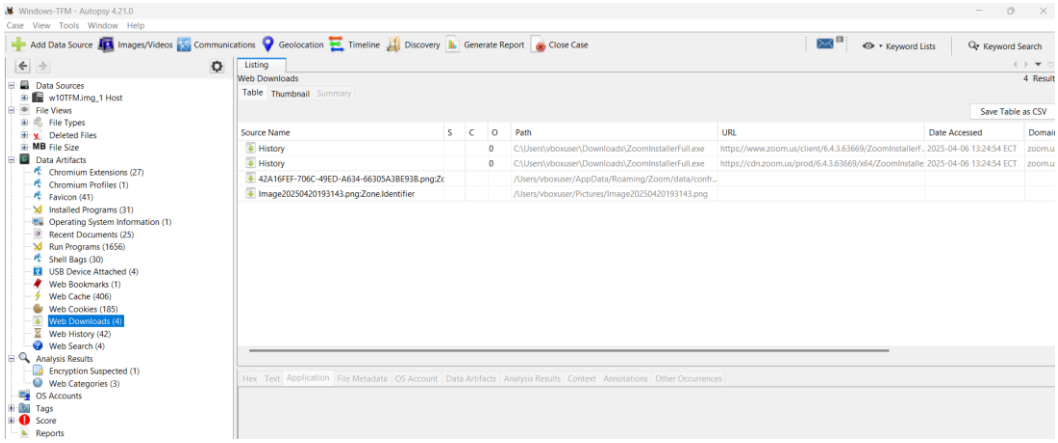


Nota. Pantalla que muestra el caché del historial del navegador

Archivos de Zoom en el navegador (Zoom Web Client):

Si se utiliza el cliente web para unirse a reuniones sin la aplicación de Zoom instalada, el navegador puede almacenar ciertos archivos de configuración o datos temporales relacionados con la reunión en su caché, pero Zoom no guarda "registros" completos como los que se guardan en la aplicación o en los servidores de Zoom como se puede ver en la Figura 70.

Figura 70
Descargas del navegador

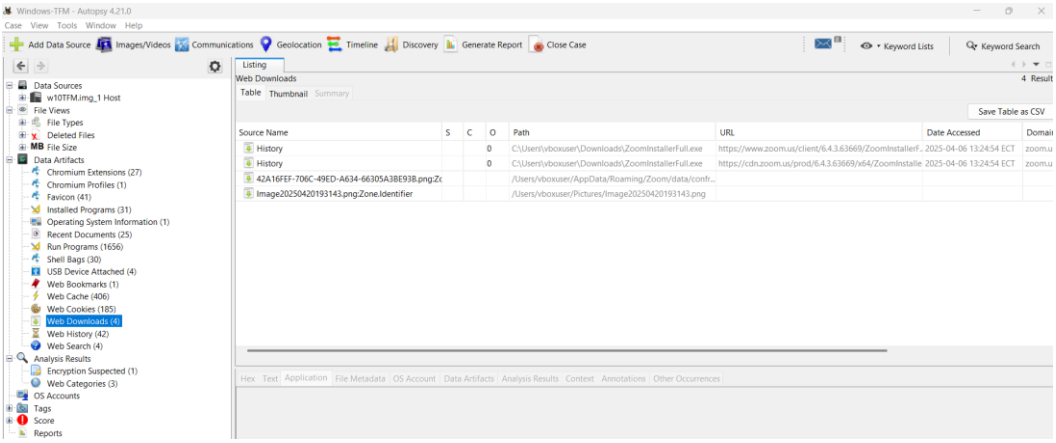


Nota. Pantalla que muestra las descargas del navegador

En las descargas del navegador se pudo identificar la fecha en la que se descargó el instalador de Zoom y también se puede identificar la descarga de imágenes colocadas en el chat de Zoom, estas son almacenadas en el directorio “/Users/[Usuario]/AppData/Roaming/Zoom/data/confres” como habíamos visto en puntos anteriores y en la Figura 71.

Figura 71

Documentos recientes del sistema Windows



Nota. Pantalla que muestra los documentos usados recientemente en plataformas Windows

En documentos recientes también se encontró información importante, ya que se identificó los archivos de una sesión de Zoom almacenados en una de las rutas utilizadas por este aplicativo y las fecha en las que se accedió a estos documentos.

