



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Análisis forense de la huella digital de un usuario en  
sistemas informáticos

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Melián Angel, Joel

Tutor/a: Terrasa Barrena, Andrés Martín

CURSO ACADÉMICO: 2022/2023



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



Escola Tècnica  
Superior d'Enginyeria  
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica  
Universitat Politècnica de València

# Análisis forense de la huella digital de un usuario en sistemas informáticos

Trabajo Fin de Grado

**Grado en Ingeniería Informática**

**Autor:** Melián Ángel, Joel

**Tutor:** Terrasa Barrena, Andrés Martín

2022/2023



# Resumen

---

Este trabajo fin de grado tiene como objetivo describir las principales técnicas actuales de análisis forense que permiten descubrir e interpretar la huella digital dejada por un usuario al utilizar un sistema de interés y aplicar dichas técnicas sobre sistemas reales para comprobar su funcionamiento y eficacia. En concreto, el proyecto se centrará en la adquisición, preservación y análisis de los datos que se generan en un sistema operativo al ser utilizado de manera habitual por un usuario cualquiera, empleando para ello herramientas actuales de análisis forense y asegurando la integridad de la información mediante técnicas de cifrado. El estudio incluirá un pequeño proyecto de experimentación de dichas técnicas y herramientas sobre ciertos sistemas existentes, tanto de la familia de sistemas Windows como Linux, de forma que pueda ilustrarse su uso y utilidad en casos de ejemplo con datos ya existentes o creados de forma intencionada a modo de prueba.

**Palabras clave:** Análisis forense; huella digital; sistemas operativos, Windows; Linux

# Abstract

---

This final degree project aims to describe the main current techniques of forensic analysis that allow discovering and interpreting the fingerprint left by a user when using a system of interest and applying these techniques on real systems to verify their operation and effectiveness. Specifically, the project will focus on the acquisition, preservation and analysis of the data generated in an operating system when used regularly by any user, using current forensic analysis tools and ensuring the integrity of the information. using encryption techniques. The study will include a small experimentation project of these techniques and tools on certain existing systems, both from the Windows and Linux family of systems, so that their use and usefulness can be illustrated in example cases with already existing or intentionally created data as a test.

**Keywords:** Forensic analysis; fingerprint; operating systems, Windows; Linux



# Tabla de contenidos

---

1.	Introducción.....	8
1.1	Motivación.....	8
1.2	Objetivos.....	9
1.3	Estructura de la memoria .....	9
2.	Estado del arte .....	11
2.1	Definición de informática forense.....	11
2.2	Historia de la informática forense.....	12
2.3	Conceptos fundamentales de la seguridad informática.....	13
2.4	Legislación y normativa.....	14
2.4.1	Legislación.....	15
2.4.1.1	Derechos fundamentales.....	15
2.4.1.2	Reglamento General de Protección de Datos.....	15
2.4.1.3	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.....	16
2.4.1.4	Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.....	17
2.4.1.5	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	17
2.4.1.6	Estatuto de los trabajadores.....	18
2.4.2	Estándares de la informática forense .....	18
2.4.2.1	ISO 71505/2013. Sistema de Gestión de Evidencias Electrónicas.....	18
2.4.2.2	ISO 71506/2013. Metodología para el análisis forense de las evidencias electrónicas.....	19
2.4.2.3	ISO/IEC 27037/2012. Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital .....	19
2.4.2.4	ISO/IEC 27042:2015. Normativa para el análisis e interpretación de evidencias digitales .....	20
2.4.3	Conclusiones acerca de las implicaciones en relación con la normativa y la legislación .....	21
3.	Herramientas de análisis forense y creación del entorno de trabajo.....	23
3.1	Herramientas empleadas para el análisis forense.....	23
3.1.1	AccessData FTK Imager .....	23
3.1.2	AccessData Registry Viewer.....	23



3.1.3	ExifTool.....	24
3.1.4	Volatility.....	24
3.1.5	WebBrowserPassView .....	25
3.1.6	Browser History Examiner .....	26
3.1.7	Autopsy.....	26
3.2	Creación del entorno de trabajo.....	27
3.2.1	Creación de un entorno de laboratorio basado en máquinas virtuales... 28	
3.2.1.1	Descarga de imágenes ISO .....	29
3.2.1.2	Creación de máquinas virtuales, asignación de recursos e instalación del sistema operativo .....	32
3.2.2	Creación de imagen de disco virtual a partir de disco duro físico .....	34
3.2.2.1	Creación de imagen de disco virtual en Windows .....	35
3.2.2.2	Creación de imagen de disco virtual en Linux .....	36
3.2.2.3	Montar disco virtual en la máquina virtual.....	37
3.2.3	Descripción final del entorno de trabajo.....	41
4.	Fuentes de información digital .....	43
4.1	Fuentes de información digital en un sistema informático .....	43
4.2	Discos duros .....	44
4.3	Memoria RAM.....	45
4.4	Registros del sistema .....	46
4.5	Navegadores web.....	46
4.6	Metadatos de archivos .....	46
4.7	Otras fuentes de información .....	47
5.	Adquisición, análisis y preservación de la información digital .....	49
5.1	Adquisición y análisis de la información digital.....	49
5.1.1	Logs y registros del sistema operativo .....	49
5.1.1.1	Logs en Linux.....	49
5.1.1.2	Logs en Windows.....	53
5.1.2	Registro de Windows .....	56
5.1.3	AccessData FTK Imager para recuperación de los archivos del registro.....	58
5.1.4	AccessData Registry Viewer para visualizar los valores de los archivos de registro.....	60
5.1.5	Recuperación de contraseñas del navegador con WebBrowserPassView..	65
5.1.6	Recuperación y análisis de datos de navegación con Browser History Examiner .....	68
5.1.7	Visualización de metadatos con ExifTool.....	77

5.1.8 Volcado de memoria RAM con AccessData FTK Imager/AVML (Acquire Volatile Memory for Linux) y extracción de información con Volatility .....	83
5.1.9 Recuperación y análisis de datos de dispositivos de almacenamiento con Autopsy .....	91
5.2 Preservación de información.....	106
5.2.1 Función hash criptográfica .....	107
6. Conclusiones.....	111
6.1 Grado de cumplimiento de los objetivos.....	111
6.2 Relación con los estudios cursados.....	112
7. Bibliografía.....	115





# 1. Introducción

---

## 1.1 Motivación

La privacidad es un aspecto importante en la vida de toda persona y resulta innato querer preservarla, ocultando y haciendo confidencial información que no queremos compartir con otras personas. Por otro lado, la curiosidad u otras motivaciones menos lícitas pueden llevar a intentar vulnerar dicha privacidad, e intentar acceder a información de la que no disponemos o que no está a nuestro alcance. En función de varios aspectos, este tipo de intentos puede constituir fácilmente un supuesto delictivo.

Hoy en día, la digitalización del mundo en el que vivimos es global, y está presente especialmente en cómo se almacena la información de personas y organizaciones, que en su práctica totalidad tiene un formato digital y es almacenada en equipos informáticos. Desde esa perspectiva, los intentos de vulnerar la privacidad que comentábamos arriba suelen producirse por medios digitales, convirtiéndose en muchas ocasiones en delitos informáticos de distintos tipos, como robo de datos, fraudes, o daños a la propiedad intelectual, entre otros.

En este contexto, el análisis forense informático incorpora un conjunto de técnicas informáticas que permiten obtener información, conservarla y analizarla cuando se produce alguna brecha de seguridad. Desde esa perspectiva, el análisis forense de sistemas es una herramienta fundamental para la prevención, detección y resolución de incidentes de seguridad informática.

Prácticamente cualquier acción que se realiza en un sistema informático queda registrada en el mismo y con las técnicas adecuadas es posible consultarla, incluso aquella que no resulta aparente en principio. Acciones como apagados o reinicios del sistema, inicios de sesión de usuarios, intentos de elevación de privilegios de usuario, borrado o modificación de datos, entre muchos otros, pueden resultar claves para detectar y obtener evidencias de posibles delitos informáticos cometidos en un sistema.

En este proyecto se quiere analizar y poner en práctica algunas de las principales técnicas de análisis forense y, en particular, aquellas que permiten obtener la denominada huella digital que los usuarios producen en un sistema informático durante su uso. En particular, seleccionaremos y utilizaremos algunas de las herramientas que suelen utilizarse en este tipo de análisis, incluyendo también ciertos aspectos legales, tales como la legislación y normativas que resultan afectadas por la práctica de la informática forense y los principales delitos que pueden ser objeto de estudio mediante esta disciplina.

A nivel personal, la motivación de este proyecto surgió tras realizar los cursos de formación en la empresa en la que estuve haciendo prácticas durante el grado, que incluyeron temas sobre análisis forense de sistemas, recuperación de archivos, criptografía y virtualización. Estos cursos ampliaron mi interés previo en esta temática, al comprobar la complejidad real de las técnicas implicadas y el uso real de ciertas herramientas en sistemas operativos actuales, como Linux o Windows.

## 1.2 Objetivos

El objetivo principal de este Proyecto fin de grado es mostrar la huella digital que deja un usuario de un sistema informático con el simple uso de dicho sistema a lo largo del tiempo, y demostrar que prácticamente toda información almacenada de forma digital puede perdurar en el tiempo como datos residuales, aunque se creyese eliminada previamente. Para poder obtener y mostrar esta huella digital será necesario recopilar, preservar y analizar datos obtenidos de las principales fuentes de información digital que podemos encontrar en un sistema operativo, tales como los archivos del usuario, el registro del sistema, la memoria o los datos recopilados por los navegadores web, entre otros.

Este objetivo principal puede matizarse en otros objetivos más concretos, entre los que destacan los siguientes:

- Describir los aspectos legales más relevantes relacionados con la informática forense, incluyendo una visión general de los delitos informáticos más comunes hoy en día, y de la legislación relacionada con este tipo de delitos y con la práctica de la informática forense.
- Estudiar y analizar las técnicas principales de la informática forense, así como algunas de las herramientas informáticas que permiten aplicar dichas técnicas.
- Utilizar estas herramientas para obtener información relevante del uso del sistema (huella o rastro digital) que podría ser útil en una investigación forense, dando ejemplos concretos de información que ha sido recopilada.
- Identificar las principales fuentes de información que permiten extraer la huella digital de un sistema informático, y comprender qué tipo de información relevante se puede extraer de cada una de ellas.
- Identificar a partir de dicha información el comportamiento del usuario que ha utilizado el sistema, con el fin de detectar actividades sospechosas o potencialmente ilícitas.
- Concienciar acerca de la seguridad digital y la privacidad en el uso de sistemas informáticos, ofreciendo una visión del rastro que un usuario deja diariamente con el mero hecho de utilizar un ordenador.

De manera adicional, pero no menos importante, el objetivo personal del alumno consiste en ampliar los conocimientos de la formación recibida, conocer más a fondo ciertas herramientas de análisis forense y de recuperación de datos, y ofrecer una visión introductoria sobre la informática forense a otras personas que estén interesadas en esta temática.

## 1.3 Estructura de la memoria

La estructura que sigue el presente documento se divide en 6 capítulos, que se complementan con la bibliografía y un anexo. A continuación, se dará una visión general de qué contenidos se tratan en cada uno de ellos.

En este primer capítulo se incluye una introducción del tema que tratará el proyecto y aquellos motivos que han impulsado la elección del tema, así como los objetivos del proyecto y el presente repaso a la estructura de la memoria.

En el segundo capítulo se proporcionará el contexto necesario acerca de la temática del proyecto, explicando en qué consiste la informática forense desde un punto de vista tecnológico y ofreciendo un contexto histórico de la misma, lo que incluye sus inicios, su evolución y su estado en la actualidad. Además, se introducen los conceptos fundamentales de la seguridad informática y cómo estos están relacionados con la informática forense. Finalmente, se presenta la legislación y la normativa por la cual se rige esta práctica y unas conclusiones sobre las implicaciones de dicha legislación y la normativa tienen sobre la temática de este proyecto.

En el tercer capítulo se presentarán las herramientas que se emplearán en la fase de análisis y recuperación de datos, destacando las capacidades, compatibilidades y funcionalidades por las que han sido elegidas. También se explicará en detalle cómo se ha montado el entorno de análisis basado en máquinas virtuales.

En el cuarto capítulo se repasan y explican las principales fuentes de información de las cuales podemos extraer información en un sistema operativo actual, y la importancia de estas por la información que contienen. Se definirán los diferentes tipos de fuentes de información y se detallará su funcionamiento, además de proporcionar una visión general del tipo de datos que estas contienen.

En el quinto capítulo emplearemos las herramientas específicas que han sido definidas en el Capítulo 3 para extraer algunos de estos datos y analizaremos el contenido de estos. También veremos cómo podemos preservar esta información mediante técnicas criptográficas, garantizando que esta no ha sido alterada desde que fue recuperada.

Finalmente, en el sexto capítulo se muestran las conclusiones del proyecto, se reflexiona acerca del cumplimiento de los objetivos que se perseguían en el proyecto y se presenta la relación que tiene este con los estudios cursados, la importancia de algunas asignaturas que han proporcionado conocimientos fundamentales para su realización.

Tras dichos capítulos y la bibliografía, de manera adicional se incluye un anexo, dedicado a la relación de los Objetivos de Desarrollo Sostenible (ODS) al proyecto realizado.

## 2. Estado del arte

---

En este capítulo se expondrá la situación actual de la informática forense. Así mismo se recogerán distintas regulaciones, normativas y estándares que construyen el marco legal y veremos todo aquello que define el concepto que conocemos como informática forense hoy en día.

### 2.1 Definición de informática forense

La informática forense, también llamada análisis o ciencia forense digital es la rama de la informática que recoge un conjunto de técnicas y procedimientos que se enfocan en la identificación, preservación, análisis y presentación de datos digitales con fines legales y judiciales los cuales se pueden presentar como evidencias en un proceso judicial. Estos datos no son de fácil acceso, por lo que se necesita un nivel de investigación más profundo por parte del analista para obtenerlos, ya que no se encuentran a simple vista, sino que tiene que obtenerlos en un nivel de datos más profundo empleando técnicas diversas para desenterrarlos.

Esta disciplina es vital en la investigación de delitos informáticos, ya que este tipo de delitos se cometen a través de dispositivos informáticos como pueden ser ordenadores, teléfonos móviles o medios de almacenamiento digital, ya que estos pueden tratarse tanto de una fuente del delito como de una víctima de este. Su objetivo principal es la extracción de datos sin alterar el estado de estos para después poder realizar una investigación sobre aquello que se ha obtenido. Es muy importante hoy en día ya que prácticamente toda la información se genera y se almacena en medios electrónicos.

Hay varios tipos de fuentes de datos de los cuales extraer evidencias, y en este caso concreto nos centraremos en el análisis de sistemas operativos, enfocando la investigación en el sistema de archivos para poder recopilar toda la información posible de los mismos. Podríamos decir que además de recuperar información que se encuentra en el sistema también se hace una labor de descubrimiento. Esto es debido a que no solamente se puede obtener la información que podemos recuperar a simple vista como un usuario normal del sistema, sino que además de eso podemos descubrir información que ha sido eliminada, ocultada o modificada de manera intencional. Podría tratarse de un error humano o de un error del propio sistema de archivos, pero no hay que descartar que estos hechos se hayan producido con fines delictivos con el objetivo de ocultar evidencias.

El análisis forense de sistemas se podría definir como el conjunto de técnicas y procedimientos enfocados a recuperar los datos generados en un sistema operativo de un equipo informático, protegerlos de modificaciones y analizarlos para su posterior presentación como evidencias.

## 2.2 Historia de la informática forense

Los inicios de la informática forense [23] se remontan a la época de 1970, cuando los expertos en informática comenzaron a investigar y analizar los sistemas informáticos en busca de pruebas relacionadas con delitos. En los primeros días de la informática, la informática forense aún no era reconocida como una disciplina formal. Sin embargo, los investigadores comenzaron a utilizar técnicas informáticas para analizar datos digitales en casos criminales. Los primeros delitos cometidos a través de sistemas informáticos se remontan al año 1978, que se detectaron en el estado de Florida. Unos años después se creó una herramienta llamada `copy2pc` por parte de Central Point Software, que era una herramienta que permitía realizar copias de los disquetes de la época y que permitía protegerlos de la piratería.

En la década de 1980 con el crecimiento de la tecnología informática y la proliferación de sistemas informáticos, surgió la necesidad de un enfoque más formal en la investigación forense digital. El término "informática forense" comenzó a utilizarse ampliamente y se desarrollaron las primeras herramientas y técnicas especializadas. La informática forense comenzó a ser reconocida como una disciplina importante en la investigación criminal. El Departamento de Defensa de los Estados Unidos desarrolló técnicas de análisis forense para investigar los delitos informáticos en sus sistemas. En el año 1983 surge una herramienta creada de la mano de Peter Norton llamada `UNERASE tool` incluida en la suite Norton Utilities que permite recuperar archivos y aplicaciones que hayan sido borradas de forma accidental incluso tras formatear el disco duro, siendo una herramienta pionera en la informática forense.

En la década de 1990, el aumento de los delitos informáticos y la utilización cada vez más extendida de tecnologías digitales en la vida cotidiana hizo que la informática forense se convirtiera en una disciplina esencial para la investigación criminal, ya que los ordenadores eran cada vez más frecuentes en los hogares y la tecnología avanzaba año tras año muy rápidamente. Se fundaron organizaciones especializadas en la investigación de delitos informáticos, como la Organización Internacional de Evidencia Digital (IOCE). A medida que los delitos informáticos se volvían más sofisticados, la informática forense se convirtió en un campo vital para la lucha contra el cibercrimen. Se crearon organizaciones especializadas para abordar este tipo de delitos como la INTERPOL Forensic Science Symposium fundada en 1998. También el FBI empieza a utilizar los sistemas informáticos para detectar delitos digitales y obtener evidencias de estos haciendo pruebas a los equipos que servían como objeto de estudio.

En la década de los 2000, se produjo un aumento significativo en la cantidad de casos de delitos informáticos y en la complejidad de las investigaciones. La informática forense se convirtió en una disciplina altamente especializada, con técnicas y herramientas avanzadas para la recopilación, análisis y presentación de pruebas digitales. Con el aumento exponencial de la cantidad de datos digitales y el desarrollo de nuevas tecnologías, como dispositivos móviles y redes sociales, la informática forense tuvo que adaptarse rápidamente. Se desarrollaron técnicas más avanzadas para la recuperación y el análisis de evidencia digital. Se establecieron los primeros laboratorios de informática forense como el laboratorio regional de la Informática Forense del FBI fundado en el año 2000.

En la década de 2010 la informática forense sigue siendo una disciplina esencial para la investigación criminal en la era digital. Los expertos en informática forense utilizan técnicas y herramientas cada vez más sofisticadas para investigar los delitos informáticos y presentar pruebas digitales en los tribunales. La informática forense

adquirió una mayor relevancia debido a casos destacados de ciberataques y filtraciones de datos como el ataque a Sony por una brecha de seguridad en los sistemas de PlayStation Network, el ataque a la red de eBay que acabó produciendo filtración de datos de sus usuarios o el escándalo electoral en EE. UU. que usó sin consentimiento la información de más de 50 millones de perfiles de Facebook con la intención de difundir la propaganda electoral. Se establecieron estándares y mejores prácticas para la recopilación y preservación de pruebas digitales. También surgieron desafíos relacionados con la privacidad y la protección de datos personales. En esta década se establecieron la mayoría de los estándares ISO y UNE que establecen las bases y los procedimientos de la informática forense.

En la actualidad, la informática forense sigue siendo una disciplina en constante evolución, ya que la tecnología sigue avanzando y los delitos informáticos se vuelven cada vez más complejos. La inteligencia artificial y el aprendizaje automático están siendo utilizados para analizar grandes volúmenes de datos de manera más eficiente. Además, se están desarrollando técnicas especializadas para abordar delitos relacionados con criptomonedas y *blockchain*. Cabe destacar que el 2020 fue el año de la pandemia del Covid-19 que comportó la integración del teletrabajo en muchos sectores. Esto produjo un incremento de los ciberataques como correos de SPAM, malware o URL maliciosas relacionadas con el Covid-19 y aumentó el número de víctimas de este tipo de ataques al ser propicio el uso de dispositivos informáticos para teletrabajar.

## 2.3 Conceptos fundamentales de la seguridad informática

La seguridad total de la información es un término que no es posible de tratar en términos absolutos, ya que no existe como tal y se suele hablar más del término de fiabilidad de los sistemas de información. Cuando hablamos de que un sistema es fiable nos referimos a la probabilidad de que se comporte de la manera esperada en función de si es alta o baja.

Uno de los objetivos de la informática forense consiste en proteger la información, es decir, garantizar la seguridad informática. El término de seguridad o fiabilidad informáticas se compone de las bases de tres conceptos fundamentales para su definición:

- **Confidencialidad:** el acceso a la información debe de estar controlado para que solo puedan acceder a ella las personas autorizadas para ello.
- **Integridad:** la información debe de ser exacta y estar libre de modificaciones ante accidentes o intentos de modificación no autorizados.
- **Disponibilidad:** la información debe de encontrarse de manera accesible para aquellos que tengan acceso a esta.

La confidencialidad consiste en mostrar la información a aquellos que estén autorizados y mantenerla en secreto u ocultarla a aquellos que no están autorizados a visualizarla, todo con el objetivo de prevenir que esta información se divulgue de forma no autorizada o accidental y se haga pública. En este término entra en juego la criptografía, que es una práctica que consiste en codificar la información con el fin de

protegerla mediante algoritmos informáticos, funciones hash, firmas digitales o claves de encriptación/descriptación. También exploraremos más a fondo el concepto de criptografía en capítulos futuros de este documento.

La integridad consiste en mantener la información sin modificaciones no autorizadas, y este concepto hace referencia a la integridad de los datos como tal y a la integridad del origen de estos. La integridad de los datos consiste en mantener los datos intactos y que la información que contienen sea exacta, mientras que la integridad del origen de los datos consiste en garantizar que la fuente de los datos es segura y fiable, por lo cual se puede confiar en ella. Aunque se haga referencia a otros dos subconceptos de esta definición se deben de cumplir ambos para asegurar la integridad de la información.