4.1.5. **Determinar la persistencia de artefactos tras eliminar Zoom o datos.**

Si Zoom fue eliminado de la computadora, no se borrarán automáticamente todos los registros o archivos relacionados con la aplicación. Aunque Zoom se desinstala, algunos archivos de configuración, caché, registros y otros datos temporales podrían permanecer en el sistema, dependiendo del sistema operativo. Vamos a ver más detalles por Sistema Operativo:

Windows:

Archivos de configuración y registros: A menudo, la desinstalación de Zoom no elimina completamente los archivos de configuración y los registros de la aplicación. Estos pueden quedar en las siguientes ubicaciones:

- C:\Users\[Usuario]\AppData\Roaming\Zoom\. En este fichero solamente quedan dos registros luego de la desinstalación, uno de ellos indica todo el proceso de desinstalación de la aplicación (installer.txt) y el otro archivo está vacío (appsafecheck.txt).
- C:\Users\[Usuario]\AppData\Local\Zoom\. Se validó el proceso y este directorio es borrado por completo cuando se realiza la desinstalación.
- C:\Users\[Usuario]\Documents\Zoom\ (si tienes grabaciones locales). La información de este directorio se mantiene intacta después de un proceso de desinstalación.

Archivos temporales: Algunos archivos temporales de Zoom también podrían quedar en el directorio de "Archivos temporales" de Windows que se almacenan en C:\Users\[Usuario]\AppData\Local\Temp. En este directorio no se identificaron archivos relacionados con la aplicación Zoom que nos puedan servir en un análisis forense.

Algunas carpetas y archivos de las reuniones no se eliminan automáticamente cuando se desinstala Zoom, se lo debe hacer de forma manual.

macOS Catalina:

Archivos de configuración y registros: Al igual que en Windows, algunos archivos de configuración y registros podrían permanecer incluso después de desinstalar la aplicación de Zoom. Estos archivos suelen encontrarse en:

- /Users/[Usuario]/Library/Application Support/Zoom.us/ Se puede observar que luego de la desinstalación se mantienen estos directorios en el equipo.
- /Users/[Usuario]/Documents/Zoom/ Se puede observar que luego de la desinstalación se

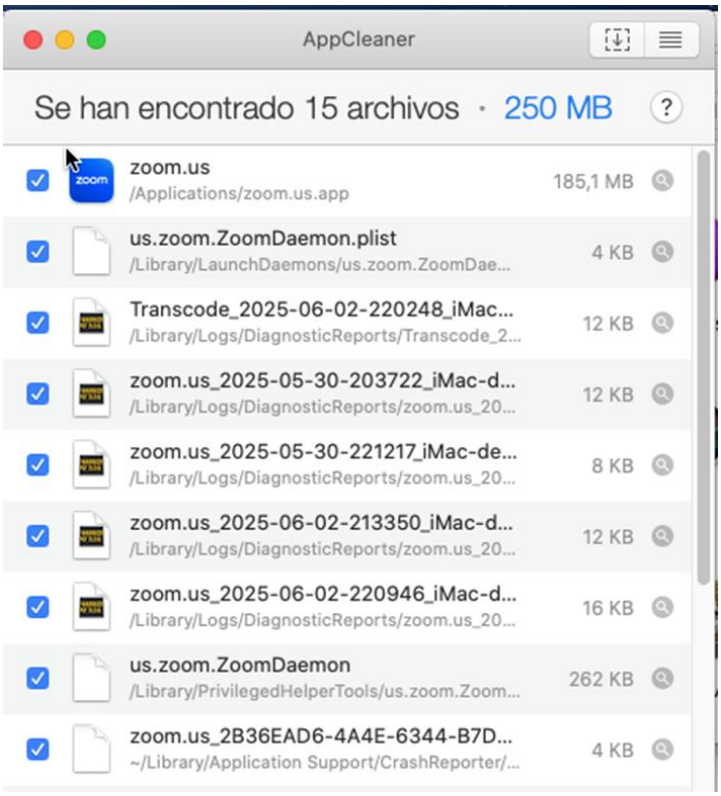
mantienen estos directorios en el equipo.