La disponibilidad consiste en tener la información de manera accesible en todo momento para aquellas personas que tengan acceso a la misma y que esté disponible para su uso o consulta en el momento que se requiera. Que la información sea accesible depende de aquel medio en el cual se almacene, por lo que si la información se almacena en un sistema informático y este sistema no tiene la disponibilidad necesaria es posible que no se pueda disponer de la información en algunos momentos.

Estos tres conceptos deben de darse todos a la vez y mantener un equilibrio entre ellos para poder garantizar la seguridad informática. Podría darse la misma prioridad a todos o bien darle mayor prioridad a algún aspecto en concreto dependiendo del entorno en el que se encuentren almacenados los datos.

La seguridad de un sistema informático acaba determinando en gran medida cómo de sencillo será acceder al sistema, extraer datos, modificarlos, eliminarlos, tanto por parte de un usuario normal, un analista o un criminal. Teniendo esto en cuenta si un sistema es más seguro costará más obtener información de este cuando no se está autorizado para ello, aunque esto suponga dificultar el trabajo de un analista o de los desarrolladores de herramientas software de análisis forense.

La seguridad informática desempeña un papel fundamental en la informática forense porque preserva la evidencia digital evitando alteraciones involuntarias, protege contra manipulación de datos y garantiza su integridad, resguarda la privacidad de las personas investigadas, protege datos confidenciales de accesos no autorizados, mantiene la integridad de la cadena de custodia a lo largo de todo el proceso de investigación, evita fugas de información y asegura el cumplimiento de leyes y estándares éticos.

## 2.4 Legislación y normativa

En este apartado se expondrá la legislación más relevante que se debe de tener en cuenta al realizar un análisis forense de un sistema informático. También se mostrarán las normativas que definen los estándares de la informática forense.



## 2.4.1 Legislación

En este apartado se recopila la legislación relacionada con el tratamiento y conservación de datos personales, derechos de los ciudadanos, así como los principales delitos informáticos tipificados en el código penal.

### 2.4.1.1 Derechos fundamentales

Es el conjunto de derechos humanos garantizados bajo el marco de la Constitución Española [1]. Son los derechos que están ligados a la dignidad y naturaleza de cada individuo como ser humano. Estos derechos se consideran inalienables, lo que significa que están arraigados en la persona misma y no pueden ser separados o transferidos. Tampoco pueden ser suprimidos, negados o renunciados por ninguna entidad o autoridad, ya que son inherentes a la condición humana y no pueden ser objeto de comercio, cesión o eliminación.

Cabe a destacar los siguientes:

- Derecho a la seguridad jurídica que nos garantice un proceso penal con garantías.
- Derecho al secreto de las comunicaciones.
- Derecho a la vida privada, a la intimidad, al honor y a la propia imagen. Este derecho se limita para no emplear la informática para proteger la intimidad personal.
- Derecho a la protección de datos.

### 2.4.1.2 Reglamento General de Protección de Datos

Regula el tratamiento que realizan personas o instituciones públicas o privadas de los datos personales que tengan que ver con personas en la Unión Europea. Es el marco legal de la Unión Europea que rige la recopilación y el tratamiento de datos de carácter personal de individuos o instituciones europeas. También se encarga de establecer las normas relacionadas con la libre circulación de los datos personales.

Este reglamento [2] establece que el uso y tratamiento de los datos deberá llevarse a cabo de manera justa y legal además de que este tratamiento debe de tener un fin específico y legítimo y que únicamente se podrán tratar aquellos datos que sean necesarios para cumplir con el objetivo que se quiere alcanzar.



### 2.4.1.3 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Establece aquellas actitudes o acciones que se establecen como delito. Son de interés aquellas acciones que se consideren delitos informáticos [3] entre los cuales destacamos los siguientes por su relevancia:

- Descubrimiento y revelación de secretos: daño a la intimidad personal, familiar o a la propia imagen de la víctima mediante conductas como acceso, uso o modificación de datos informáticos de carácter personal, o difusión no autorizada de material privado de la víctima.
- Descubrimiento y revelación de secretos empresariales: la diferencia con respecto al anterior es que no daña la intimidad personal, sino que atenta contra el patrimonio de la empresa y sus intereses sociales y económicos.
- Acceso ilícito a sistemas informáticos: acceder de manera ilícita a un sistema vulnerando las medidas de seguridad de este y en contra de la voluntad de su usuario legítimo, interceptar datos informáticos sin permiso mediante técnicas o artificios, o facilitar programas o contraseñas que nos permitan vulnerar la seguridad de estos sistemas y poder cometer los delitos mencionados anteriormente.
- Daños informáticos: acciones que traten de dañar, borrar, alterar o hacer inaccesible un sistema de información, como puede ser una manipulación indebida de la máquina física o un ataque de denegación de servicio (DoS).
- Falsedades informáticas: se recopilan todas las falsedades comunes que puedan llevarse a cabo en el ámbito informático, como falsificar una moneda, documento, certificado, tarjetas bancarias o cheques de viaje.
- Estafa informática: manipulaciones informáticas para obtener sin autorización una transferencia de bienes patrimoniales en perjuicio de una tercera persona, uso y distribución de programas informáticos con ese fin, o realizar operaciones no autorizadas con tarjetas bancarias de un tercero.
- Defraudación de comunicaciones: utilizar un terminal de telecomunicaciones sin autorización de su titular causando daños económicos al mismo.
- Cibercrimes sexuales: recoge todos los tipos de abuso sexual contemplados en el código penal, pero de forma específica se destaca la utilización de las tecnologías de la información para contactar con un menor y engatusarlo para concertar un encuentro sexual o para que este le facilite contenido sexual en el que aparezca un menor. También se recoge el exhibicionismo ante menores, difusión de material con contenido sexual y delitos relacionados con prostitución, explotación y corrupción de menores a través del uso de las tecnologías de la información.
- Delitos contra la propiedad intelectual: Reproducción, plagio o distribución de una obra pública con ánimo de lucro y sin autorización de los autores originales, incluyendo las acciones que pretendan eliminar o modificar las reglas informáticas que se emplean para proteger estas obras de las acciones mencionadas anteriormente, así como el uso y distribución de medios

destinados a neutralizar medidas de seguridad que pretenden proteger programas informáticos u obras.

- Delitos contra el honor: cuando se trata de dañar el honor de una persona o una institución con calumnias e injurias, así como de la difusión de este tipo de mensajes por cualquier medio tecnológico.
- Amenazas y coacciones: llevar a cabo estas acciones en el mundo digital como chantaje, intimidación, engaño o acoso.
- Delitos de odio y apología al terrorismo: atentar contra los derechos fundamentales de un individuo promoviendo o incitando el odio, violencia o discriminación por motivos racistas, religiosos, prejuicios sociales, ideología, discapacidad u orientación sexual. Enaltecer de forma pública actos terroristas cuando estos se difunden por medios digitales.

#### **2.4.1.4 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**

Su objetivo [4] es determinar qué información resulta relevante como para ser recopilada con el fin de poder rastrear delitos con el fin de prevenirlos y aumentar la seguridad ciudadana. Esto permite que los teleoperadores de telecomunicaciones puedan recopilar datos o generarlos, con la finalidad de que los miembros de los Cuerpos Policiales puedan acceder a ellos dentro del marco de una investigación criminal. Estos datos se obtienen de telefonía fija, móvil, internet y cualquier medio de comunicación digital. Se conservan los datos necesarios para poder trazar toda comunicación desde el origen a su destino.

#### **2.4.1.5 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.**

La Ley Orgánica de Protección de Datos (LOPD) [5] tiene como objetivo principal salvaguardar y garantizar los derechos y libertades de las personas físicas en relación con el procesamiento de sus datos personales. Esta legislación está diseñada para preservar la dignidad, intimidad y privacidad de los individuos al regular el manejo de la información que los identifica de manera personal.

La LOPD establece normativas y principios que las organizaciones deben seguir al recopilar, almacenar, procesar y compartir datos personales, asegurando que se trate esta información con responsabilidad y respeto.

Otro de sus objetivos es adaptar el Reglamento General de Protección de Datos de la Unión Europea a la legislación en España. Establece leyes acerca del tratamiento de los datos de carácter personal, y deben de cumplir con ella individuos y organizaciones que traten este tipo de datos.

La Agencia Española de Protección de Datos es la institución que se encarga del cumplimiento de esta ley y de sancionar a los que la incumplen. Esta ley deroga a la

anterior Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, aunque sigue siendo aplicada para ciertos escenarios.

#### **2.4.1.6 Estatuto de los trabajadores**

Es una normativa [6] que regula las relaciones entre la empresa y los profesionales que realizan su labor en ella. Es de obligada aplicación en cualquier sector de producción. En relación con la informática podemos destacar dos artículos en concreto que interfieren entre sí:

- Art. 18: Derecho a la intimidad personal de los trabajadores y a mantener en secreto sus comunicaciones y su vida privada.
- Art 20.3: El empresario tiene el poder de vigilar y controlar el cumplimiento de las labores de trabajo de sus empleados.

Ambos artículos entran en conflicto porque se contradicen, ya que por una parte el trabajador tiene derecho a que se respete la intimidad de sus datos, pero el empresario tiene el poder de acceder a estos si se trata de un control laboral.

#### **2.4.2 Estándares de la informática forense**

Son documentos que sirven como patrón y referencia que determinan las normas técnicas que se usan en el ámbito del análisis forense. Estos son elaborados por la Organización Internacional de la Normalización (ISO), que reuniendo la opinión de expertos mundiales en el tema en concreto se redactan las normas técnicas acerca del mismo con el objetivo de hacerlas internacionales [7].

##### **2.4.2.1 ISO 71505/2013. Sistema de Gestión de Evidencias Electrónicas**

Define los aspectos técnicos para garantizar la integridad de las evidencias electrónicas. En este documento se resuelven las principales cuestiones en relación con la obtención y conservación de las evidencias. Consta de tres partes bien diferenciadas:

1. Sistema de Gestión de las evidencias Electrónicas (Vocabulario y conceptos generales): Define los conceptos de la seguridad de la información en relación con las evidencias electrónicas y describe definiciones y términos.
2. Buenas prácticas en la gestión de las evidencias electrónicas: Se centra en los procesos para establecer, poner en marcha, controlar mantener y mejorar un Sistema de Gestión de Evidencias Electrónicas.

3. Formatos y mecanismos técnicos: Define el formato de las evidencias electrónicas como la cabecera, el contenido o las credenciales de seguridad.

#### **2.4.2.2 ISO 71506/2013. Metodología para el análisis forense de las evidencias electrónicas**

Esta norma ha sido creada para definir cuál es el proceso de análisis forense a la hora de gestionar las evidencias obtenidas en el proceso de recuperación de la información. Trata de ser una ampliación o un complemento de los aspectos definidos en las Normas ISO 71505. Esta se compone de varias fases:

1. Preservación de la información: Aborda la forma en que se debe almacenar y mantener la evidencia digital para asegurar que no se modifique, degrade ni pierda su validez con el tiempo.
2. Adquisición de los datos: Ofrece recomendaciones sobre cómo recolectar y adquirir datos digitales de manera que se preserven su integridad y autenticidad.
3. Documentación del procedimiento: Indica cómo debe llevarse a cabo la documentación y el registro de las acciones tomadas durante la identificación, adquisición y preservación de la evidencia digital.
4. Análisis de las evidencias: En esta fase, se realizan análisis detallados de las evidencias digitales recopiladas. Se examinan los datos en busca de información relevante. Esto puede incluir la recuperación de archivos eliminados, el análisis de metadatos o la identificación de patrones de comportamiento.
5. Presentación del informe: Después de completar el análisis, se prepara un informe detallado que resume los hallazgos, métodos utilizados y conclusiones. El informe debe ser claro, completo y comprensible para personas no técnicas, como abogados, jueces o miembros del jurado.

#### **2.4.2.3 ISO/IEC 27037/2012. Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital**

Esta norma aborda la dirección, los principios y las prácticas de la evidencia digital. Este estándar tiene como objetivo proporcionar orientación y mejores prácticas para identificar, adquirir y preservar evidencia digital de manera efectiva y legalmente sólida. Proporciona pautas para que la evidencia digital se maneje de manera adecuada para garantizar su validez y utilidad.

Presenta el concepto de cadena de custodia que es el procedimiento controlado que asegura la integridad y autenticidad de los elementos probatorios hallados en la investigación desde que son encontradas hasta que se aportan como evidencias en el proceso y la autoridad competente ordene su conclusión.

Algunos aspectos que esta norma aborda incluyen:

1. Identificación de evidencia digital: Proporciona pautas para identificar qué tipos de datos digitales pueden ser considerados como evidencia en un contexto forense o legal.
2. Adquisición de evidencia digital: Ofrece recomendaciones acerca de cómo recolectar y adquirir datos digitales de forma que se preserven su integridad y autenticidad.
3. Preservación de evidencia digital: Aborda la forma en que se debe almacenar y mantener la evidencia digital para asegurar que no se modifique, degrade ni pierda su validez con el tiempo.
4. Documentación y registro: Indica cómo debe llevarse a cabo la documentación y el registro de las acciones tomadas durante la identificación, adquisición y preservación de la evidencia digital.
5. Consideraciones legales y éticas: Aborda cuestiones legales y éticas relacionadas con la recopilación y el uso de evidencia digital en investigaciones y procedimientos legales.

#### **2.4.2.4 ISO/IEC 27042:2015. Normativa para el análisis e interpretación de evidencias digitales**

Esta norma brinda directrices para el análisis y la interpretación de evidencias digitales, abordando cuestiones de continuidad, validez y repetibilidad. Establece las buenas prácticas en la selección, diseño e implementación de procesos analíticos, asegurando que estos puedan ser escrutados independientemente.

Proporciona orientación para demostrar la competencia del perito informático en la selección de métodos y la interpretación de evidencia digital. La norma aborda la complejidad del análisis forense, considerando circunstancias donde los peritos informáticos deben justificar sus enfoques y adaptar métodos nuevos. Los métodos utilizados pueden afectar la interpretación de la evidencia digital.

Establece un marco común para el manejo de incidentes de seguridad en sistemas de información, ofreciendo pautas para implementar nuevos métodos y estándares mínimos para la evidencia digital resultante. Describe el proceso de análisis e

interpretación de evidencia digital en incidentes, desde la identificación hasta su aceptación como prueba en juicios.

La norma también especifica elementos que deben incluirse en informes periciales, como calificaciones del perito, información inicial, detalles del incidente y la investigación, daños en la evidencia, procesos y herramientas utilizados, interpretaciones y conclusiones, así como recomendaciones para futuras investigaciones para asegurar una documentación completa y precisa del proceso de análisis forense y sus resultados.

### **2.4.3 Conclusiones acerca de las implicaciones en relación con la normativa y la legislación**

Cabe destacar que toda esta legislación y normativa es aplicable a una investigación de informática forense. En el caso de este proyecto el análisis será realizado desde un sistema personal y no el de un tercero, por lo que el tratamiento de los datos no requerirá de ningún permiso especial o de autorizaciones judiciales de investigación como si se tratase del ordenador de otra persona. Tampoco es necesaria la presentación de un informe ni la presentación de pruebas, ya que en este caso no se está investigando ningún delito, sino que se están recopilando datos de fuentes diversas para ver su contenido y recopilar información acerca de ellos.

En el caso de que tuviéramos que investigar el sistema de un tercero algunos de los cumplimientos que deberíamos de realizar son:

- Respetar los derechos de privacidad del individuo o entidad cuyo sistema se investiga, asegurando un acceso legal y ético a datos personales o confidenciales.
- Cumplir con los requisitos de autorización, ya que en muchos países exigen obtener una orden judicial para garantizar que la investigación se realice dentro de los límites legales y respetando los derechos de las partes afectadas.
- Mantener una cadena de custodia adecuada para preservar la integridad de los datos recopilados, lo que es crucial para que la evidencia sea admisible en un tribunal.
- Cumplir con regulaciones específicas que se apliquen a la informática forense, especialmente en casos que involucren datos sensibles como los de salud o financieros.
- Garantizar la confidencialidad de los resultados de la investigación, evitando la divulgación no autorizada que podría tener consecuencias legales.

- Obtener consentimiento informado cuando sea necesario, especialmente en investigaciones corporativas, antes de realizar una investigación forense en un sistema.
- Asegurar que todo el proceso de investigación y recopilación de evidencia se realice de manera que la evidencia resultante sea admisible en un tribunal, incluyendo un manejo adecuado de la evidencia y documentación de la cadena de custodia.
- Seguir códigos de ética profesional que rigen la conducta y prácticas de los investigadores forenses para mantener estándares éticos en su trabajo.

## 3. Herramientas de análisis forense y creación del entorno de trabajo

---

En este capítulo se expondrán las herramientas software empleadas para el análisis y extracción de información relevante presente en el sistema que será objeto de análisis. Posteriormente veremos cómo se ha creado el entorno de trabajo y explicaremos en detalle el montaje del entorno de laboratorio mediante máquinas virtuales creadas a partir de las imágenes de disco de los sistemas originales.

### 3.1 Herramientas empleadas para el análisis forense

En este apartado se verá una serie de herramientas que serán empleadas para realizar la obtención y el análisis de los datos obtenidos por estas. Se les dará un uso enfocado de manera práctica y técnica sobre cada herramienta ya que veremos sus funciones y las probaremos en el entorno de laboratorio.

#### 3.1.1 AccessData FTK Imager

FTK Imager [8] consiste en una herramienta independiente del FTK (Forensics Toolkit) desarrollado también por AccessData que es compatible para sistemas Windows. La principal función de este programa es la de guardar imágenes de disco que puede ser guardada en diversos formatos, aunque el más común es el formato RAW.

Además de eso este programa también es capaz de realizar volcados de memoria y de recuperar archivos del sistema como los registros de Windows, funciones por las cuales va a ser una herramienta muy importante en el proceso de obtención de datos.

#### 3.1.2 AccessData Registry Viewer

Registry Viewer [9] es un programa que es capaz de visualizar el contenido de los archivos de registro del sistema operativo. Esta herramienta permite acceder a los archivos protegidos del registro los cuales contienen contraseñas, nombres de usuario y otra información a la que no podríamos acceder directamente con el editor de registro de Windows.

Tiene una interfaz de usuario dividida en 2 vistas, por lo que podremos obtener información más general de todo el archivo de registro desde la vista completa o bien podremos obtener datos más concretos y significativos del área común. Dispone de un visor hexadecimal para poder ver cualquier propiedad seleccionada en formato hexadecimal. Mediante este programa podremos analizar en detalle los archivos de registro del sistema recuperados previamente por el programa FTK Imager.



### 3.1.3 ExifTool

ExifTool [10] es una herramienta de software de línea de comandos desarrollada en Perl por Phil Harvey. Esta herramienta es capaz de leer, escribir y manipular metadatos en una amplia variedad de formatos de archivos digitales empleando bibliotecas de lectura y escritura específicas de formato para acceder a los metadatos en los archivos.

ExifTool puede procesar metadatos de una amplia gama de tipos de archivos, incluyendo imágenes en formato JPEG, RAW, PNG, GIF, entre otros. También es compatible con archivos de audio en formato MP3, WAV, FLAC, y archivos de vídeo en formato MP4, MOV, AVI, y más. Además, puede trabajar con metadatos en archivos de documentos como PDF, DOC, XLS, y otros formatos populares.

La herramienta ExifTool permite realizar diversas operaciones en los metadatos, como extraer información detallada de los archivos, modificar o agregar nuevos metadatos, eliminar metadatos específicos, copiar metadatos entre archivos y renombrar archivos en función de los metadatos. Además, ExifTool ofrece una amplia gama de etiquetas de metadatos predefinidas para diferentes tipos de archivos, así como la capacidad de crear etiquetas personalizadas para abordar requisitos específicos si el archivo lo requiere.

ExifTool se ejecuta a través de la línea de comandos, lo que permite una mayor flexibilidad y automatización en su uso. Los usuarios pueden utilizar comandos y opciones específicas para realizar operaciones precisas en los metadatos de los archivos. Además, ExifTool es una herramienta multiplataforma y está disponible para sistemas operativos como Windows, macOS, Linux y otros. Además de su presentación a través de línea de comandos dispone también de una versión con interfaz gráfica de usuario como complemento de esta herramienta haciendo que su uso sea más ágil y sencillo para cualquiera que la utilice.

Debido a su capacidad para trabajar con una amplia gama de formatos de archivos y su versatilidad en el manejo de metadatos, ExifTool es ampliamente utilizado en diversos campos, como la fotografía, la informática forense y la gestión de archivos. Además, su desarrollo activo y su amplia base de usuarios contribuyen a su reputación como una de las herramientas líderes en la manipulación de metadatos en archivos digitales. Con ExifTool podremos examinar los metadatos de casi cualquier archivo.

### 3.1.4 Volatility

Volatility [11] es una herramienta de análisis forense de código abierto basado en Python cuya función es recuperar la información que se almacena en la memoria RAM. Permite el análisis y la extracción de información valiosa de imágenes de memoria volátil, como procesos en ejecución, servicios, controladores, conexiones de red, registros de eventos y otros artefactos del sistema.

El marco Volatility Forensics proporciona una amplia gama de comandos y plugins que se utilizan para identificar y analizar estructuras de datos en la memoria RAM, como tablas de procesos, tablas de descriptores de archivos, estructuras de red y registros del sistema. Estos plugins permiten extraer información clave, como nombres de archivos abiertos, direcciones IP, contraseñas en memoria, claves de registro y otras evidencias importantes en una investigación.

Volatility Forensics es muy portátil y es compatible con varios sistemas operativos, incluyendo Windows, Linux y macOS. Puede analizar imágenes de memoria adquiridas de sistemas en vivo o imágenes de memoria volcadas de forma forense además de poseer características más avanzadas como la recuperación de archivos eliminados de la memoria y el análisis de archivos de paginación.

Al tratarse de un programa de código abierto cuenta con una comunidad de usuarios que permiten mejorar a esta herramienta al añadirle nuevas características mediante plugins.

Como complemento a esta herramienta disponemos de Volatility Workbench que se trata de una interfaz gráfica de usuario para Volatility que está disponible para Windows. Esta interfaz desarrollada por la compañía PassMark Software hace que el uso de esta potente herramienta sea todavía más sencillo para el usuario.

Mediante esta herramienta podremos obtener la información de los volcados de memoria que generemos con programas como AccessData FTK Imager.

### 3.1.5 WebBrowserPassView

WebBrowserPassView [12] es un software de recuperación de contraseñas desarrollado por NirSoft cuya función es revelar los pares usuario/contraseña que los usuarios almacenan manualmente en el navegador. Está diseñada para sistemas operativos Windows. Esta herramienta utiliza técnicas de extracción de contraseñas específicas de cada navegador para recuperar las contraseñas guardadas en los perfiles de usuario de los navegadores web, y esta es capaz de recuperar cualquier contraseña de cualquier sitio web siempre y cuando esta esté almacenada en el navegador.

La herramienta es compatible con una amplia variedad de navegadores, incluyendo los más usados y conocidos como se trata de Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge, Opera entre otros. A pesar de sus limitaciones a la hora de poder recuperar las contraseñas dependiendo de la versión del navegador o de otros factores es una herramienta muy útil para recuperar contraseñas de forma eficaz.

Muestra información de la URL junto al par usuario/contraseña con el que se ha iniciado sesión y que el usuario ha decidido guardar. WebBrowserPassView requiere acceso al perfil de usuario y a las bases de datos de contraseñas de los navegadores para poder recuperar la información y por lo tanto, se requieren permisos de administrador para ejecutar la herramienta correctamente. Una vez recuperadas las contraseñas estas se pueden exportar en un archivo en varios formatos como texto plano, HTML, CSV o XML.

WebBrowserPassView es una herramienta útil para casos en los que se necesita recuperar contraseñas almacenadas en navegadores web, como cuando se olvida una contraseña o se requiere acceder a una cuenta en un navegador sin tener que recordarla manualmente. Sin embargo, se podría emplear en casos de una investigación forense para recuperar los datos de acceso a las cuentas del usuario que se esté investigando si este ha cometido algún delito cibernético a través de estas de tal forma que el acceso a las cuentas nos haga poder disponer de una mayor cantidad de información y esto a su vez haga más fácil la tarea de encontrar alguna evidencia

que nos resulte relevante para poder presentarla como una prueba de las acciones delictivas de la persona investigada.

### 3.1.6 Browser History Examiner

Browser History Examiner [13] es una herramienta de análisis forense desarrollada por Foxtan Forensics compatible con sistemas Windows que es empleada para extraer y visualizar el historial de internet que se almacena en el navegador. Esta herramienta recopila la información de aquellas páginas web que se han visitado y permite visualizar el historial de navegación, y la caché de imágenes y sitio web, así como la fecha en la que se ha visitado esa página, la URL, el título de la página, un contador de visitas y el navegador desde el cual se ha accedido a esa página en concreto. El programa es capaz de extraer la información de los principales navegadores como Firefox, Edge, Chrome o Safari. Tiene una interfaz muy sencilla de usar y fácil de visualizar, haciendo que la tarea de analizar la información que nos proporciona el programa resulte cómodo y sencillo para el usuario. Se trata de un software portable que no requiere ninguna instalación en el sistema operativo.

Por sus características es una herramienta muy útil que se podría considerar una versión avanzada de Browser History Viewer, que se trata de una versión con menos funcionalidades que se limita a capturar el historial de navegación en su formato original para que pueda ser analizado posteriormente con otras herramientas externas. Este programa se puede usar de forma gratuita, pero no dispone de todas las funciones adicionales que tiene su versión mejorada cuyo uso está gestionado mediante una suscripción de pago. Entre las funciones extra que difieren de la versión gratuita destaca la captura de datos de forma remota, el uso de filtros y búsqueda avanzada o la recuperación del historial de navegación que ha sido borrado.

A pesar de que no se trata de una herramienta gratuita se ha elegido utilizarla ya que es una herramienta muy completa en cuanto a funciones y es superior a otras herramientas gratuitas ya disponibles, y al disponer de una versión de prueba se cuenta con tiempo más que de sobra para utilizarla de tal forma que cumpla su función extrayendo los datos que nos interesa recuperar y para poder hacer una valoración técnica del propio software como tal.

Con Browser History Examiner recuperaremos los datos almacenados en el navegador como por ejemplo el historial de búsqueda, datos de formularios, inicios de sesión, entre otros.

### 3.1.7 Autopsy

Autopsy [14] es un programa de software de código abierto utilizado en el ámbito del análisis forense digital. Este programa está basado en The Sleuth Kit que es una biblioteca forense digital y un conjunto de herramientas de línea de comandos. Autopsy proporciona una plataforma completa para examinar y analizar evidencias digitales en investigaciones forenses. Fue creada por Brian Carrier y hoy en día es mantenida por Basis Technology, además de los programadores de la comunidad de usuarios. Esta herramienta ha evolucionado a lo largo de los años para adaptarse a las necesidades cambiantes de los profesionales de la informática forense.

Autopsy ofrece una amplia gama de herramientas y características para ayudar en el proceso de análisis forense. Permite examinar imágenes de discos, sistemas de archivos y otros medios digitales para identificar y extraer datos relevantes. El programa puede recuperar y mostrar metadatos, realizar búsquedas de palabras clave, visualizar relaciones de archivos y generar informes de análisis detallados. Hablando a grandes rasgos Autopsy se podría definir como la interfaz gráfica de la biblioteca Sleuth Kit además de otras herramientas de análisis forense adicionales.

La principal ventaja de Autopsy es su interfaz de usuario intuitiva y fácil de usar, que facilita la navegación y el análisis de grandes volúmenes de datos. Además, cuenta con una amplia variedad de módulos complementarios que amplían su funcionalidad, como la capacidad de realizar análisis de memoria RAM, descodificación de contraseñas, etc. Estos módulos adicionales pueden ser propios y desarrollados por terceros.

Autopsy es compatible con múltiples sistemas operativos, incluyendo Windows, Linux y macOS, lo que lo convierte en una herramienta muy versátil. Al ser de código abierto permite a la comunidad de usuarios contribuir a aumentar las funcionalidades del programa, mejorar su funcionalidad y corregir posibles errores.

Se ha elegido Autopsy ya que es una herramienta muy completa que reúne muchas de las funcionalidades de otras herramientas vistas anteriormente, cuenta con una interfaz gráfica sencilla y amigable, y se trata de software gratuito listo para usar.

Esta herramienta nos va a permitir analizar un disco duro a fondo gracias a sus funcionalidades. Podremos explorar todos los datos recuperados como si de un explorador de archivos se tratase pudiendo analizar archivos sueltos, agrupados, recuperar archivos eliminados a partir de archivos residuales, entre otras funciones.

## **3.2 Creación del entorno de trabajo**

En este apartado se verá con cierto detalle el proceso de creación del entorno de laboratorio que será el entorno de trabajo en el que se desarrollará la fase de análisis. Posteriormente se describirán las herramientas empleadas para la creación del entorno, así como las empleadas para la obtención de las imágenes de disco de las máquinas originales que nos permitirán la virtualización completa de las máquinas físicas. El entorno virtual será el entorno de instalación de las herramientas software de análisis y extracción de datos que nos permitirán obtener las evidencias posteriormente.

### 3.2.1 Creación de un entorno de laboratorio basado en máquinas virtuales

La virtualización es la técnica informática que permite crear entornos de máquinas virtuales completos tanto la parte hardware como la parte software dentro de un sistema físico llamado host.

La virtualización de hardware se refiere a la creación de una capa de abstracción que permite que los recursos hardware de una máquina física sean compartidos por múltiples máquinas virtuales. En este enfoque, se utiliza un software llamado hipervisor o monitor de máquinas virtuales, que se instala en la máquina física y se encarga de gestionar y controlar las máquinas virtuales. El hipervisor se sitúa entre el hardware físico y las máquinas virtuales, asignando los recursos de hardware (CPU, memoria RAM, almacenamiento, tarjetas de red) de manera virtualizada a cada máquina virtual, lo que permite que funcionen de manera aislada y se ejecuten diferentes sistemas operativos y aplicaciones en cada una de ellas. Existen hipervisores de tipo 1 y de tipo 2:

- Tipo 1 (*Bare Metal*): Se ejecuta sobre el hardware físico y es la capa de virtualización entre el hardware y las máquinas virtuales.
- Tipo 2 (*Hosted*): Se ejecuta como un software instalado en un sistema operativo host, es decir, el de la máquina física, y requiere de este ya que el sistema operativo de esta máquina le proporciona recursos al hipervisor y a las máquinas virtuales.

La virtualización de software, por otro lado, se refiere a la creación de un entorno virtualizado dentro de un sistema operativo existente. En este enfoque, se utiliza un software de virtualización que crea una capa de abstracción y aísla las aplicaciones y los recursos de software en un entorno virtual. Esto permite ejecutar múltiples aplicaciones y sistemas operativos en el mismo sistema físico sin interferencias entre ellos.

Si juntamos ambos conceptos tenemos virtualizada una máquina al completo, como si se tratase de una máquina física, con sus recursos virtuales, pero que se comporta como una máquina real ya que puede hacer todo lo que esta es capaz de hacer.

Para construir el entorno de trabajo se ha escogido un hipervisor de tipo 2 para llevar a cabo esta tarea, ya que para este caso en concreto es justo lo que se necesita. Se ha escogido Oracle VM VirtualBox [15] ya que es un hipervisor que además de ser gratuito se trata de un software que he utilizado personalmente a lo largo de mis estudios en el grado y durante los cursos de virtualización que hemos recibido por parte de la empresa, además de que en estos cursos hemos utilizado Hyper-V de Microsoft y VMware Workstation, pero me he acabado decantando por la solución de Oracle por su sencillez y el uso común en ambos ámbitos, ya que tampoco es necesario disponer de un hipervisor muy sofisticado para la tarea que se llevará a cabo con este.

Se puede descargar desde la página web oficial y en el momento se encuentra en su versión 7.0 del programa.

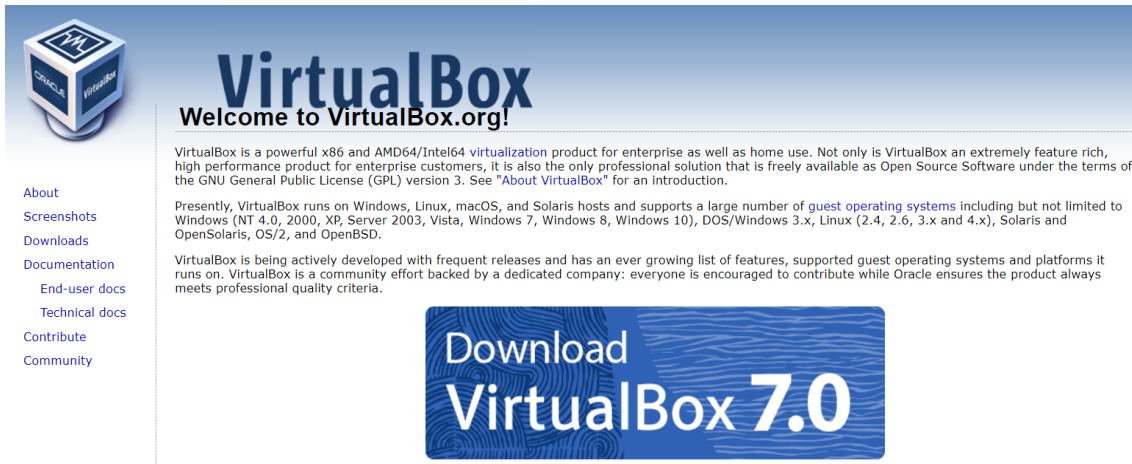


Ilustración 1: Página de descarga de VirtualBox

Una vez descargado e instalado este software procederemos a descargar las imágenes ISO de los sistemas operativos que instalaremos en las máquinas virtuales de nuestro entorno.

### 3.2.1.1 Descarga de imágenes ISO

Una imagen ISO de un sistema operativo es un archivo que contiene una copia exacta de todos los datos y archivos necesarios para instalar y configurar ese sistema operativo en un equipo (en este caso virtual). El formato ISO es un estándar que define una representación digital de un disco óptico, como un CD o un DVD. A pesar de que este tipo de dispositivos de almacenamiento están en desuso se trata de un formato de archivo que resulta muy útil en un entorno de virtualización, ya que estas imágenes ISO se montan directamente sobre las máquinas virtuales y dotan de sistema operativo a la máquina.

La obtención de las imágenes de los sistemas operativos se puede hacer mediante una descarga a través de internet, la cual llevaremos a cabo a través de los medios oficiales que nos proporcionan los desarrolladores de dichos sistemas operativos.

Para el caso de una ISO de cualquier distribución Linux podemos obtenerla desde la página web oficial. En este caso se ha elegido Ubuntu 22.04.2, que posteriormente se ha actualizado a la versión Ubuntu 23.04 tras su uso. En la Ilustración 2 se muestra la pantalla de descarga de Ubuntu Desktop [16].



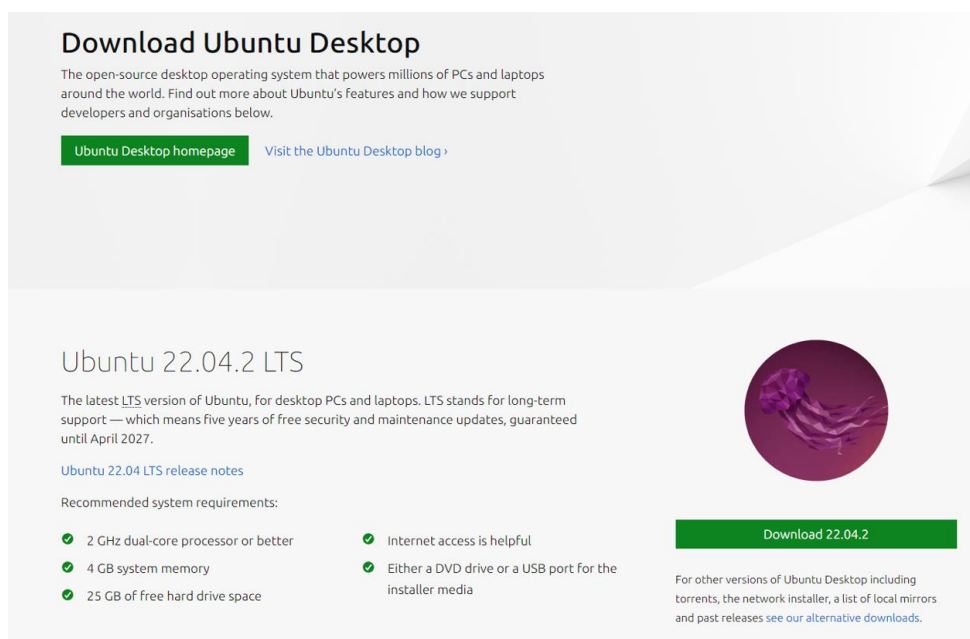


Ilustración 2: Página de descarga de ISO's de Ubuntu

Tan solo basta con descargar la imagen ISO directamente sin ninguna complicación.

Para obtener una imagen ISO de Windows 10 deberemos descargar una herramienta de creación de medios llamada MediaCreationTool, la cual nos puede crear un disco de arranque con la imagen del sistema o simplemente descargar la imagen original del sistema como un archivo ISO [17].

### ¿Estás deseando instalar Windows 10 en tu PC?

Para empezar necesitas tener una licencia para instalar Windows 10, y luego podrás descargar y ejecutar la herramienta de creación de medios. Para obtener más información sobre cómo utilizar la herramienta, consulta las instrucciones que se muestran abajo.

[Descargar ahora la herramienta](#)

Privacidad

[+](#) [Uso de la herramienta para actualizar el equipo a Windows 10 \(haz clic para mostrar más o menos información\)](#)

[+](#) [Uso de la herramienta para crear medios de instalación \(dispositivo de memoria USB, DVD o archivo ISO\) para instalar Windows 10 en un equipo distinto \(haz clic para mostrar más o menos información\)](#)



Ilustración 2: Página de descarga de la herramienta MediaCreationTool de Microsoft

Al ejecutar esta herramienta hay que seleccionar ciertas opciones para obtener la imagen ISO del sistema como un archivo separado. Se escoge la opción de crear medios de instalación para que la herramienta descargue la imagen del sistema en nuestro sistema.

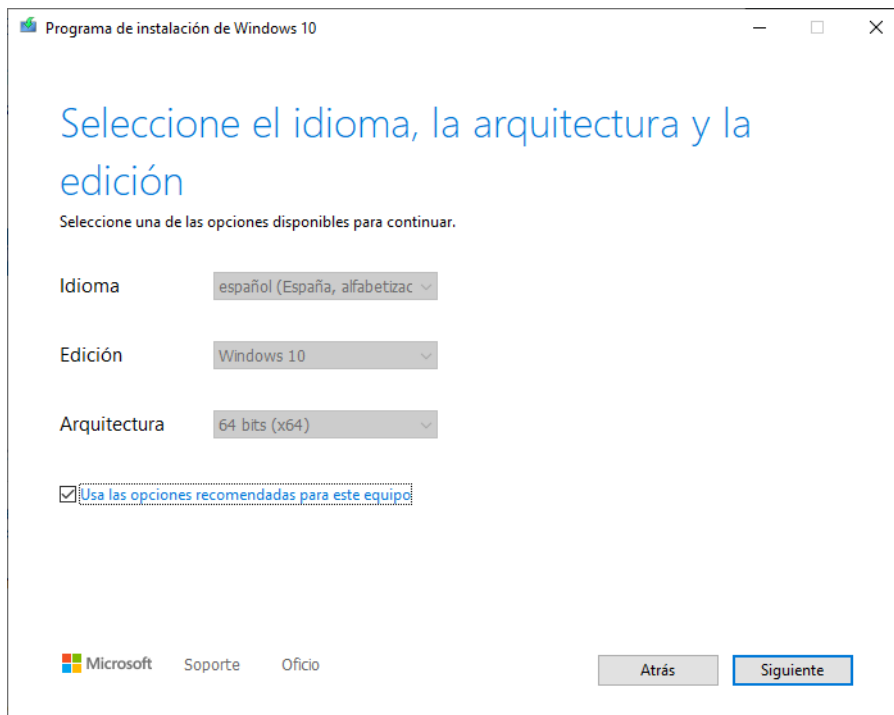


Ilustración 3: Pantalla inicial de MediaCreationTool

Se seleccionan las características del sistema operativo del que queremos descargar la imagen ISO.

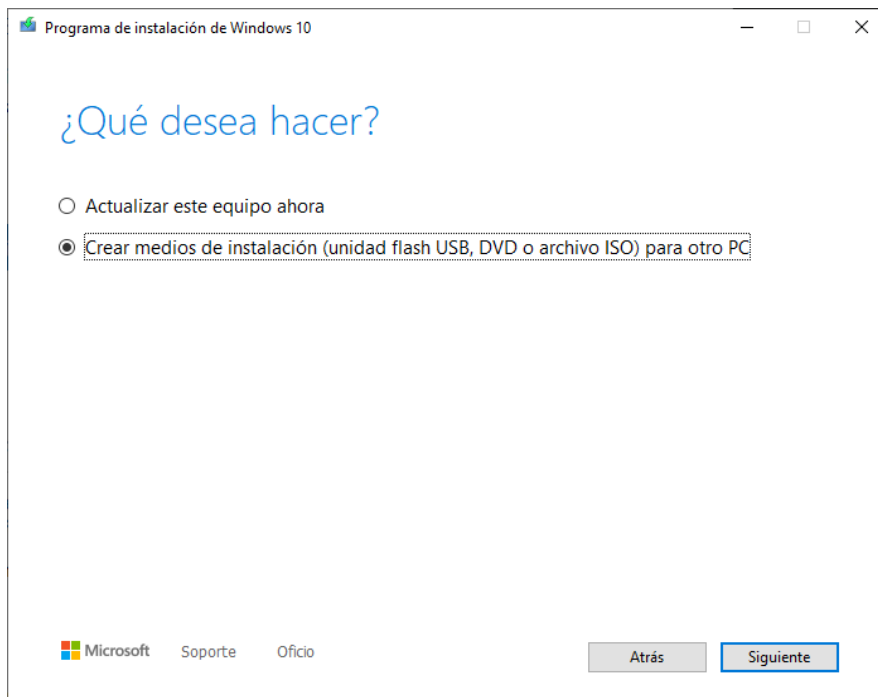


Ilustración 4: Selección de idioma de descarga

Finalmente seleccionamos el medio de instalación que utilizaremos, que en nuestro caso será un archivo ISO.





Ilustración 5: Selección de medio de almacenamiento

Tras estos pasos comienza la descarga del archivo:

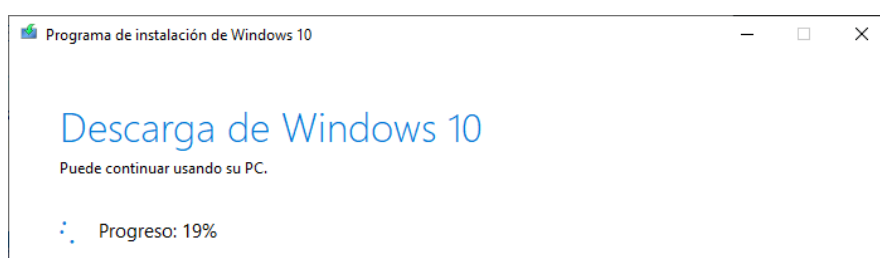


Ilustración 6: Descarga de la ISO de Microsoft Windows

Una vez tengamos descargadas las imágenes del sistema podemos montar el entorno de trabajo de máquinas virtuales en VirtualBox.