- /Users/[Usuario]/Library/Logs/Zoom.us/ Se puede observar que luego de la desinstalación se mantienen estos directorios en el equipo.
- /Users/[Usuario]/Downloads Se puede observar que luego de la desinstalación se mantienen estos directorios en el equipo.

Para eliminar completamente esos archivos, se lo debe hacer manualmente después de desinstalar la aplicación, se validó que sucede cuando usamos una herramienta que permite desinstalar aplicaciones y eliminar archivos residuales, en este caso usamos AppCleaner la cual si borro los directorios donde se instala la aplicación Zoom (no topa los directorios donde se guardó información de reuniones o el directorio de descargas) como se muestra en la Figura 72. Lo que se pudo observar es que, pese a ese proceso, la información aún se queda en la papelera de reciclaje, como se observa en la Figura 73.

Figura 72

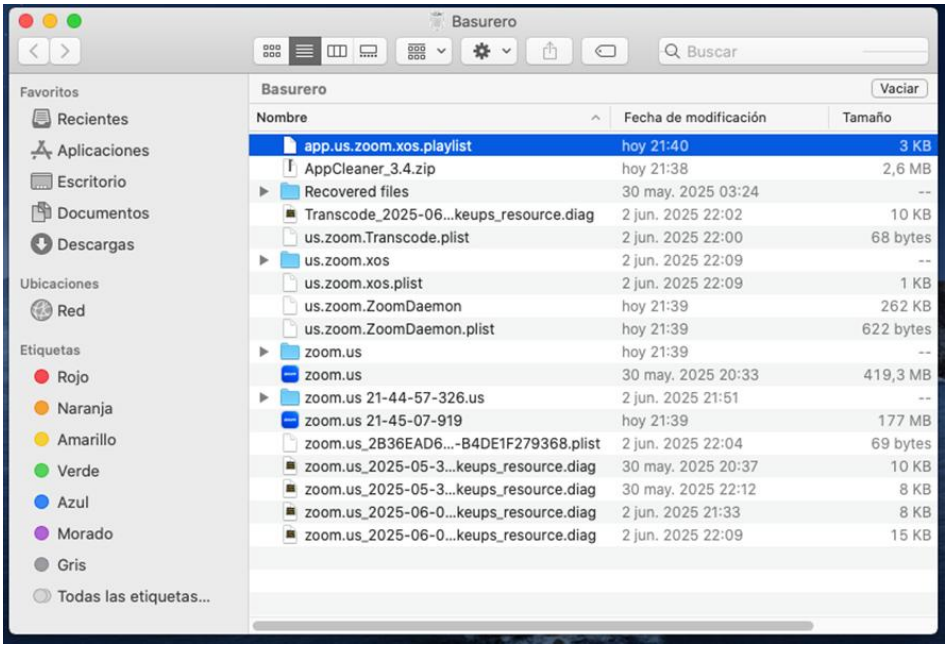
Desinstalación de Zoom con AppCleaner



Nota. Pantalla que muestra lo que se va a borrar con AppCleaner

Figura 73

Documentos recientes del sistema Windows



Nota. Pantalla que muestra los archivos borrados en la papelera de reciclaje

Linux Ubuntu:

Archivos de configuración y registros: Los archivos de configuración y registros pueden permanecer en las siguientes ubicaciones:

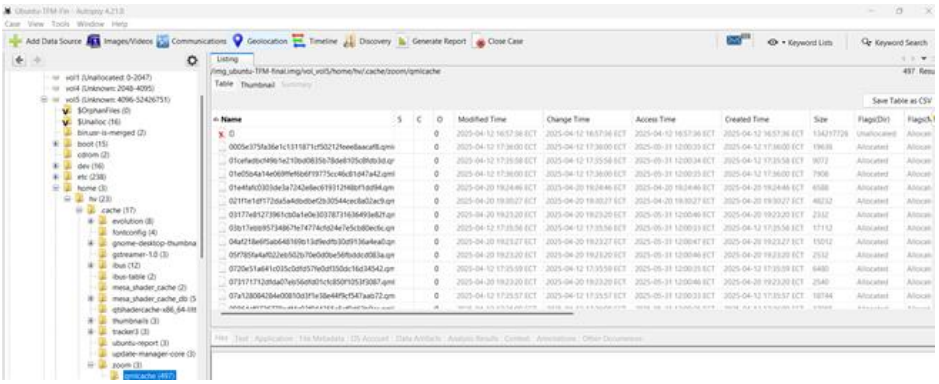
- /home/[Usuario]/.zoom/ Este directorio no se borra por completo, es necesario realizar un proceso manual o a través de un script.
- /home/[Usuario]/Documents/Zoom/ Este directorio no es borrado cuando se realiza el proceso de desinstalación, el borrado se debe realizar de forma manual.