### 3.2.1.2 Creación de máquinas virtuales, asignación de recursos e instalación del sistema operativo

Una vez dispongamos de la instalación de VirtualBox y de las imágenes de disco ya descargadas podemos crear las máquinas virtuales que utilizaremos a lo largo del desarrollo del trabajo.

Dentro de VirtualBox crearemos una máquina virtual desde sus cimientos escogiendo la opción de “Nueva”.



Ilustración 7: Ventana de inicio de VirtualBox

Escogemos un nombre para la máquina, la ruta de instalación y la imagen ISO del sistema operativo.

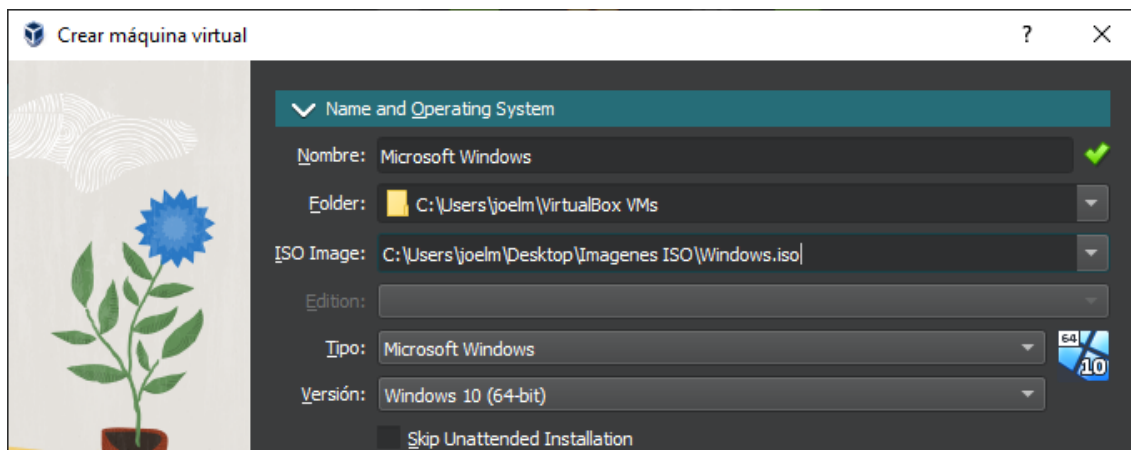


Ilustración 8: Creación de máquina virtual

En la ilustración 9 creamos un usuario por defecto llamado “user” y le damos una contraseña. Elegimos de nombre de host “Microsoft-Windows”.

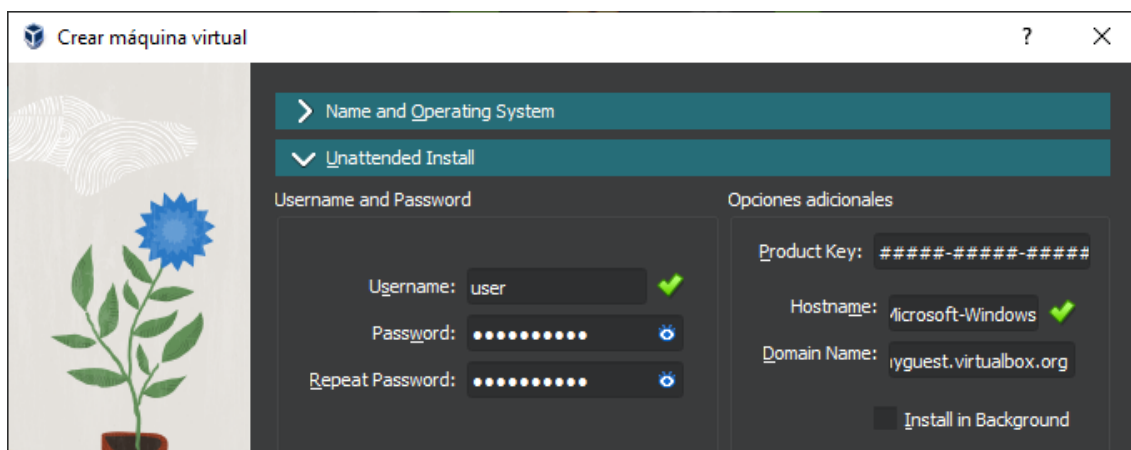


Ilustración 9: Creación de usuario por defecto

En el apartado de recursos le asignaremos 4GB de memoria RAM y 4 procesadores lógicos.

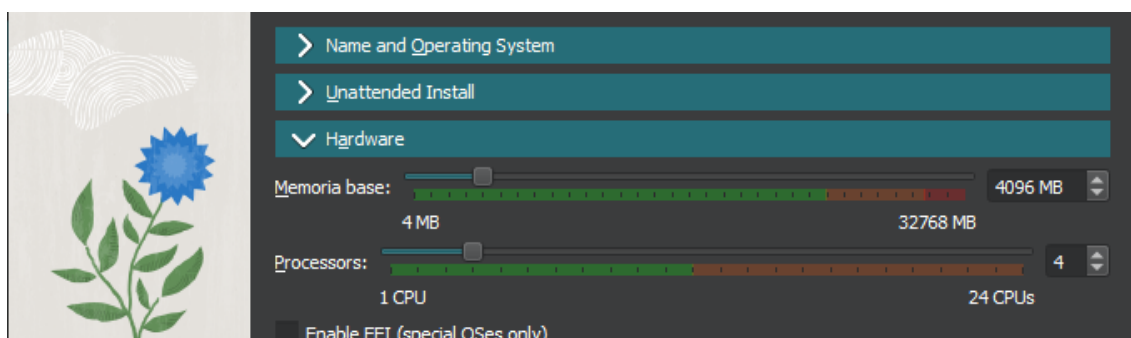


Ilustración 10: Asignación de recursos a la máquina virtual

Creamos un disco virtual que servirá de disco de arranque para el sistema operativo además de almacenar todo el software dedicado al análisis y recuperación de archivos que será instalado posteriormente.

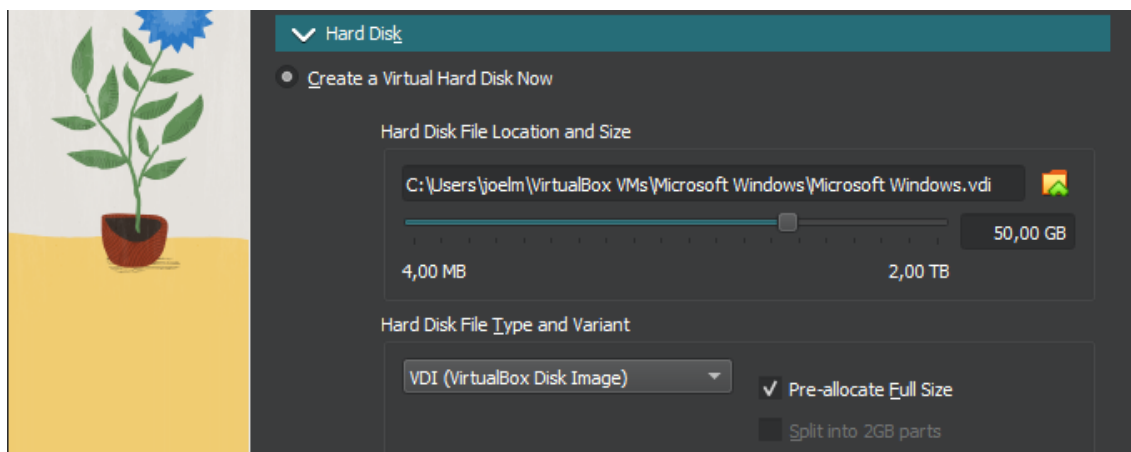


Ilustración 11: Creación de disco virtual

Escogemos un tamaño de 50GB, el formato de disco virtual VDI (*VirtualBox Disk Image*) desarrollado por VirtualBox. Marcamos la opción “Pre-allocate Full Size” para que el tamaño del disco virtual sea asignado desde el principio en el almacenamiento físico de la máquina host y que no crezca de forma dinámica hasta llegar a su capacidad máxima conforme vayamos instalando programas o se almacenen archivos en el disco.

Se ha decidido proporcionar recursos superiores a los requisitos mínimos a las máquinas virtuales ya que de esta forma se garantiza un buen funcionamiento de estas. En mi caso personal dispongo de un equipo con la capacidad de recursos suficiente como para que esta decisión no suponga un problema de rendimiento.

De esta forma crearemos una máquina virtual con Windows 10 como sistema operativo host. No hace falta detallar el mismo procedimiento con la otra máquina virtual con Linux como sistema operativo host ya que se trata de un proceso análogo a este. Por simplicidad se le han otorgado los mismos recursos salvo por el almacenamiento, que será de 25GB por ser más que suficiente para cumplir con los requisitos mínimos del sistema.

A estas alturas ya disponemos del entorno de laboratorio montado sobre el que se llevará a cabo todo procedimiento relacionado con el análisis forense, pero para eso tendremos que preservar la información de alguna forma para poder almacenarla en las máquinas virtuales donde podremos analizarla a fondo.

### 3.2.2 Creación de imagen de disco virtual a partir de disco duro físico

Una vez tenemos el entorno de laboratorio montado tan solo nos haría falta disponer de la información que vamos a necesitar para nuestro análisis. Como debería de ser lógico, no realizaremos el análisis de los datos sobre la misma máquina que es objeto de investigación, sino que aseguraremos estos datos y los analizaremos en el entorno virtual aislado de toda posible modificación externa. Una forma de abarcar toda la información de un sistema es la de clonar su almacenamiento para traspassarlo a otra máquina diferente para que ahí sea analizado. Para lograr ese objetivo nos

serviremos de algún software que se encargue de esta tarea, que consiste en crear una copia del disco duro físico en un formato de archivo de disco virtual.

Una imagen de disco virtual es un archivo que representa una copia exacta o una representación virtual de un disco físico o de una partición de almacenamiento. Esta imagen contiene todos los datos y la estructura del disco original, es decir, es una representación digital del disco duro virtual de una máquina virtual, que puede ser utilizado para crear y configurar nuevas máquinas virtuales con la misma configuración que la original.

Aquí es donde empieza la fase de preservación de datos en el análisis forense. El objetivo es obtener una imagen de disco virtual de la máquina física como si de un clon se tratase, y posteriormente montarlo en la máquina virtual para analizarlo.

### 3.2.2.1 Creación de imagen de disco virtual en Windows

Para llevar a cabo esta tarea emplearemos una herramienta famosísima para la creación de imágenes de disco que luego podremos montar en un entorno virtual. Se trata de la herramienta `Disk2vhd` [18] proporcionada por Sysinternals que forma parte de Microsoft y fue desarrollada por Mark Russinovich.

`Disk2vhd` es una herramienta gratuita que permite crear imágenes de disco virtual (VHD y VHDX) a partir de discos duros físicos o particiones de un sistema en ejecución. La herramienta permite virtualizar un disco o una partición completa, incluyendo los archivos almacenados en él. Esta herramienta es útil para realizar la migración de un sistema físico a una máquina virtual, lo que facilita la transición de un entorno físico a uno virtual sin tener que realizar una instalación desde cero. También es útil para realizar copias de seguridad de sistemas en ejecución y crear instantáneas virtuales de un estado particular del sistema.

La herramienta `Disk2vhd` permite seleccionar las unidades o particiones que se desean convertir en imágenes de disco virtual, y proporciona opciones para especificar el nombre del archivo VHD resultante, la ubicación de almacenamiento y el tamaño máximo del archivo VHD. Una vez que se completa el proceso, se obtiene un archivo VHD que puede ser utilizado por diferentes plataformas de virtualización que soporten el formato, como es el caso de nuestro elegido `VirtualBox`, para crear una máquina virtual con la configuración y los datos originales.

Es importante destacar que `Disk2vhd` se ejecuta en el sistema que se va a convertir, por lo que no se puede utilizar para crear imágenes de disco virtual de sistemas operativos en ejecución en otros equipos o máquinas virtuales. Además, es recomendable realizar una copia de seguridad completa del sistema antes de utilizar la herramienta para evitar la pérdida de datos.

Se ha escogido esta herramienta porque se trata de una herramienta muy potente y fácil de usar, además de ser gratuita y distribuida por Microsoft. En la Ilustración 12 se muestra la ventana principal del programa.

La interfaz de la herramienta es muy sencilla, ya que tan solo debemos seleccionar el formato de imagen, ruta y nombre del archivo que se generará y las unidades de disco que se copiarán.

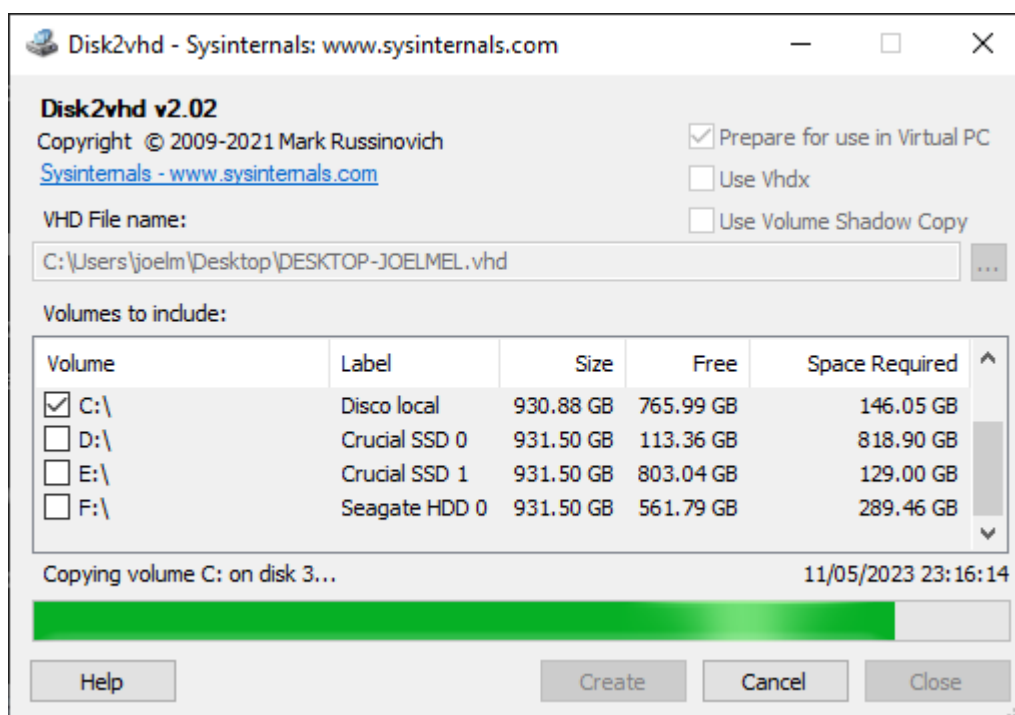


Ilustración 12: Creación de imagen de disco virtual con Disk2vhd

Cuando se termina de ejecutar obtendremos un archivo de disco virtual en formato VHD que podremos montar sobre la máquina virtual para su posterior análisis. De esta forma obtenemos una copia completa del disco duro físico sin alterar su contenido, y como disponemos de una copia del disco podemos hacer todo tipo de pruebas con él, ya que en el caso de que nos equivoquemos siempre conservaremos la imagen original.

### 3.2.2.2 Creación de imagen de disco virtual en Linux

Para crear una imagen de disco virtual en una distribución Linux no lo vamos a tener tan fácil como en el caso de Windows. Disponemos de varias herramientas que cumplen con esta función, pero emplearemos una combinación de dos herramientas para cumplir con este propósito. Se trata de Data Duplicator (dd) [19] y qemu-img [20].

Entre todas las opciones de las que disponemos en Linux se ha escogido dd, ya que la dificultad de uso es bastante inferior en comparación con otras herramientas más famosas como Clonezilla que se trata de un software libre muy potente pero complicado de usar, y a pesar de ser una herramienta de línea de comandos no tiene una sintaxis demasiado complicada, además de que viene preinstalada en la mayoría de distribuciones Linux como es en nuestro caso y por lo tanto no requiere de un esfuerzo extra para poder utilizarla.

En cuanto a la elección de qemu-img se ha escogido por ser justo la herramienta de conversión que necesitamos para convertir el archivo de imagen que hemos generado con dd.

La herramienta `dd` se trata de una utilidad de línea de comandos muy versátil que se utiliza para copiar y convertir archivos o dispositivos, además de servir como un método de copia de seguridad. Es capaz de realizar una copia de dispositivos físicos como puede ser un disco duro, que es justamente la funcionalidad que nos interesa para generar una imagen de disco.

La herramienta `qemu-img` también es una herramienta de consola que permite crear, convertir y administrar imágenes de disco para su uso con QEMU y otros programas de virtualización compatibles como es el caso de VirtualBox. La funcionalidad que nos interesa es la de la conversión de archivos de imagen, ya que deberemos de convertir un archivo en formato IMG a formato VHD para poder montar la imagen de disco en la máquina virtual del laboratorio.

Primero crearemos la imagen de disco con `dd`, para ello desde un terminal ejecutaremos el siguiente comando:

```
sudo dd if=/dev/sda of=/home/user/imagen.img bs=4M
```

Su ejecución nos creará una imagen de disco `imagen.img` a partir del disco duro físico `/dev/sda` con un tamaño de bloque de 4 megabytes.

Para convertir el archivo `imagen.img` al formato deseado ejecutaremos la herramienta `qemu-img`. Para instalar la herramienta ejecutamos el siguiente comando:

```
sudo apt-get install qemu-utils
```

Para realizar la conversión del archivo al formato correspondiente ejecutamos el siguiente comando:

```
qemu-img convert -O vpc /home/user/imagen.img /home/user/disco.vhd
```

Tras su ejecución se habrá generado un archivo en formato `.vhd` a partir de la imagen creada anteriormente y que ahora podemos utilizar en nuestro laboratorio virtualizado.

### 3.2.2.3 Montar disco virtual en la máquina virtual

Una vez disponemos de los archivos de disco virtual podemos montarlos sobre una máquina virtual como si de un disco físico se tratase. Para ello iremos a las propiedades de la máquina que hemos creado en VirtualBox.

En la Ilustración 13 se muestran las propiedades de la máquina virtual. Dentro de la pestaña de “Almacenamiento” veremos los dispositivos de almacenamiento de la máquina virtual. Seleccionaremos el controlador SATA y añadiremos el disco.

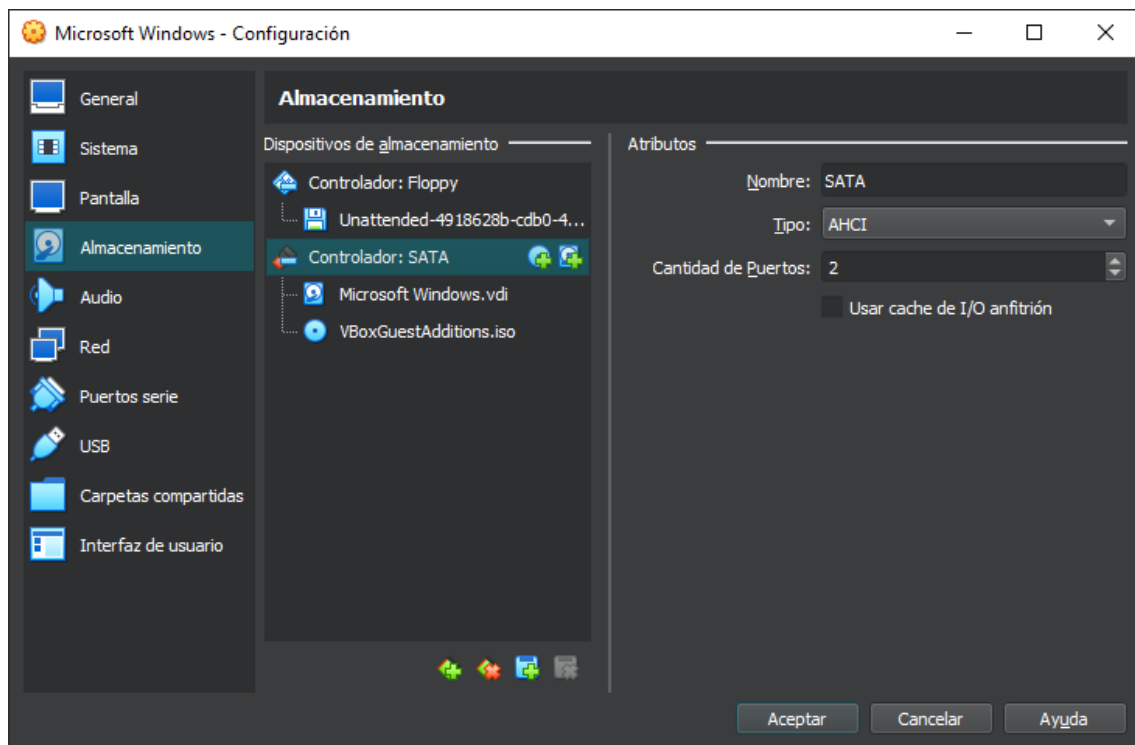


Ilustración 13: Propiedades de la máquina virtual

Una vez estemos en el selector de disco duro añadiremos el disco virtual que hemos generado a partir del dispositivo físico. Mediante el botón “Añadir” representado por un disco duro con el símbolo “+” se nos abrirá la ventana que muestra la ilustración 14. Una vez dentro desde la opción de “Añadir” se nos abrirá una ventana en el explorador que nos permite la selección de archivos y escogeremos el disco duro virtual que hemos creado en el apartado anterior para agregarlo a las propiedades de la máquina.