Archivos temporales y caché: Los archivos temporales también pueden quedar en:

- /home/[Usuario]/.cache/zoom/ Este directorio no se borra por completo, es necesario realizar un proceso manual, la información de esta ruta se puede observar en la Figura 74.

Figura 74

Ruta del caché en Ubuntu



Nota. Pantalla que muestra los archivos almacenados en el caché de Ubuntu

4.1.6. **Determinar si es posible reconstruir eventos a partir de los datos.**

Con base en la información que hemos recabado, si es posible reconstruir eventos a partir de los datos siempre y cuando la reunión haya sido grabada, de esta manera se obtendrá información más clara y detallada, ya que podremos contar con audio, video, chat, imágenes del chat, etc. Si la sesión no fue grabada, va a ser muy difícil encontrar evidencias, ya que la mayoría de los archivos de los cuales podríamos obtener información valiosa se encuentra cifrada, a continuación, colocamos un resumen de las rutas y archivos más importantes identificados.

Tabla 3

Comparativa de los resultados

Sistema Operativo	Ruta	Archivo	Detalle
Windows	C:\Users\[Usuario]\AppData\Roaming\Zoom\logs\zoomcrash_xxxxxx_xxxx	xxxx.dmp	El archivo dmp es un dump de memoria que contiene información del error presentado.
Windows	C:\Users\[Usuario]\AppData\Roaming\Zoom\logs\zoomcrash_xxxxxx_xxxx	xxxx.xml	Datos importantes relacionados con las capacidades y características del computador como por ejemplo el consumo de memoria, versión de sistema operativo, memoria disponible, fecha de inicio de la reunión, fecha de logueo en la reunión, la versión de Zoom, en ocasiones el ID de la reunión,
Windows	C:\Users\[Usuario]\AppData\Roaming\Zoom\	installer.txt	Contiene información detallada del proceso de instalación, actualizaciones y desinstalación.
Windows	C:\Users\[Usuario]\AppData\Local\Zoom\		En esta ruta no se encontró información relevante para nuestro análisis, de lo validado contiene emojis que utiliza la aplicación.
Windows	C:\Users\[Usuario]\Documents\Zoom\		Si la reunión fue grabada vamos a encontrar la grabación, el audio, la información que se colocó en el chat de la reunión, entre otros. Zoom va a crear un directorio para cada reunión que se grabe.
Windows	C:\Users\[Usuario]\AppData\Roaming\Zoom\data\confres		En esta ruta se almacenan las capturas y gráficos enviados por el chat de las reuniones si la misma fue grabada
Windows	C:\Users\[Usuario]\AppData\Roaming\Zoom\data\net_records	ZoomNetRecord_xxxxxx_win.log	este archivo guarda información relevante para nuestro análisis, ya que contiene información de las solicitudes HTTP realizadas por la aplicación cuando se encuentra en funcionamiento. El archivo está en formato json el cual contiene detalles de las interacciones de Zoom con sus servidores, hay campos importantes como http_code para saber si fallo o fue exitoso, el campo url que es la url del servidor de Zoom contactado