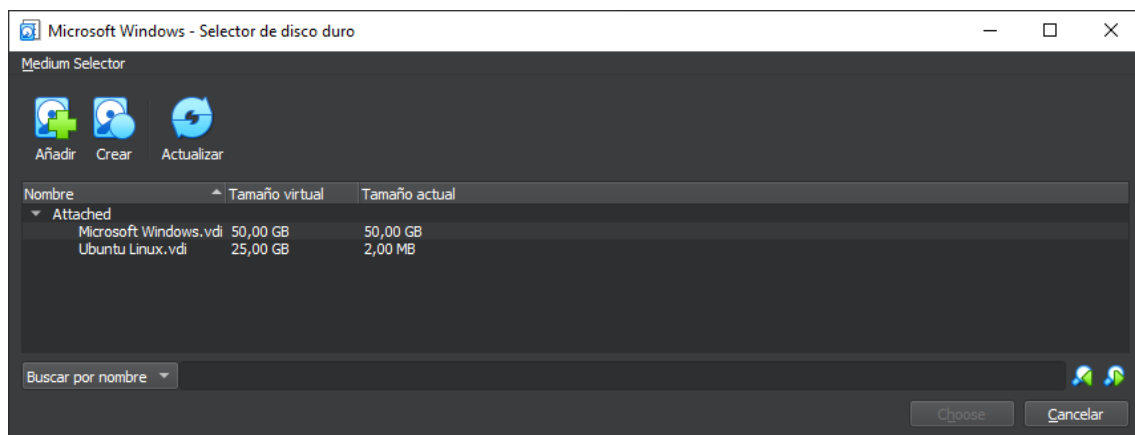


Ilustración 14: Añadir disco duro a máquina virtual

Una vez se selecciona aparece reflejado en las propiedades de almacenamiento como podemos apreciar en la Ilustración 15.

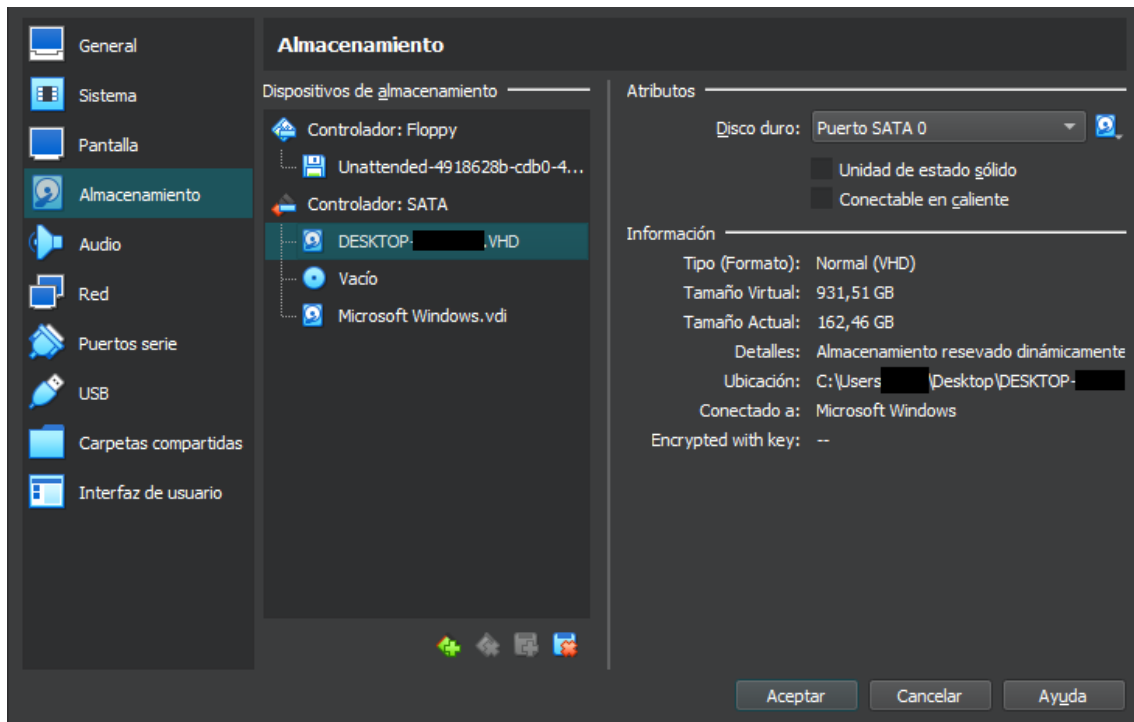


Ilustración 15: Disco virtual añadido en las propiedades de la máquina virtual

De esta forma hemos montado un disco virtual en una máquina virtual que ya está listo para su uso. Finalmente cambiaremos la ubicación del puerto SATA al puerto 0 ya que este se trata del puerto principal del sistema y el de mayor prioridad en el arranque del sistema.

Una vez hecho esto nos dirigimos a la configuración de la máquina y en el apartado de “Sistema” seleccionamos el orden de arranque de los dispositivos se utilizará el disco duro que hemos añadido como disco duro de arranque del sistema, con lo que habremos virtualizado por completo la máquina física que será objeto de análisis.

La BIOS virtual de la máquina iniciará el sistema empezando por el dispositivo que tenga mayor orden de prioridad en la lista, que en este caso es el disco duro que se encuentra en la parte superior como podemos observar en la Ilustración 16 tras configurarlo de esta manera:

En el caso de que no sea suficiente esta configuración pulsaremos la tecla F12 para seleccionar temporalmente el dispositivo de arranque del sistema durante el arranque de la máquina virtual. Nos aparecerá la ventana que se observa en la Ilustración 17.



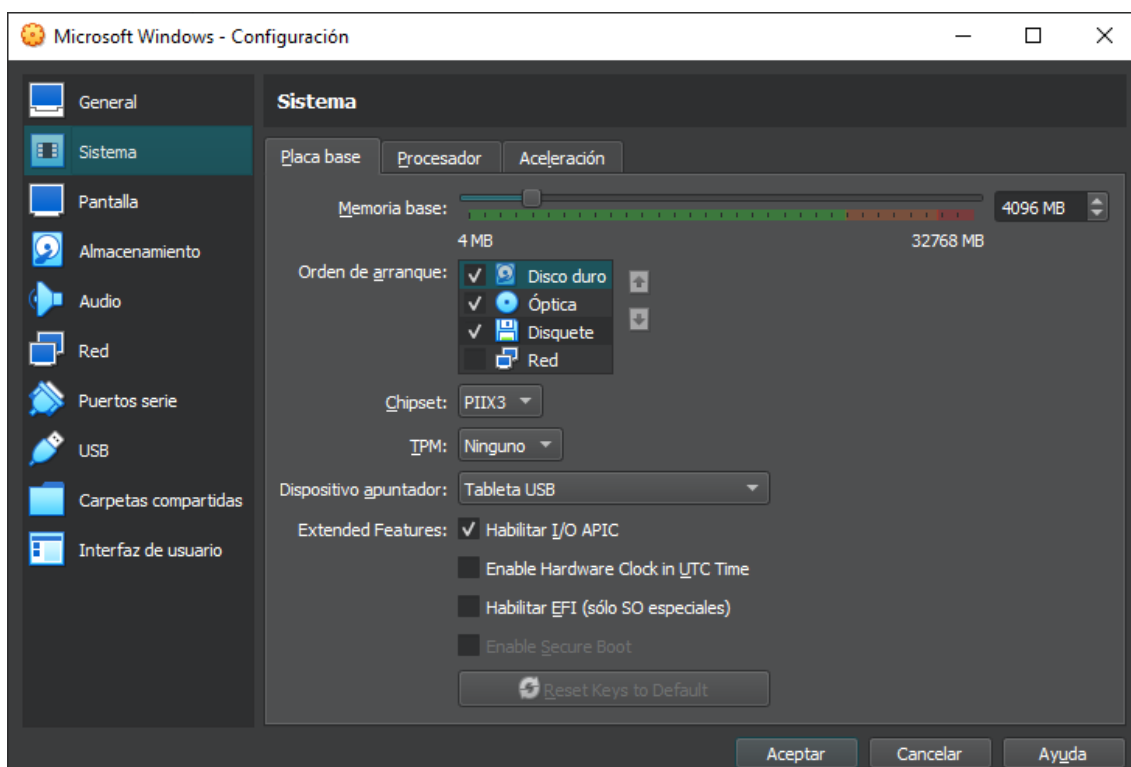
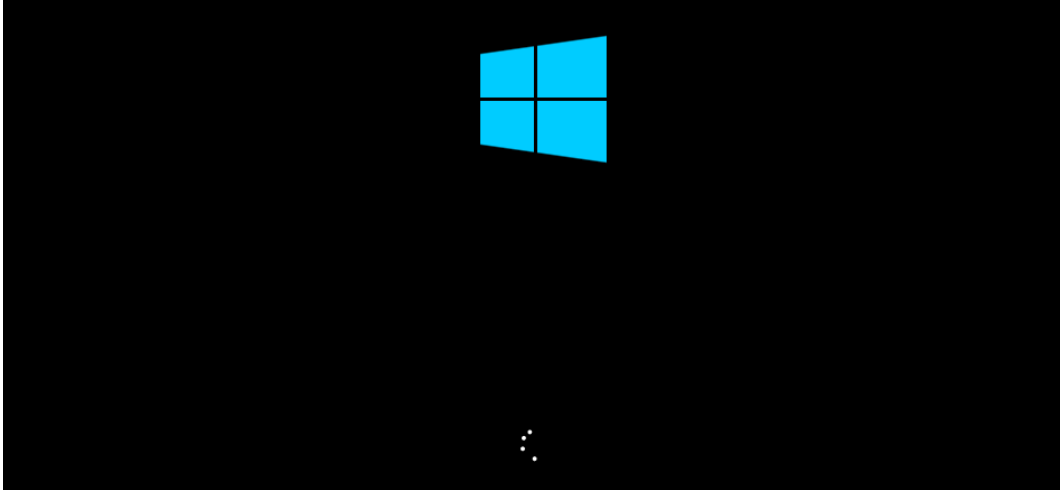


Ilustración 16: Orden de arranque de los dispositivos de la máquina



Ilustración 17: Selección del dispositivo de arranque

Seleccionaremos el disco primer disco duro con el teclado pulsando la tecla numérica correspondiente. Una vez seleccionemos el dispositivo de arranque el sistema cargará como muestra la Ilustración 17.



*Ilustración 18: Arranque del sistema Windows en la máquina virtual*

No es necesario mostrar cómo se añade el disco virtual a la máquina Linux porque el proceso es análogo al que se ha mostrado en este apartado.

### 3.2.3 Descripción final del entorno de trabajo

Tras montar el entorno de trabajo con máquinas virtuales hemos logrado aislar la máquina física en una máquina virtual, por lo que con esto disponemos de una copia exacta de la máquina física y disponemos de una copia de seguridad de esta en formato de disco virtual, por lo que no solamente dejamos la máquina original intacta, sino que además hemos preservado una imagen de la máquina con la que podemos empezar a trabajar en el entorno virtual.

Es ahora cuando nos debemos de encargar de instalar todas las herramientas que vayamos a utilizar en nuestras máquinas virtuales. Estas herramientas podrían ser instaladas en las máquinas *host* o físicas, y también en las máquinas *guest* o máquinas virtuales. La elección de instalar estos programas en las máquinas virtuales ha sido para poder emplear todas las herramientas de la misma manera, que es como si se ejecutasen sobre la máquina física, pero en este caso estamos aislando la máquina virtualmente y podemos trabajar directamente sobre ella sin alterar la original manteniendo la integridad de los datos.

El diagrama muestra la organización del entorno de trabajo, siendo una máquina física el objeto a estudiar, de la cual obtenemos una imagen de disco virtual con el fin de crear una copia exacta de la máquina. Esta imagen de disco virtual podemos montarla en máquinas virtuales las cuales irán virtualizadas dentro de otro sistema huésped y serán gestionadas y utilizadas mediante un hipervisor de tipo 2:

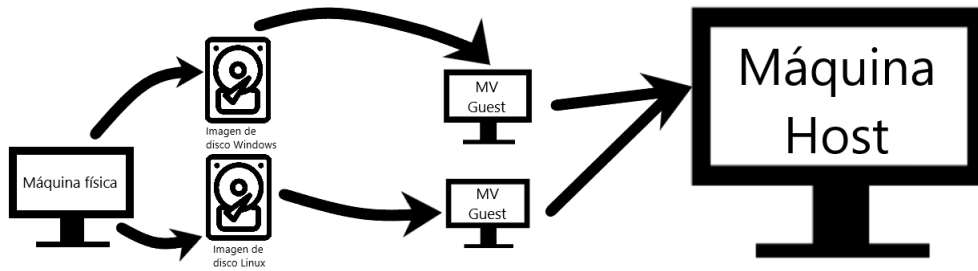


Ilustración 19: Diagrama del entorno de trabajo

La instalación de las herramientas no requiere de ningún procedimiento especial, ya que tanto en Windows como en Linux estas se pueden obtener directamente de sus respectivas páginas web de descarga (y en el caso de Linux podemos recurrir al comando `apt get` y el nombre del programa que queramos instalar y el sistema los descargará de la fuente de repositorios de la que dispone) y se ejecutarán los correspondientes instaladores. El único programa que sí que depende de librerías externas se trata de Volatility, que tanto en Linux como en Windows necesita la instalación de las librerías de Python [21] de la misma manera que se menciona anteriormente, ya sea por descarga directa del instalador o por la obtención de paquetes de los repositorios oficiales.

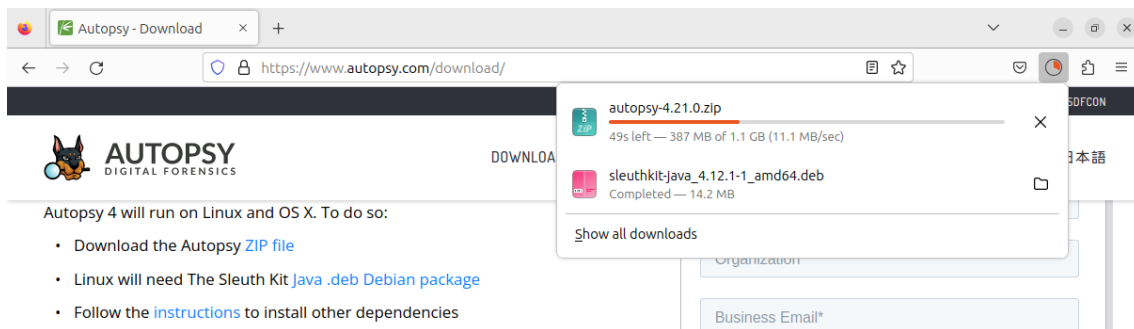


Ilustración 20: Descarga de Autopsy en Linux

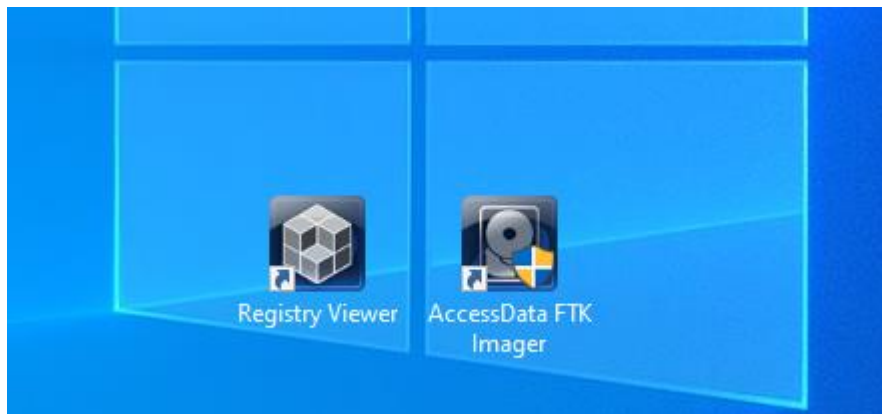


Ilustración 21: Registry Viewer y FTK Imager instalados en Windows

## 4. Fuentes de información digital

---

En este capítulo se expondrán y se describirán las principales fuentes de información de un sistema informático y veremos los tipos de información que almacenan cada una de ellas.

### 4.1 Fuentes de información digital en un sistema informático

En un sistema informático se almacena una gran cantidad de información de muchos tipos que puede ser empleada para obtener información muy valiosa a la hora de realizar una investigación forense. Un sistema operativo está compuesto por diversos elementos básicos que permiten su gestión y funcionamiento como pueden ser *kernel*, gestor de memoria, gestor de procesos, sistema de archivos, interfaz de usuario, controladores de dispositivos, servicios, aplicaciones, y un largo etcétera. Podríamos asegurar que la gran mayoría de estas características están presentes en todos los sistemas operativos, pero lo que no podemos asegurar con certeza es que a pesar de que sean comunes a todos sean exactamente iguales en diferentes sistemas operativos. Cada sistema operativo tiene una arquitectura y una forma diferente de organización a pesar de que sea posible que se compartan características con otros sistemas. No obstante, aunque parezca que estamos ante algo exactamente igual su lógica interna puede ser completamente diferente de un caso a otro.

Dependiendo de la arquitectura del sistema operativo los datos estarán estructurados de una forma u otra, además de que sus fuentes de información pueden variar en cantidad, tipo de datos que contengan o incluso en formato. Cada sistema operativo puede soportar unos formatos de archivo distintos a pesar de que hay muchos formatos soportados por la mayoría de los sistemas operativos que podríamos considerar comunes como pueden ser archivos multimedia (imágenes, archivos de audio, vídeos), archivos de texto (texto plano, scripts, archivos de configuración), documentos de texto, archivos comprimidos, archivos ejecutables, archivos de navegación web, etc.

Siendo conscientes de la cantidad de archivos que puede albergar un sistema informático podemos recopilar una cantidad inmensa de información según aquello que nos interese investigar. Cabe mencionar que no todas las fuentes de información son igual de fáciles o cómodas de consultar y esto dependerá del tipo de archivo, de la fuente en sí y de la arquitectura y la seguridad del sistema operativo, ya que si se trata de un sistema que restringe mucho la información según políticas de seguridad del sistema o según los permisos del usuario puede dificultar la tarea de extraer esta información. Esto es un impedimento que dificulta la tarea de investigación, pero no impide recuperar los archivos si se emplean técnicas para vulnerar estas medidas de seguridad propias del sistema, pero para ello es necesario tener conocimientos del sistema operativo que será analizado además de conocer sus errores, vulnerabilidades, modificaciones que podamos hacer al sistema y disponer de las

herramientas que sean necesarias para realizar estas tareas. Entre las más comunes se encuentran las de elevación de privilegios de usuario para acceder a datos restringidos según los permisos asignados.

Un caso práctico podría ser el siguiente: Queremos recuperar las imágenes que se envían y se reciben por WhatsApp mediante un teléfono Android, pero se trata de las imágenes que solamente pueden visualizarse una vez. WhatsApp dispone de una función que permite enviar fotos y vídeos para que sean visualizados una única vez, y una vez el usuario salga de la visualización no podrá volver a ver el archivo multimedia que le ha sido compartido, al igual que si el usuario envía otro archivo multimedia. Estos archivos se almacenan dentro de una carpeta de los datos de la aplicación, pero esta no es accesible a simple vista, sino que se requieren permisos de superusuario para poder acceder a esta carpeta para así recuperar los archivos. Para ello hay que conseguir los permisos del usuario *root*, y una vez los obtengamos se podrá visualizar la carpeta y los archivos contenidos en ella. Cabe destacar que para poder obtener estos privilegios de usuario debemos previamente desbloquear el gestor de arranque o *bootloader*, pero esta acción implica un formateo del dispositivo haciendo que se pierdan todos los archivos almacenados incluidos los archivos multimedia que queríamos recuperar.

Podríamos considerar que el bloqueo del gestor de arranque es una medida de seguridad para el sistema Android (al igual que para otros sistemas), y por eso viene bloqueado de serie en todos los teléfonos inteligentes. De esta forma dificultan que un usuario pueda modificar el terminal y su sistema y que no pueda acceder a los archivos del sistema o realice acciones que dejen el teléfono inservible.

Si lo consideramos una medida de seguridad para proteger la privacidad de los datos compartidos en una aplicación de mensajería cumple con su propósito, ya que si pretendemos recuperar esos datos en concreto no vamos a poder hacerlo, ya que si desbloqueamos el gestor de arranque toda la información se perderá, pero esto no impide que una vez se desbloquee el gestor de arranque y se obtengan permisos de superusuario podamos recuperar sin ningún esfuerzo adicional cualquier archivo multimedia que nos envíen para poder verlo una única vez de ahora en adelante. Esto frustra el intento de recuperar la información que se requiere en el momento ya que un usuario normal no requiere de permisos de superusuario para emplear el teléfono en el día a día, y de nada sirve recuperar los archivos de ahora en adelante porque ya no son objeto de investigación.

Dejando atrás este ejemplo anecdótico, se podría dar algún caso diferente en otro sistema operativo que nos lleve a realizar un esfuerzo extra para poder recuperar la información de ciertas fuentes.

A continuación, se exponen las principales fuentes de información que se encuentran en un sistema operativo según su importancia para obtener hallazgos de la huella digital de un usuario:

## 4.2 Discos duros

Estos dispositivos de almacenamiento son la forma más común de almacenamiento de datos a largo plazo en un sistema informático y nos referimos a ellos como la memoria secundaria de un ordenador. Estos pueden tener distintos formatos de forma y velocidades de transferencia de datos. Habitualmente se emplean

los discos duros magnéticos (HDD, *Hard Disk Drive*) para almacenar datos a largo plazo, pero también existen las unidades de estado sólido (SSD, *Solid State Drive*) que son más rápidos ya que almacenan los datos en microchips con memorias flash interconectadas haciendo que la transferencia de archivos sea mucho más rápida. Pueden tener distintos formatos de sistema de archivos, aunque el más común es FAT (*File Allocation Table*, tabla de asignación de archivos), o sus variantes como FAT32 o exFAT. También existe algún formato de sistema de archivos propio de los sistemas operativos como NTFS (*New Technology File System*) propio del sistema operativo Windows o bien ext4 (*Fourth Extended File System*) propio del sistema operativo Linux. Estos formatos proporcionan características adicionales como seguridad, compresión de archivos, nombres de archivo más largos, mayores tamaños de archivo o rendimiento mejorado. Estos dispositivos almacenan una gran variedad de datos según el propósito para el que se destine el disco. Estos pueden contener el propio sistema operativo si el disco se ha destinado a ese uso, aplicaciones y programas, documentos de los usuarios, copias de seguridad, etc. Estos dispositivos pueden copiarse bit a bit para crear una copia exacta de los archivos que contenía el disco original y destinar esta copia para realizar la investigación forense. También se puede crear una imagen virtual del disco en cuestión y analizarlo directamente como si de un archivo se tratase, pudiendo analizarse directamente con ciertos programas que soporten el formato de los discos virtuales o bien montar el disco virtual en una máquina virtual como si se tratase de un dispositivo de almacenamiento físico.