MAC	/Users/[Usuario]/Library/Logs/Zoom.us/crashlog	usage.txt	Registra información detallada sobre errores que ocurren en Zoom, dentro de la información almacenada se encuentra el ID de la reunión e información relacionada con el consumo de recursos
MAC	/Users/[Usuario]/Library/Application Support/Zoom.us/data/xxxxxxx/confres/xxxxxxxx		Contiene información de las capturas o imágenes colocadas en el chat de la reunión
MAC	/Users/[Usuario]/Documents/Zoom/		Si la reunión fue grabada en esta ruta se crea una carpeta por cada reunión en la cual se almacena el audio, video, chat de la reunión y el archivo de configuración el cual contiene un ID específico que identifica a los archivos de audio y video generados en esa reunión.
MAC	/Users/[Usuario]/Downloads		Los archivos compartidos durante las reuniones no se encuentran en ninguno de los directorios ya nombrados, estos datos se almacenan en la carpeta de descargas
Linux	/home/[Usuario]/.zoom/logs	zoom_stdout_stderr.log	
Linux	/home/[Usuario]/.zoom/		En este directorio hay varios subdirectorios, en su mayoría son archivos que se encuentran cifrados y cuya data no es legible
Linux	/home/[Usuario]/.zoom/data/confres/		Posee las imágenes que fueron compartidas en la reunión si esta fue grabada, esta información si pudiera ser relevante en un análisis forense
Linux	/home/[Usuario]/Documents/Zoom/		Si la reunión fue grabada en esta ruta se crea una carpeta por cada reunión en la cual se almacena el audio, video, chat de la reunión y el archivo de configuración el cual contiene el ID que forma parte de los nombres de los archivos de audio y video generados
Linux	/var/log/apt/	history.log	En este archivo se puede encontrar la fecha de instalación de Zoom

Nota. En la Tabla 3 se puede observar las rutas más importantes para un análisis forense de Zoom.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

El análisis forense de artefactos generados durante reuniones virtuales utilizando aplicaciones como Zoom ha demostrado ser un campo crítico y de creciente interés por todas las personas, dado el creciente uso del uso de estas herramientas para actividades sociales, laborales y académicas.

Con trabajo final de maestría denominado “RECOLECCIÓN, IDENTIFICACIÓN Y ANÁLISIS DE ARTEFACTOS FORENSES GENERADOS DURANTE VIDEOLLAMADAS DE ZOOM” se comprobó que, durante una reunión virtual utilizando Zoom, se genera información relevante desde el punto de vista forense, como por ejemplo archivos temporales, logs de la conexión, historial de chats y documentos compartidos, grabaciones locales y metadatos que pueden ser analizados en futuras investigaciones digitales.

El análisis comparativo entre Windows 10, macOS Catalina y Linux Ubuntu nos permitió identificar que la generación de los artefactos puede variar dependiendo del sistema operativo que se está utilizando, lo cual representa un reto técnico para la estandarización de metodologías forenses. Cada sistema operativo tiene su particularidad en el momento de utilizar herramientas forenses, no todas son compatibles, adicionalmente, el tiempo que toma cargar las imágenes de cada sistema operativo varía lo cual puede generar inconvenientes si se tiene poco tiempo para realizar un análisis forense.

En el trabajo final se utilizaron las herramientas FTK Imager y Autopsy, las cuales demostraron ser buenas en la obtención y análisis de imágenes de cada sistema operativo usado, con estas herramientas se facilitó la recuperación de información relevante sin comprometer la integridad de los datos. La herramienta Autopsy tomó mucho más tiempo en extraer la información de las imágenes que FTK Imager; pero la ventaja de usar Autopsy, es que la información extraída fue mucho más completa y detallada, lo cual es una ventaja sumamente importante al momento de realizar un análisis forense.

Al desinstalar Zoom de una computadora, no todos los archivos y registros relacionados se eliminan automáticamente. Es posible que queden archivos de configuración, caché y registros en tu sistema que tendrás que borrar manualmente. Además, los registros relacionados con tus reuniones,

chats y grabaciones en la nube se mantienen en los servidores de Zoom y no se eliminan al desinstalar la aplicación.

Sería muy importante para el análisis forense poder replicar la investigación realizada en este trabajo final utilizando otras herramientas que se encuentran en el mercado como por ejemplo Microsoft Teams, Google Meet o Cisco Webex, que también son utilizadas en el mundo. Con esto, se podría ampliar el alcance del estudio y establecer comparativas que fortalezcan el ciberestudio.

REFERENCIAS BIBLIOGRÁFICAS

[1] Casey, E. (2019). *Digital Forensics and Cyber Crime: Methods, Applications, and Challenges*. Academic Press.