### 4.3 Memoria RAM

La memoria de acceso aleatorio (RAM, *Random Access Memory*) es una forma de memoria volátil que almacena datos temporalmente mientras el sistema está en funcionamiento, perdiéndose una vez el sistema se apaga ya que para que los datos sean persistentes en la memoria debe de recibir alimentación eléctrica. Es un elemento hardware necesario para un ordenador y es crucial para el rendimiento del sistema, siendo conocida como memoria principal en un ordenador. Hay varios tipos de memoria RAM, aunque el tipo más habitual es DDR SDRAM (*Double Data Rate Synchronous Dynamic Random Access Memory*), el cual ya va por la quinta generación (DDR5), aunque por el momento DDR4 es el más usado en la gran mayoría de ordenadores de sobremesa hoy en día por precio frente a la nueva generación y compatibilidad con la mayoría de las placas base. También hay diferentes formatos físicos de memoria RAM como DIMM (*Dual In-Line Memory Module*) que es el más usado en ordenadores de escritorio y servidores o SODIMM (*Small Outline DIMM*) que son módulos más pequeños que los DIMM estándar y son empleados en dispositivos más pequeños como portátiles. Este tipo de memoria se comunica con la CPU (Unidad Central de Proceso) o procesador de la máquina. En la memoria RAM se almacenan los datos de forma temporal como el sistema operativo o los programas, para que la CPU pueda acceder rápidamente a su contenido. Estas memorias son mucho más rápidas que los dispositivos de almacenamiento, ya que su tecnología es diferente para proporcionar un tiempo de acceso y una velocidad de transferencia superiores ya que es capaz de acceder a cualquier ubicación de la memoria en un tiempo constante sin importar la ubicación física de los datos requeridos. Algunos de los datos más comunes almacenados por la RAM son programas en ejecución, sistema operativo, caché o controladores de dispositivo. Se puede hacer un volcado de memoria para analizar el contenido de esta mientras el sistema esté en funcionamiento.

## 4.4 Registros del sistema

También conocidos como archivos del sistema o logs del sistema son los archivos que registran eventos y actividades del sistema operativo y contienen información acerca del sistema, las aplicaciones, componentes hardware, etc. Estos pueden variar en estructura y contenido según el sistema operativo, pero la finalidad de estos es la misma. Estos registros almacenan datos como registros de eventos como inicio, apagado o reinicio del sistema, cambios en la configuración del sistema, fallos de hardware, errores del sistema, inicio y cierre de sesión de usuarios, cambios de permisos, intentos de sesión fallidos, inicio y cierre de aplicaciones o accesos a archivos y directorios como accesos, modificaciones y eliminaciones. Estos registros se pueden analizar filtrando por eventos con el fin de identificar patrones y ver si hay correlación entre los eventos.

## 4.5 Navegadores web

Son las aplicaciones software que permiten acceder a páginas web en internet. Para facilitar la navegación y mejorar el rendimiento hay algunos datos que son recopilados por los navegadores de forma automática como son el historial de navegación que recopila todos los sitios web a los que se ha accedido mediante el uso del navegador, las cookies de los sitios visitados que contiene información del usuario como preferencias, información de inicio de sesión o datos de seguimiento, la caché del navegador que se almacena temporalmente de las imágenes, hojas de estilo CSS y scripts de los sitios web visitados. Estos datos se almacenan automáticamente para mejorar la experiencia de navegación ya que de esta forma se almacenan las preferencias del usuario en el archivo de las cookies y los datos de las páginas web en la caché del navegador haciendo que no sea necesario volver a descargar estos datos del servidor que aloja el sitio web ya que estos se pueden recuperar localmente. Hay otros tipos de datos que se almacenan en el navegador, pero estos no se almacenan automáticamente y depende de la elección del usuario. Estos datos son contraseñas, formularios y marcadores del navegador. Algunos usuarios pueden considerar útil guardar sus contraseñas o los datos personales introducidos en formularios web para no tener que escribirlos nuevamente o no tener que acordarse de memoria, al igual que con los marcadores que permiten guardar las direcciones de los sitios web para acceder rápidamente a ellos en el futuro. Además de estos datos los navegadores también pueden almacenar información de las extensiones instaladas, configuración del navegador o descargas de sitios web. Todos estos datos pueden ser extraídos del navegador para su posterior análisis.

## 4.6 Metadatos de archivos

Los metadatos son información adicional acerca de los datos y los dota de contexto, ya que describen características, propiedades o atributos de archivos ya existentes. Estos se emplean para facilitar la organización, identificación y búsqueda

de archivos. Algunos ejemplos de datos recopilados pueden ser descripción del archivo, autoría, fecha y hora de creación y modificación, formato y tipo de archivo, ubicación geográfica como dirección o datos GPS, tamaño y resolución de archivos multimedia, información de la cámara y configuración, historial de cambios en documentos o etiquetas empleadas para su clasificación. Los metadatos desempeñan un papel importante en la gestión de información y en la organización eficiente de grandes volúmenes de datos. Permiten que los datos sean identificados, descubiertos y utilizados de manera más efectiva, facilitando su búsqueda, recuperación y uso apropiado. Además, los metadatos pueden ser utilizados por sistemas informáticos y aplicaciones para proporcionar funcionalidades adicionales, como la clasificación automática o la búsqueda avanzada de recursos digitales. Los tipos de información que se almacenan en los metadatos son muy diversos y pueden proporcionar información muy valiosa a la hora de realizar un análisis de un archivo facilitando incluso la obtención de nueva información a partir de sus metadatos con simples búsquedas en internet.

## **4.7 Otras fuentes de información**

Existen otras fuentes de información en un sistema operativo, como por ejemplo los registros de red, pero al no tratarse de un entorno en red y el objetivo de análisis es un ordenador personal no vamos a pararnos a analizar estos registros, ya que la información que obtendremos de ellos no será relevante ni será de utilidad en nuestro caso particular.







# 5. Adquisición, análisis y preservación de la información digital

---

En este capítulo veremos cómo obtendremos los datos mediante herramientas propias del sistema y de las herramientas forenses escogidas para esta tarea. El análisis de la información obtenida se hará a la vez que esta se obtiene para agilizar el proceso, ya que se analizará la información por partes dependiendo de su fuente de información y no como un conjunto de toda la información que obtengamos finalmente. Veremos de forma práctica cómo se emplean estas herramientas, así como los datos y la información que estos son capaces de recopilar.

## 5.1 Adquisición y análisis de la información digital

En este apartado veremos las fuentes de información más relevantes en cuanto a contenido y emplearemos las herramientas de extracción y visualización de datos que nos permitan adquirir y analizar la información que contienen.

### 5.1.1 Logs y registros del sistema operativo

En este apartado veremos los logs y los registros de un sistema operativo y la información que estos contienen. También se verán una serie de herramientas que serán empleadas para la obtención de los archivos de registro de Windows y el análisis de estos. Cada herramienta será expuesta de forma práctica y en el caso de Linux se obtendrán los logs de forma directa mediante herramientas propias del sistema.

#### 5.1.1.1 Logs en Linux

Los logs del sistema en Linux se encuentran ubicados en el directorio `/var/log` y en sus subdirectorios. Estos logs registran información relevante de todo el sistema como inicios de sesión, paquetes instalados o qué programas están siendo ejecutados en el sistema. Son ficheros de texto que registran todo tipo de actividades que ocurren en el sistema operativo, y en el caso de Linux se registra absolutamente todo. Son una fuente básica de información. La forma de ver su contenido puede ser mediante la propia Terminal de Linux o bien usando algún editor de texto para facilitar las búsquedas y filtrados dentro del archivo. Dependiendo de para qué log debemos de disponer de permisos de administrador para poder visualizar su contenido.

El fichero `auth.log` registra todas las actividades que impliquen un proceso de autenticación, como los intentos fallidos de autenticación, los usuarios que han iniciado sesión en el sistema, los comandos ejecutados con el comando `sudo`, entre otros.

Como podemos observar en la Ilustración 22 se ha registrado la creación del usuario `user` y la pertenencia a grupos con permisos especiales. En este caso el autor de estas acciones ha sido el mismo sistema operativo durante su instalación ya que el sistema requiere de un usuario y lo dota de permisos añadiéndolo a los grupos de superusuarios para que herede sus permisos.

```
2023-07-22T12:10:24.736652+00:00 ubuntu chfn[2514]: changed user 'user' information
2023-07-22T12:10:24.743210+00:00 ubuntu gpasswd[2520]: members of group users set by root to user
2023-07-22T12:10:24.780660+00:00 ubuntu usermod[2527]: add 'user' to group 'sudo'
2023-07-22T12:10:24.780733+00:00 ubuntu usermod[2527]: add 'user' to shadow group 'sudo'
2023-07-22T12:10:24.813813+00:00 ubuntu usermod[2535]: add 'user' to group 'adm'
2023-07-22T12:10:24.813885+00:00 ubuntu usermod[2535]: add 'user' to shadow group 'adm'
2023-07-22T12:10:24.847895+00:00 ubuntu usermod[2543]: add 'user' to group 'cdrom'
2023-07-22T12:10:24.848000+00:00 ubuntu usermod[2543]: add 'user' to shadow group 'cdrom'
2023-07-22T12:10:24.887876+00:00 ubuntu usermod[2551]: add 'user' to group 'dip'
2023-07-22T12:10:24.887947+00:00 ubuntu usermod[2551]: add 'user' to shadow group 'dip'
2023-07-22T12:10:24.924938+00:00 ubuntu usermod[2559]: add 'user' to group 'lpadmin'
2023-07-22T12:10:24.925007+00:00 ubuntu usermod[2559]: add 'user' to shadow group 'lpadmin'
2023-07-22T12:10:24.958294+00:00 ubuntu usermod[2567]: add 'user' to group 'plugdev'
2023-07-22T12:10:24.958365+00:00 ubuntu usermod[2567]: add 'user' to shadow group 'plugdev'
2023-07-22T12:10:25.126008+00:00 ubuntu accounts-daemon: request by system-bus-name::1.62 [/usr/libexec/gnome-initial-s
etup pid:1964 uid:122]: set password and hint of user 'user' (1000)
```

Ilustración 22: Creación de un usuario (`auth.log`)

En la Ilustración 23 podemos observar que se ha registrado el inicio de sesión del usuario `user`.

```
2023-07-22T12:10:26.386314+00:00 ubuntu systemd-logind[1420]: New session 2 of user user.
2023-07-22T12:10:26.466993+00:00 ubuntu systemd: pam_unix(systemd-user:session): session opened for user user(uid=1000)
by (uid=0)
2023-07-22T12:10:27.406869+00:00 ubuntu gdm-password]: gkr-pam: unlocked login keyring
2023-07-22T12:10:32.103678+00:00 ubuntu gnome-keyring-daemon[2956]: discover_other_daemon: 1
2023-07-22T12:10:32.103878+00:00 ubuntu gnome-keyring-daemon[2638]: The PKCS#11 component was already initialized
2023-07-22T12:10:32.104147+00:00 ubuntu gnome-keyring-daemon[2955]: discover_other_daemon: 1
2023-07-22T12:10:32.105370+00:00 ubuntu gnome-keyring-daemon[2638]: The Secret Service was already initialized
2023-07-22T12:10:32.105635+00:00 ubuntu gnome-keyring-daemon[2957]: discover_other_daemon: 1
2023-07-22T12:10:35.711587+00:00 ubuntu polkitd(authority=local): Registered Authentication Agent for unix-session:2 (s
ystem bus name :1.87 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.
UTF-8)
```

Ilustración 23: Inicio de sesión de usuario (`auth.log`)

En la Ilustración 24 se registra el inicio de sesión y el cierre de sesión del usuario `root`.

```
2023-07-22T12:11:01.151307+00:00 ubuntu CRON[3644]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2023-07-22T12:11:01.153271+00:00 ubuntu CRON[3644]: pam_unix(cron:session): session closed for user root
```

Ilustración 24: Inicio y cierre de sesión de usuario

El fichero `kern.log` proporciona información de los mensajes del `kernel`, y resulta útil para detectar problemas de detección de hardware como vemos en la Ilustración 25.

```

user@ubuntu:~/var/log$ cat kern.log
2023-07-22T12:08:08.118796+00:00 ubuntu kernel: [ 0.000000] Linux version 6.2.0-20-generic (buildd@lcy02-amd64-035)
(x86_64-linux-gnu-gcc-12 (Ubuntu 12.2.0-17ubuntu1) 12.2.0, GNU ld (GNU Binutils for Ubuntu) 2.40) #20-Ubuntu SMP PREEMPT_DYNAMIC Thu Apr 6 07:48:48 UTC 2023 (Ubuntu 6.2.0-20.20-generic 6.2.6)
2023-07-22T12:08:08.118884+00:00 ubuntu kernel: [ 0.000000] Command line: BOOT_IMAGE=/casper/vmlinuz auto=true prese
ed/file=/cdrom/preseed.cfg priority=critical quiet splash noprompt noshell automatic-ubiquity debian-installer/locale=en_US keyboard-configuration/layoutcode=us languagechooser/language-name=English localechooser/supported-locales=en_US.U
TF-8 countrychooser/shortlist=ES --
2023-07-22T12:08:08.118885+00:00 ubuntu kernel: [ 0.000000] KERNEL supported cpus:
2023-07-22T12:08:08.118886+00:00 ubuntu kernel: [ 0.000000] Intel GenuineIntel
2023-07-22T12:08:08.118886+00:00 ubuntu kernel: [ 0.000000] AMD AuthenticAMD
2023-07-22T12:08:08.118887+00:00 ubuntu kernel: [ 0.000000] Hygon HygonGenuine
2023-07-22T12:08:08.118888+00:00 ubuntu kernel: [ 0.000000] Centaur CentaurHauls
2023-07-22T12:08:08.118888+00:00 ubuntu kernel: [ 0.000000] zhaoxin Shanghai
2023-07-22T12:08:08.118889+00:00 ubuntu kernel: [ 0.000000] [Firmware Bug]: TSC doesn't count with P0 frequency!
2023-07-22T12:08:08.118889+00:00 ubuntu kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating p
oint registers'
2023-07-22T12:08:08.118890+00:00 ubuntu kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
2023-07-22T12:08:08.118890+00:00 ubuntu kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
2023-07-22T12:08:08.118891+00:00 ubuntu kernel: [ 0.000000] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
2023-07-22T12:08:08.118892+00:00 ubuntu kernel: [ 0.000000] x86/fpu: Enabled xstate features 0x7, context size is 83
2 bytes, using 'standard' format.
2023-07-22T12:08:08.118892+00:00 ubuntu kernel: [ 0.000000] signal: max sigframe size: 1776
2023-07-22T12:08:08.118893+00:00 ubuntu kernel: [ 0.000000] BIOS-provided physical RAM map:
2023-07-22T12:08:08.118893+00:00 ubuntu kernel: [ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] u
sable

```

Ilustración 25: Mensajes del kernel (kern.log)

En la Ilustración 25 se pueden apreciar las comprobaciones de hardware como el procesador o la memoria RAM. Nos muestra los procesadores que son soportados por el *kernel* como los Intel o AMD.

El fichero `syslog` recopila información acerca de los mensajes del sistema y las aplicaciones en ejecución. En la Ilustración 26 se refleja que las aplicaciones LibreOffice y Firefox se encuentran en ejecución.

```

2023-07-22T12:11:28.190994+00:00 ubuntu kernel: [ 227.842050] audit: type=1326 audit(1690027888.183:88): auid=1000 uid
=1000 gid=1000 ses=3 subj=snap.firefox.firefox pid=3665 comm="firefox" exe="/snap/firefox/2517/usr/lib/firefox/firefox"
sig=0 arch=c000003e syscall=314 compat=0 ip=0x7f1c89198a3d code=0x50000
2023-07-22T12:08:08.119465+00:00 ubuntu kernel: [ 20.276600] audit: type=1400 audit(1690027679.456:20): apparmor="STA
TUS" operation="profile_load" profile="unconfined" name="libreoffice-soffice" pid=1368 comm="apparmor_parser"

```

Ilustración 26: Aplicaciones en ejecución (syslog)

El fichero `boot.log` que se muestra en la ilustración 27 contiene toda la información de arranque del sistema como el arranque de los servicios del sistema, si las unidades de almacenamiento se montan correctamente, averiguar errores en el inicio del sistema, entre otros. Como se puede observar en la ilustración se ha almacenado la comprobación inicial del sistema al arrancar, marcando con OK aquellos elementos o servicios que se han inicializado correctamente.

```

[ OK ] Finished gpu-manager.service - Detect the available GPUs and deal with any system changes.
[ OK ] Started dbus.service - D-Bus System Message Bus.
Starting NetworkManager.service - Network Manager...
Starting wpa_supplicant.service - WPA supplicant...
[ OK ] Started avahi-daemon.service - Avahi mDNS/DNS-SD Stack.
[ OK ] Started systemd-logind.service - User Login Management.
[ OK ] Started switcheroo-control.service - Switcheroo Control Proxy service.
Starting alsa-restore.service - Save/Restore Sound Card State...
[ OK ] Finished alsa-restore.service - Save/Restore Sound Card State.

```

Ilustración 27: Arranque del sistema (boot.log)

El fichero `wtmp` registra los usuarios que tienen una sesión abierta en el sistema o han iniciado sesión. Para visualizarlo correctamente debemos de utilizar un sencillo

programa `utmpdump` para leer su contenido, ya que este registro se encuentra en formato binario y no podemos usar las típicas herramientas de texto. Para abrir el archivo con este programa utilizaremos el comando `utmpdump wtmp` como se muestra en la Ilustración 28.

```
Utmp dump of wtmp
[2] [00000] [~~ ] [reboot ] [~      ] [6.2.0-20-generic ] [0.0.0.0      ]
[2023-07-22T12:07:46,887459+00:00]
[1] [00053] [~~ ] [runlevel] [~      ] [6.2.0-20-generic ] [0.0.0.0      ]
[2023-07-22T12:08:59,932532+00:00]
[7] [02659] [  ] [user   ] [seat0  ] [login screen  ] [0.0.0.0      ]
[2023-07-22T12:10:27,573188+00:00]
[7] [02659] [  ] [user   ] [:1     ] [:1     ] [0.0.0.0      ]
[2023-07-22T12:10:28,964260+00:00]
```

Ilustración 28: Datos históricos (wtmp)

En este caso solamente tiene sesión iniciada el usuario `user` y se observa un reinicio del sistema.

Además de los logs se puede emplear otro comando que nos proporciona información acerca de los paquetes instalados en el sistema, de tal forma que si ejecutamos el comando `dpkg-query -l` nos mostrará por pantalla los programas instalados indicando nombre, versión, arquitectura del sistema y una breve descripción como podemos ver en la Ilustración 29.

```
root@ubuntu:/var/log# dpkg-query -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name          Version          Architecture Description
-----
ii accountsservice 22.08.8-1ubuntu7 amd64      query and manipula
ii acl              2.3.1-3          amd64      access control lis
ii adduser          3.129ubuntu1    all        add and remove use
ii adwaita-icon-theme 41.0-1ubuntu1   all        default icon theme
ii alsa-base        1.0.25+dfsg-0ubuntu7 all        ALSA driver config
ii alsa-topology-conf 1.2.5.1-2       all        ALSA topology conf
ii alsa-ucm-conf    1.2.6.3-1ubuntu8 all        ALSA Use Case Mana
ii alsa-utils       1.2.8-1ubuntu1  amd64      Utilities for conf
ii amd64-microcode 3.20220411.1ubuntu3 amd64      Processor microcode
ii anacron          2.3-36ubuntu2   amd64      cron-like program
ii apg              2.2.3.dfsg.1-5build2 amd64      Automated Password
ii fdisk            2.38.1-4ubuntu1 amd64      collection of part
ii file             1:5.44-3        amd64      Recognize the type
ii findutils        4.9.0-3ubuntu1  amd64      utilities for find
ii firefox          1:1snap1-0ubuntu3 amd64      Transitional packa
ii firmware-sof-signed 2.2.4-1         all        Intel SOF firmwar
ii fontconfig       2.14.1-3ubuntu3 amd64      generic font confi
ii fontconfig-config 2.14.1-3ubuntu3 amd64      generic font confi
ii fonts-arphic-ukai 0.2.20080216.2-5 all        "AR PL UKai" Chine
ii fdisk            2.38.1-4ubuntu1 amd64      collection of part
ii file             1:5.44-3        amd64      Recognize the type
ii findutils        4.9.0-3ubuntu1  amd64      utilities for find
ii firefox          1:1snap1-0ubuntu3 amd64      Transitional packa
ii firmware-sof-signed 2.2.4-1         all        Intel SOF firmwar
ii fontconfig       2.14.1-3ubuntu3 amd64      generic font confi
ii fontconfig-config 2.14.1-3ubuntu3 amd64      generic font confi
ii fonts-arphic-ukai 0.2.20080216.2-5 all        "AR PL UKai" Chine
```

Ilustración 29: Paquetes instalados

Podemos observar que hay instalados paquetes del sistema y de otras aplicaciones como el navegador Firefox.

Una alternativa es el uso del comando `apt list` que muestra la salida de la Ilustración 30.

```
root@ubuntu:/var/log# apt list
Listing... Done
accountsservice/lunar,now 22.08.8-1ubuntu7 amd64 [installed,automatic]
acct/lunar 6.6.4-5 amd64
acl/lunar,now 2.3.1-3 amd64 [installed,automatic]
acpid/lunar 1:2.0.33-2ubuntu1 amd64
adcli/lunar 0.9.1-2ubuntu1 amd64
adduser/lunar,now 3.129ubuntu1 all [installed,automatic]
adsys/lunar 0.11.0 amd64
advancecomp/lunar 2.5-1 amd64
adwaita-icon-theme/lunar,now 41.0-1ubuntu1 all [installed,automatic]
aide-common/lunar 0.18-2 all
aide/lunar 0.18-2 amd64
```

*Ilustración 30: Salida del comando "apt list"*

Cabe destacar que la arquitectura de los logs de Linux se organiza de una forma peculiar, ya que emplea un mecanismo de rotación de logs y esto se observa viendo que hay varios que tienen un nombre parecido como por ejemplo `auth.log`, `auth.log.1` y `auth.log.2.gz`, que a pesar de que sean casi idénticos permite diferenciar unos de otros. El fichero `auth.log` es el fichero principal en el que se recopila información, de tal forma que semanalmente su contenido se traslada al `auth.log.1`, y a su vez su contenido se comprime y se traslada al fichero `auth.log.2.gz` de tal forma que el fichero `auth.log` siempre esté vacío y pueda seguir recopilando información.

De este modo se organiza mejor la información semanalmente y facilita la tarea de revisión de los logs, ya que no cuesta lo mismo revisar un log general cuyo origen puede remontarse al primer inicio del sistema que a un log que solo contenga la información de esa semana.

### 5.1.1.2 Logs en Windows

Los eventos del sistema en Windows se recopilan de forma diferente que en Linux a pesar de que la función que cumplan sea la misma. Los eventos del sistema se pueden ver desde el Visor de eventos de Windows que es una herramienta propia del sistema. El visor dispone de una vista general que ordena los eventos según su categoría y permite crear vistas personalizadas a partir de estas vistas predeterminadas con filtros de eventos por tipo, identificador del evento, tiempo, entre otros.

Los registros de eventos del sistema, seguridad y aplicaciones se pueden visualizar desde el Visor de eventos, que se trata de un componente propio del sistema Windows.

El registro de la aplicación registra eventos relacionados con aplicaciones y servicios instalados en el sistema, mientras que el registro del sistema incluye eventos que tienen que ver con los componentes y controladores del sistema.

Los inicios de sesión, los intentos fallidos de inicio de sesión y otros incidentes relacionados con la seguridad se documentan en el registro de seguridad. Las entradas de este registro de eventos de Windows incluyen información detallada, como la fecha y la hora en que ocurrió el evento, la fuente del evento, código de error, identificador del evento y más información relevante.

Entre los registros de Windows podemos destacar los registros de aplicación, seguridad y sistema.

El registro de aplicación recoge los eventos que generan las aplicaciones del sistema. Podemos encontrar eventos de arranque y parada de aplicaciones, así como instalaciones y desinstalaciones.

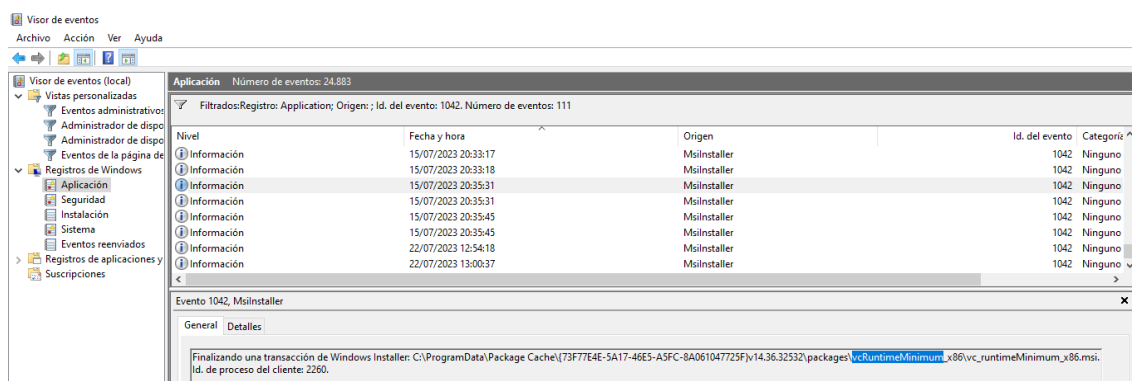


Ilustración 31: Evento de instalación

En la Ilustración 31 podemos ver la notificación que envía el instalador de Windows cuando termina de instalar un programa, que en este caso corresponde a la biblioteca de Microsoft Visual C++ Redistributable.

El registro de seguridad recoge aquellas acciones en el sistema que requieran de una autenticación por parte del usuario como inicios de sesión, inicios de sesión fallidos, etc.



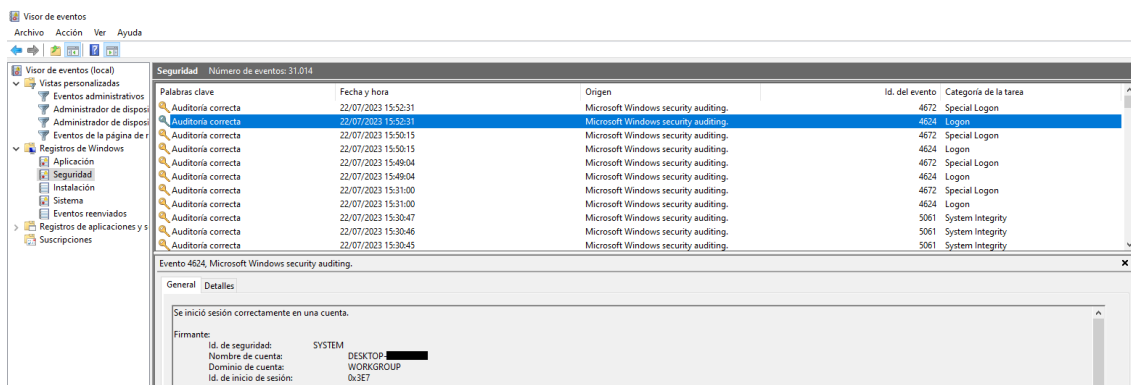


Ilustración 32: Evento de inicio de sesión de usuario

En la Ilustración 32 se puede apreciar que se ha registrado un evento de auditoría del sistema, en el que muestra el nombre de la cuenta de usuario local del sistema en la que se ha realizado un inicio de sesión.

Si inspeccionamos el registro del sistema podemos ver los apagados y reinicios, arranques y paradas de servicios del sistema, tiempo que lleva el sistema encendido, entre otros.

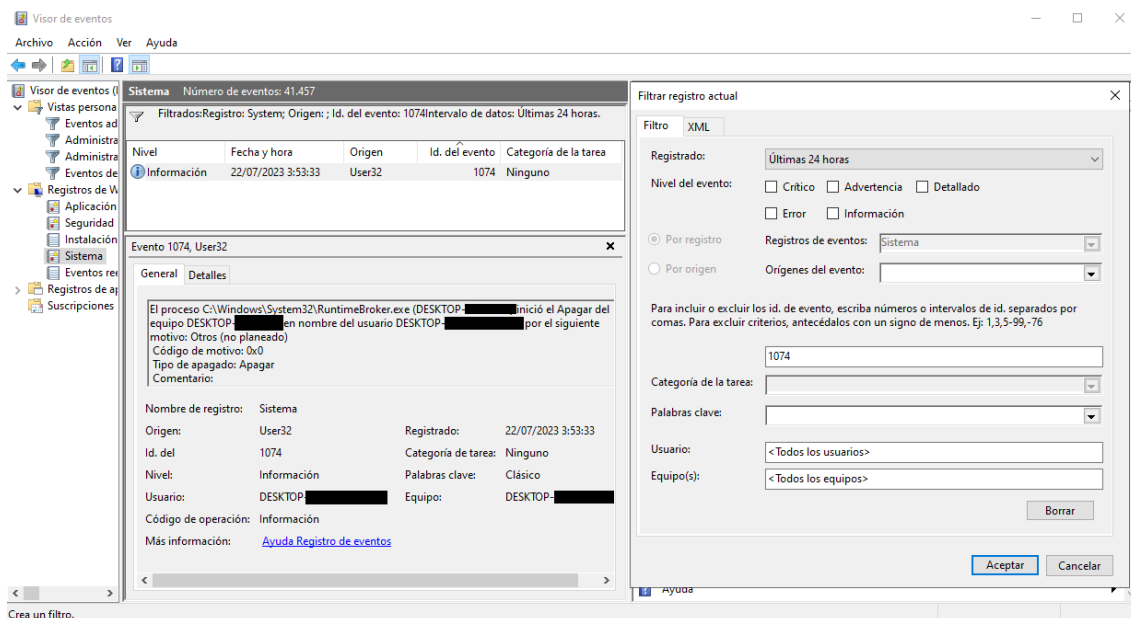


Ilustración 33: Evento de reinicio del sistema

En la Ilustración 33 podemos observar que si filtramos este registro con el ID de proceso 1074 que corresponde a los reinicios y apagados del sistema podemos darnos cuenta de que ha sido reiniciado por la aplicación RuntimeBroker.exe en nombre de un usuario local sin dar ningún motivo para el reinicio. Este proceso forma parte de Windows y se encarga de controlar las aplicaciones universales del sistema.





### 5.1.2 Registro de Windows

Además del visor de eventos, disponemos del Editor de registro de Windows que se trata de un visor y editor de los registros del sistema. Este fue ideado para almacenar configuraciones, opciones, información de hardware y software, así como otras preferencias del sistema y del usuario. Es una parte fundamental del funcionamiento del sistema operativo, ya que contiene datos importantes necesarios para que Windows funcione correctamente y para personalizar la experiencia del usuario.

El Registro de Windows se organiza en una estructura jerárquica similar a un árbol, donde los datos se almacenan en forma de claves y valores los cuales se identifican mediante rutas y nombres únicos. Cada clave puede contener subclaves y valores:

- Una clave es similar a una carpeta en la estructura del registro. Puede contener subclaves y valores. Las claves se organizan jerárquicamente en una estructura de árbol que comienza con la clave raíz, que es la base de todo el registro. Las claves tienen nombres únicos y están identificadas por rutas que comienzan con la denominación HKEY.
- Un valor es similar a un archivo en la estructura del registro. Se encuentra dentro de una clave y contiene información específica. Cada valor tiene un nombre, un tipo de datos (por ejemplo, cadena de texto, número entero, binario, etc.) y su contenido. Los valores se utilizan para almacenar configuraciones, preferencias del usuario y otra información relevante.

El Registro almacena información sobre una amplia variedad de elementos, incluyendo configuraciones del sistema, configuraciones de software, usuarios, perfiles de usuario, hardware y controladores de dispositivo, programas en ejecución, etc.

El Registro es una parte esencial del sistema operativo y es accedido y utilizado por Windows en todo momento para mantener la configuración del sistema actualizada. Sin embargo, es una base de datos delicada, y modificar o eliminar valores incorrectos en el Registro puede causar problemas graves en el funcionamiento del sistema. Antes de realizar cambios en el registro se recomienda realizar siempre una copia de seguridad para poder revertir los cambios en caso de fallo del sistema.

En Windows, los registros se organizan jerárquicamente en claves y valores dentro de una estructura de árbol. La información se almacena en archivos con extensiones .reg y .hive, aunque internamente, los registros se almacenan en archivos específicos en el directorio "C:\Windows\System32\config".

El registro de Windows es tan extenso y alberga tanta información que resulta imposible poder dar una visión completa de todo aquello que contiene. Sin embargo, se puede dar una visión general de los cinco apartados principales que se encuentran en la raíz del registro:

- **HKEY\_CLASSES\_ROOT:** Esta sección contiene información sobre las asociaciones de archivos y las aplicaciones registradas en el sistema. Aquí se almacena qué aplicación debe abrir cada tipo de archivo. Por ejemplo, determinará qué programa se utiliza para abrir archivos .txt o .pdf.
- **HKEY\_CURRENT\_USER:** Aquí se almacenan las configuraciones específicas del usuario que tiene la sesión iniciada en ese momento. Incluye preferencias personalizadas, como políticas energéticas o temas de escritorio elegidos por el usuario actual.
- **HKEY\_USERS:** Al igual que el apartado anterior, contiene configuraciones, pero estas son aplicables a todos los usuarios del sistema, no solo al que está utilizando el equipo en ese momento.
- **HKEY\_LOCAL\_MACHINE:** Esta sección es diferente a las demás, ya que contiene claves y valores que varían según el estado actual del equipo. Almacena información sobre dispositivos conectados al equipo, controladores de hardware, información de la máquina local y otros datos esenciales para el funcionamiento del sistema
- **HKEY\_CURRENT\_CONFIG:** Contiene información sobre el perfil de hardware utilizado cuando el sistema se inicia. La información aquí está relacionada con el apartado anterior y es relevante para la configuración del hardware del equipo.

Si hacemos hincapié dentro de estos apartados podremos encontrar otros registros con información todavía más concreta. Entre todos los registros que podemos encontrar en los sistemas Windows cabe destacar los siguientes:

- **SAM (Security Accounts Manager):** El administrador de cuentas de seguridad almacena información relacionada con las cuentas de usuarios locales y las políticas de seguridad en el sistema. Podemos encontrar datos sensibles como contraseñas cifradas, identificadores de las cuentas de usuario, sus opciones y configuraciones, e información acerca de cuentas bloqueadas o deshabilitadas. Sin embargo, debido a su importancia en la seguridad, está protegido y no se puede acceder mientras el sistema está en funcionamiento normal ya que se requieren permisos especiales.
- **SYSTEM:** Archivo necesario para el funcionamiento del sistema. Recopila información acerca del sistema como el nombre del equipo, drivers y dispositivos montados en el equipo, configuración del sistema, zona horaria o información de los servicios instalados en el sistema. Contiene la información clave para garantizar que el sistema pueda operar de manera eficiente y adaptarse a las preferencias y necesidades del usuario.
- **NTUSERDAT:** Este archivo es específico para cada usuario y se encuentra en el perfil de usuario. Es un componente personalizado del registro que guarda la configuración y preferencias específicas de un usuario individual. Aquí se



almacenan las configuraciones del escritorio, preferencias del explorador de archivos, configuraciones de impresoras y otros ajustes personalizados para ese usuario en particular.

- **SECURITY:** Archivo esencial para establecer políticas de seguridad locales que protegen al sistema contra amenazas potenciales. Aquí se almacenan claves y valores que definen configuraciones como la complejidad de las contraseñas, los intentos de inicio de sesión fallidos permitidos antes de bloquear una cuenta, y otras políticas de seguridad. Además, contiene información sobre las cuentas de seguridad y los permisos asociados con cada cuenta, asegurando que los usuarios y grupos tengan los privilegios adecuados para acceder a recursos y funciones.
- **SOFTWARE:** Juega un papel crucial en el registro al almacenar información sobre el software y aplicaciones instaladas en el sistema. Aquí se encuentran claves y valores relacionados con las preferencias, configuraciones y opciones específicas de cada programa. También rastrea la instalación y desinstalación de programas, así como las actualizaciones aplicadas, lo que permite que el sistema mantenga un registro detallado de las acciones relacionadas con el software.

Como hemos comentado anteriormente los valores de cada clave tienen un tipo y un formato distinto, por lo que visualizar su contenido no puede hacerse a simple vista solamente empleando el Editor de registro, y para ello utilizaremos herramientas externas para recuperar los archivos relevantes del registro de Windows y poder analizar su contenido visualizándolo con intérpretes de código binario y hexadecimal.

### 5.1.3 AccessData FTK Imager para recuperación de los archivos del registro

Mediante FTK Imager obtendremos los archivos de registro más relevantes en cuanto a información contenida. Para comenzar la extracción abriremos el programa y en su ventana principal desde el apartado de Archivo seleccionaremos la opción de Obtener archivos protegidos.

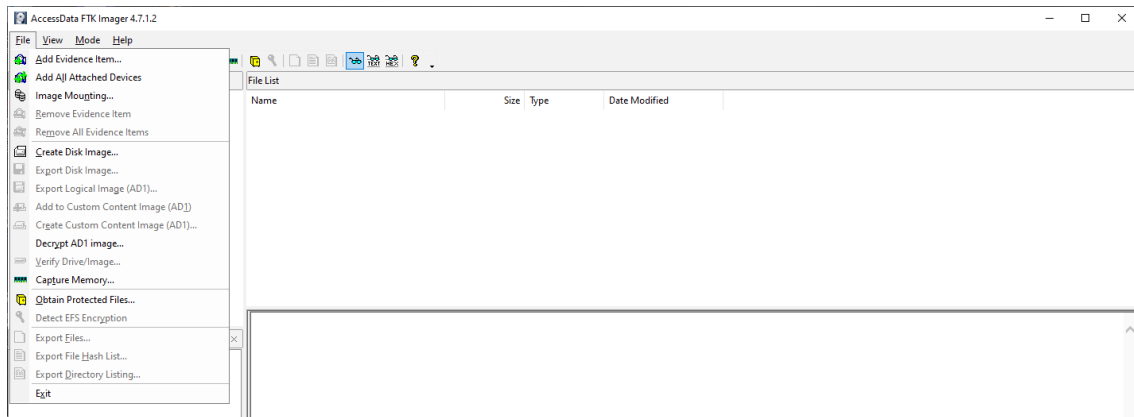


Ilustración 34: Ventana principal de AccessData FTK Imager

Después debemos seleccionar una ruta de extracción de los archivos y marcar la opción de recuperar contraseñas y todos los archivos del registro.

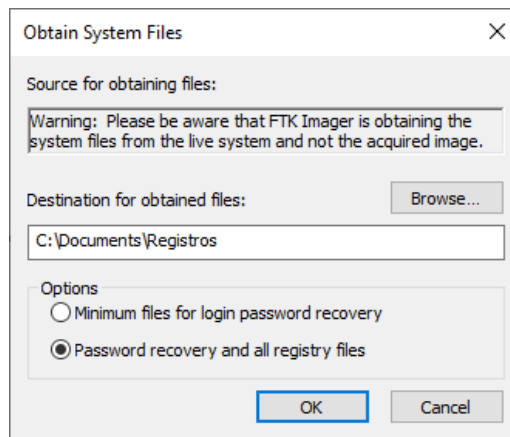


Ilustración 35: Recuperación de archivos de registro

Veremos el progreso de extracción de los archivos y una vez termine veremos los archivos en la ruta designada.

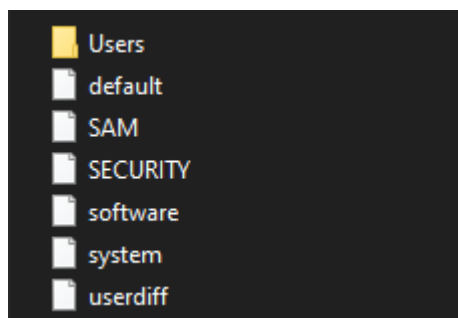


Ilustración 36: Archivos de registro extraídos

### 5.1.4 AccessData Registry Viewer para visualizar los valores de los archivos de registro

Para poder visualizar en detalle el contenido de los archivos usaremos Registry Viewer. En la ventana principal del programa iremos al apartado Archivo y Abrir, seleccionando el archivo que queremos visualizar en detalle.

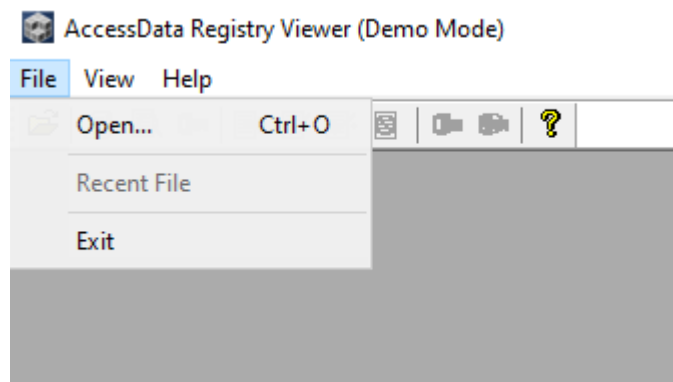


Ilustración 37: Ventana principal de AccessData Registry Viewer

Al abrir el archivo observaremos las secciones de visualización con las que cuenta el programa, que son una vista general del archivo como si de una jerarquía de carpetas se tratase, el contenido de la carpeta seleccionada, y dos visores del contenido de la clave seleccionada, uno que muestra las propiedades y los valores de las claves y otro que es un visor hexadecimal.

Cargando el archivo SAM podremos observar las cuentas de usuario existentes en el sistema, ya sean predeterminadas, de creación manual, creadas por el sistema o se encuentren deshabilitadas. En concreto se visualiza la cuenta de usuario principal del sistema en la cual se puede visualizar su ID, nombre de usuario, nombre completo, la última vez que cambió la contraseña de acceso y la dirección de correo perteneciente a la cuenta.

Con estos datos podemos determinar que se trata de la cuenta personal de un usuario y que se trata de una cuenta de Microsoft ya que lleva asociada un correo electrónico de Outlook como se observa en la Ilustración 38.

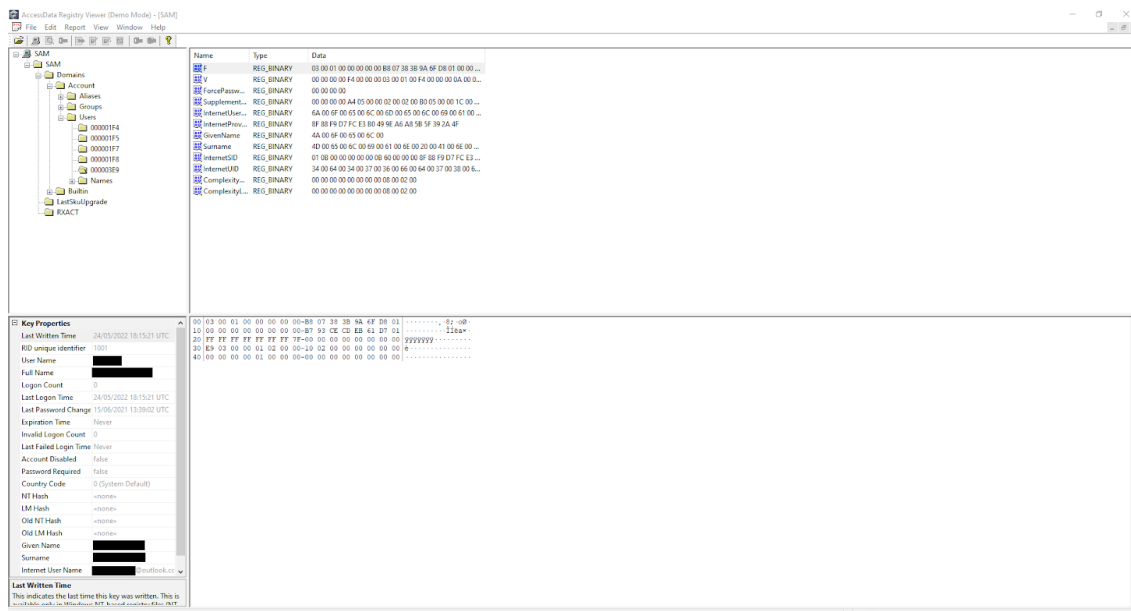


Ilustración 38: Detalle de cuenta de usuario

En comparación a la vista general que ofrece el Editor de Registro de Windows es mucho más completa y detallada.