[2] Zoom Video Communications, Inc. (2023). *Security and Compliance in Zoom*. https: //zoom.us/security

[3] AccessData. (2023). *FTK Imager User Guide*. https://www.accessdata.com/ products-services/forensic-toolkit-ftk

[4] Basis Technology. (2023). *Autopsy: Digital Forensics Platform*. https://www. autopsy.com/

[5] X-Ways Software Technology. (2023). *X-Ways Forensics Manual*. https://www. x-ways.net/forensics/

[6] Microsoft. (2023). *Log Parser Studio Documentation*. https://www.microsoft. com/en-us/download/details.aspx?id=24659

[7] Wireshark Foundation. (2023). *Wireshark Users Guide*. https://www.wireshark. org/docs/

[8] Magnet Forensics. (2023). *Magnet AXIOM Product Overview*. https://www. magnetforensics.com/products/magnet-axiom/

[9] Guidance Software. (2023). *EnCase Forensic Overview*. https://www. guidancesoftware.com/encase-forensic

[10] SANS Institute. (2022). *Digital Forensics and Incident Response: Tools and Techniques*. https://www.sans.org/cyber-security-courses/ digital-forensics-incident-response/

[11] Ministerio de Seguridad de la Nación. (2023). Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. Revista Pensamiento Penal. https://www.pensamientopenal.com.ar/system/files/Documento1096.pdf

[12] National Institute of Standards and Technology. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[13] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-86/final

[14] Scientific Working Group on Digital Evidence. (2022). Best practices for computer forensics. https://www.swgde.org/documents

[15] Association of Chief Police Officers. (2012). ACPO good practice guide for digital evidence (5th ed.). Home Office Centre for Applied Science and Technology. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1181057/digital-evidence-5th-edition.pdf

[16] International Organization for Standardization. (2012). ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html

[17] Zoom Video Communications. (s.f.). *Una plataforma para conectarse*. Zoom.

[18] CISO Global. 27 Oct 2019. How to Convert a VirtualBox Disk File (.vdi) to a Raw Image File. https://www.youtube.com/watch?v=60Nv1zPVzjc&t=56s

[19] TI-Forensik Wiki. Nov 2021. Lokale Webkonferenz-Artefakte Bewertung der forensischen Aussagekraft und der Datensicherheit. https://it-forensik.fiw.hs-wismar.de/index.php/Olaf_Hoffmann

[20] Seguridad y Redes. 24 Mar 2008. Análisis de red con Wireshark. Filtros de captura y visualización. https://seguridadyredes.wordpress.com/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacian/

[21] ComoFriki. 10 Dic 2020. Cómo usar Wireshark para capturar, filtrar y analizar paquetes. https://comofriki.com/como-usar-wireshark-capturar-filtrar-analizar-paquetes/

[22] Canonical. (s.f.). *Download Ubuntu Desktop*. Ubuntu. https://ubuntu.com/download/desktop

[23] Apple Inc. (s.f.). *Apple*. https://www.apple.com/

[24] Exterro. (s.f.). FTK Imager: Forensic data imaging and preview solution. Exterro. https://www.exterro.com/digital-forensics-software/ftk-imager

[25] Al Barghuthi, N. B., & Said, H. (2013). Social networks IM forensics: Encryption analysis. Journal of Communications, 8(11), 708–715.

[26] O'Flaherty, K. (2020). Beware Zoom users: Here's how people can 'zoom-bomb' your chat. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/

[27] Lorenz, T., & Alba, D. (2020). 'Zoombombing' becomes a dangerous organized effort. The New York Times. https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

[28] Setera, K. (2020). FBI warns of teleconferencing and online classroom hijacking during COVID-19 pandemic. Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[29] Azab, A., Watters, P., & Layton, R. (2012). Characterizing network traffic for Skype forensics. In 2012 Third Cybercrime and Trustworthy Computing Workshop (pp. 19–27). IEEE. https://doi.org/10.1109/CTC.2012.6393513

[30] Majeed, A. (2016). Forensic analysis of social media apps in Windows 10. NUST Journal of Engineering Sciences.

Apéndices

Enlace a los archivos y recursos usados para el presente proyecto.

https://www.1024tera.com/spanish/sharing/link?surl=Gb_wWkt5A0bHlwpG_upTxA