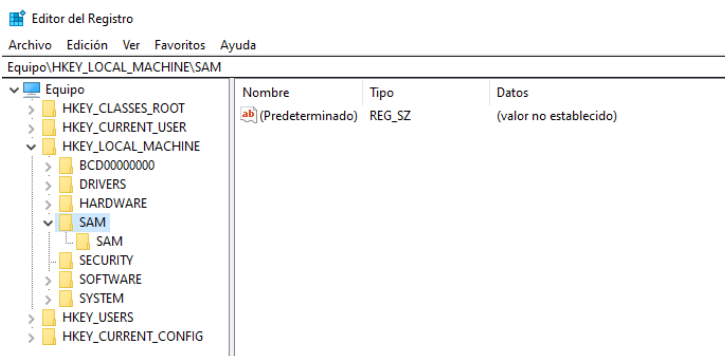


Ilustración 39: Ventana del editor de registro de Windows

Si esta vez cargamos el archivo SYSTEM podremos observar datos relacionados con la información del sistema operativo.

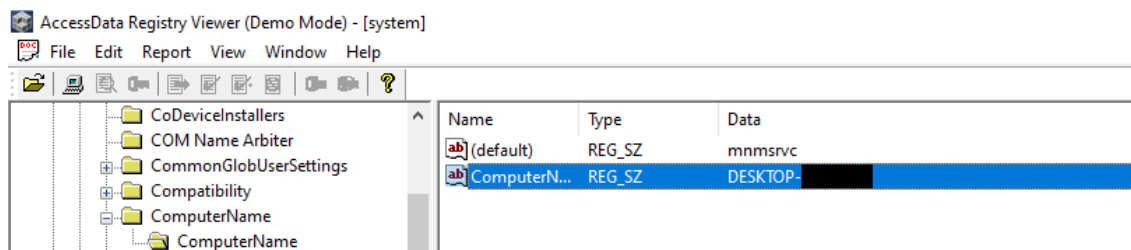


Ilustración 40: Nombre del equipo

Por ejemplo, en la ilustración 40 podemos ver el nombre del equipo que tiene el sistema. Esto además de ser importante para identificar el equipo que está siendo



analizado también sirve para que se identifique dentro de una red para conectar impresoras, compartir recursos o realizar conexiones remotas.

También podremos determinar la zona horaria como vemos en la ilustración 41. En este caso se trata de la zona horaria que corresponde a (UTC+01:00) Madrid, Paris.

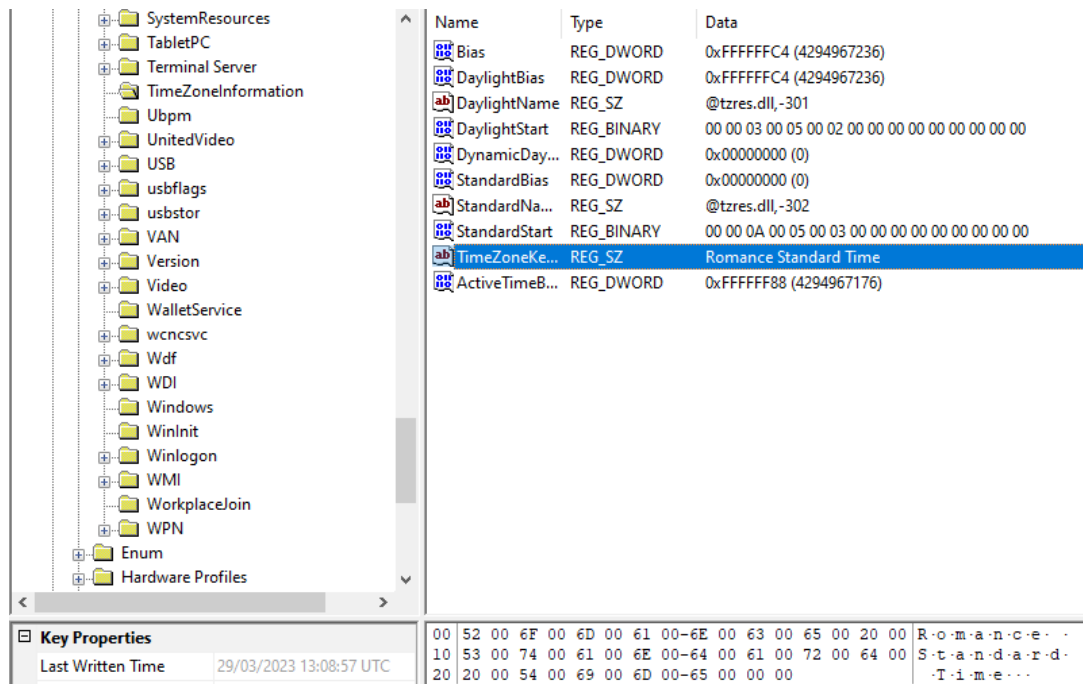


Ilustración 41: Zona horaria del sistema

También es posible obtener un historial de todos los dispositivos de almacenamiento que han sido conectados al equipo como muestra la ilustración 42. En este caso concreto observamos que se ha conectado una unidad de almacenamiento USB externa de la marca Sony, pero también podemos observar que se han conectado otras unidades de disco duro o unidades externas como las unidades D, E, F, G, H, I, J y K.

Si queremos inspeccionar el archivo NTUSER.DAT podremos encontrar información acerca de los programas instalados en ese perfil de usuario.

En la Ilustración 43 podemos ver que este usuario ha instalado videojuegos, una herramienta de desarrollo Android llamada AdbAppControl, controladores del fabricante de procesadores AMD, software antivirus de Avast y el cliente BitTorrent.

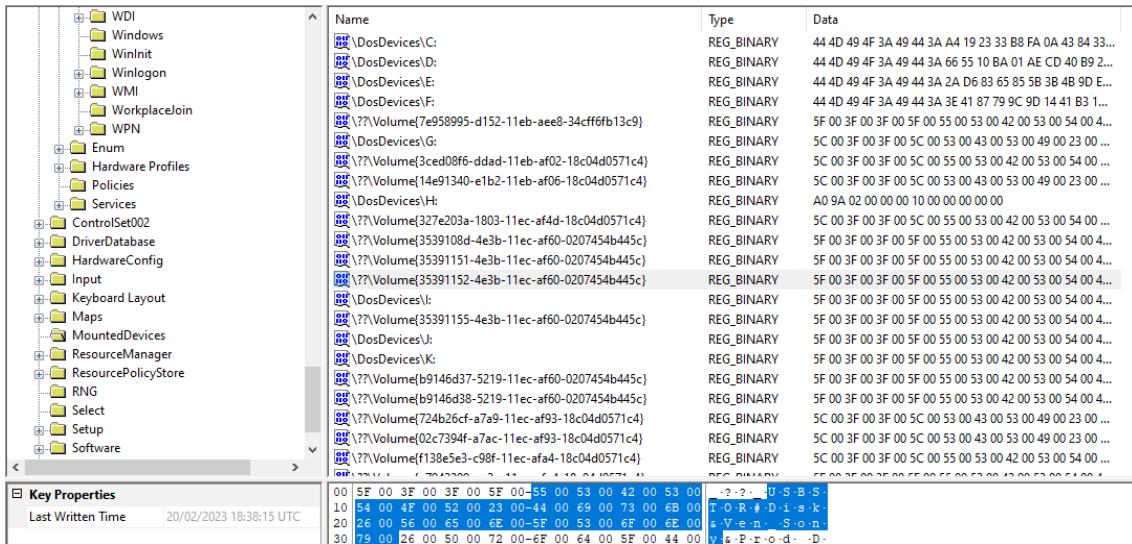


Ilustración 42: Dispositivos de almacenamiento

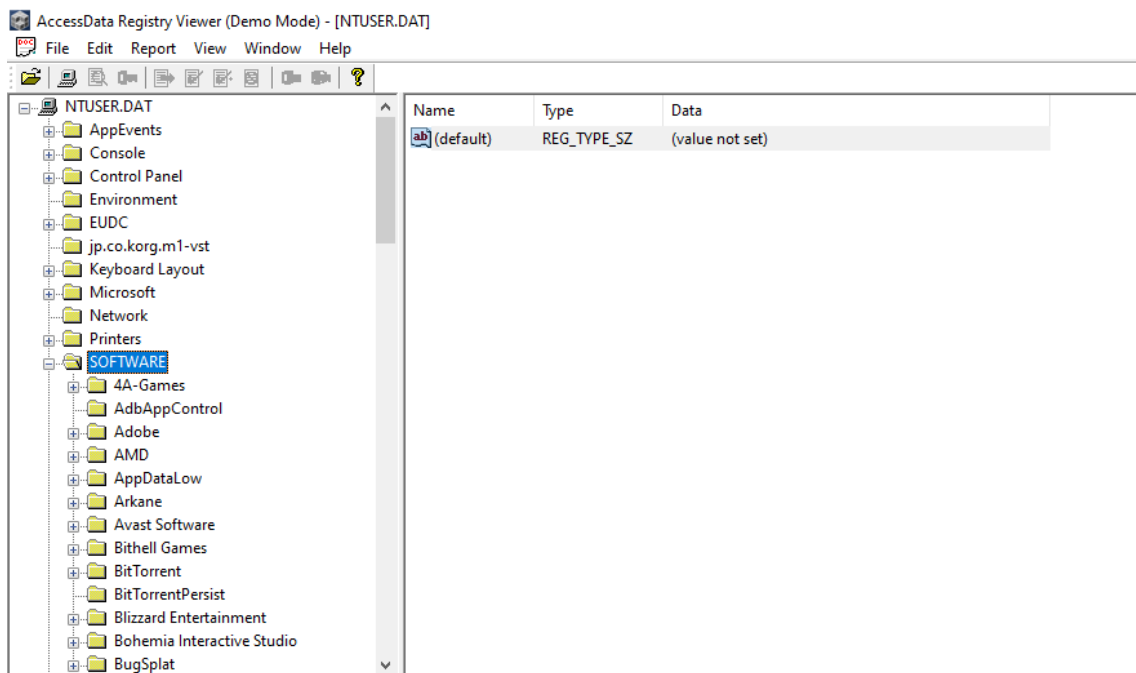


Ilustración 43: Programas instalados

Podemos ver las impresoras configuradas para usar en el equipo. La Ilustración 45 muestra marca y modelo de una impresora Epson.





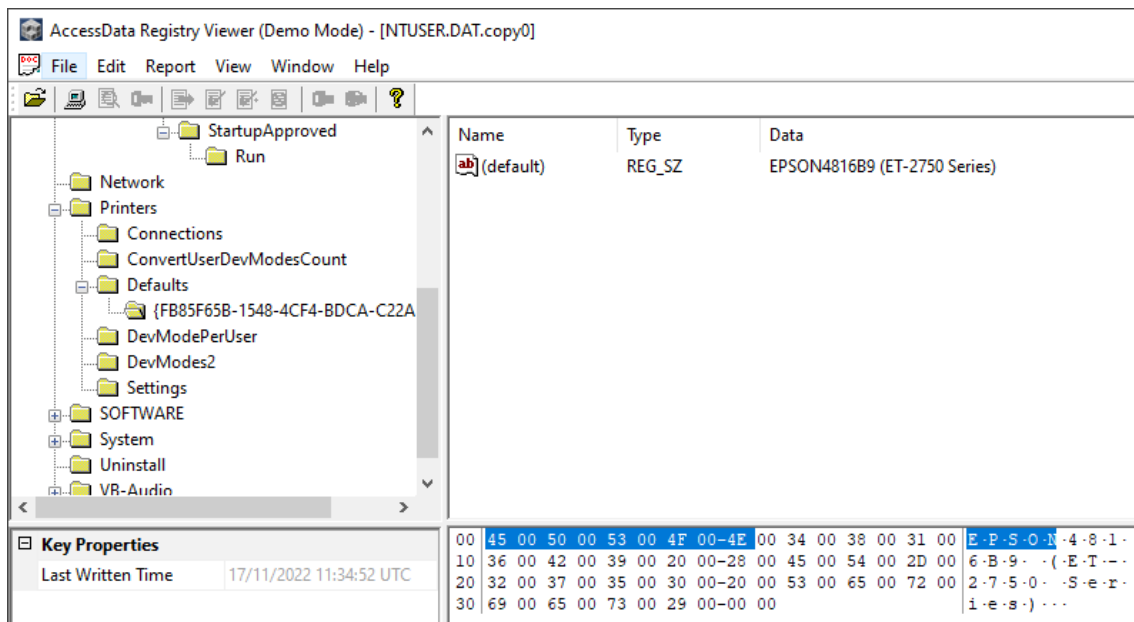


Ilustración 44: Impresoras del equipo

También es posible obtener la lista de periféricos, dispositivos de entrada y sus controladores de dispositivo que se han instalado en el equipo como se aprecia en la Ilustración 44.

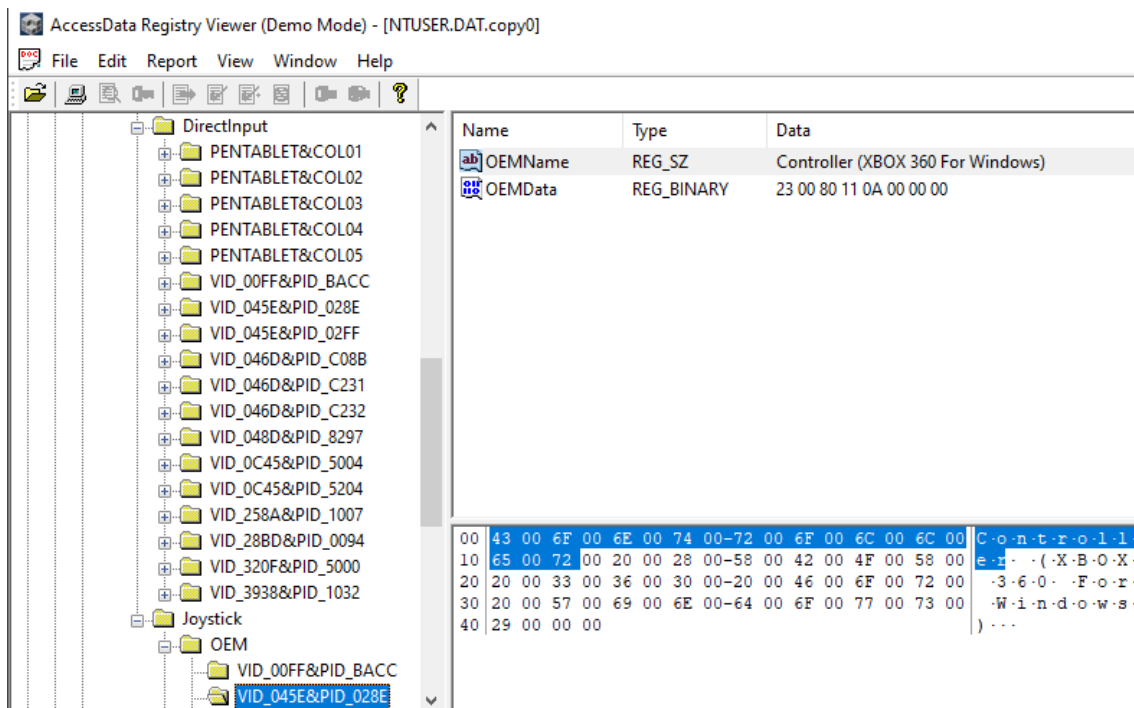


Ilustración 45: Dispositivos y periféricos instalados en el sistema

En este caso estamos viendo que ha sido instalado un mando de la consola Xbox One que es compatible de forma nativa con Windows en el apartado de Joysticks y otro tipo de dispositivos de entrada directa como son teclados, ratones y un dispositivo PENTABLET que corresponde a una tableta gráfica.

Si abrimos el registro SOFTWARE encontraremos datos acerca de los programas instalados en el equipo.

En la Ilustración 46 nos encontramos con los datos acerca del programa RyzenMaster que se trata de un monitor de rendimiento para procesadores AMD. Podemos ver la ruta de instalación del programa y la ubicación de su ejecutable, así como el número de versión del programa que está instalada en el equipo. También podemos ver que se han instalado programas de Adobe o los controladores de sonido de ASIO.

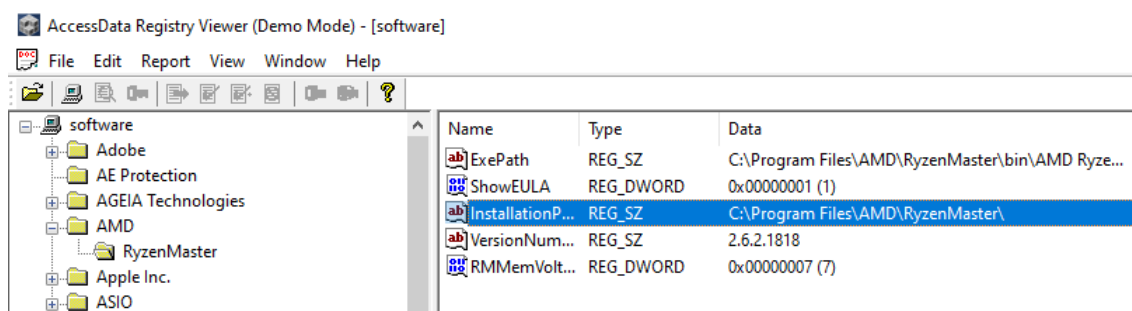


Ilustración 46: Programas instalados y ruta de instalación

También podemos averiguar los programas que se arrancan al inicio del sistema. Podemos ver que los procesos que se inician con Windows pertenecen a los controladores de audio Realtek o el antivirus Avast como observamos en la Ilustración 47.

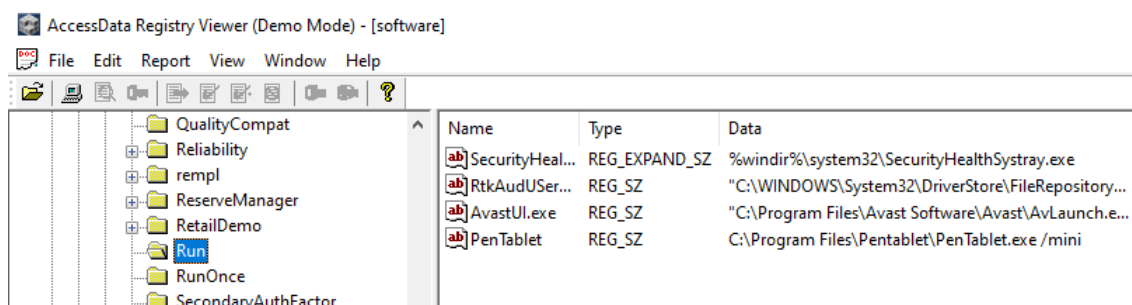


Ilustración 47: Programas de inicio

Recuperando los archivos de registro podemos obtener información acerca de los usuarios del sistema, los programas que instalan y utilizan, los dispositivos que conectan al equipo y las acciones que realizan dentro del sistema, por lo que podemos establecer un perfil de usuario en función de la información recopilada, ver si sigue patrones de uso, etc.

### 5.1.5 Recuperación de contraseñas del navegador con WebBrowserPassView

Mediante esta herramienta portable y de uso gratuito vamos a recuperar las contraseñas guardadas en los navegadores que haya empleado el usuario. Debido a que guardar las contraseñas en el navegador supone una brecha de seguridad no se recomienda esta práctica, pero para ilustrar las capacidades de esta herramienta se han guardado contraseñas generadas a modo de prueba con nombres indicativos como tal a modo de ejemplo.



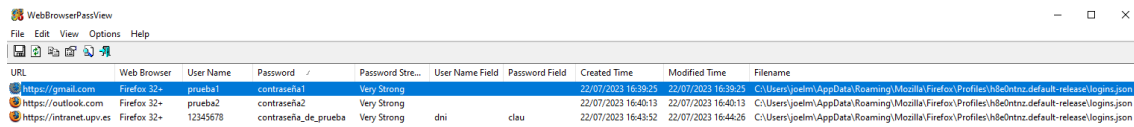


Ilustración 48: Vista principal del programa WebBrowserPassView

El programa consta de una única ventana donde se muestran los pares usuario/contraseña que ha sido capaz de recuperar de los navegadores. Como se puede observar a modo de prueba se han recuperado las contraseñas de ejemplo generadas previamente a la ejecución de la herramienta. También proporciona la URL del sitio visitado, así como el navegador en el cual se ha guardado la contraseña. Toda la información que se muestra en la ventana del programa puede ser recuperada y guardada en un fichero de texto en diferentes formatos como txt o csv.

A modo de curiosidad es posible recuperar los usuarios y las contraseñas de un sitio concreto sin necesidad de gastar esta herramienta. Es algo que podría considerarse una vulnerabilidad y que no es posible hacerlo en cualquier sitio web. Por ejemplo, en Firefox si vamos a su apartado de Configuración nos podemos mover hasta el apartado de Privacidad y es ahí donde veremos las contraseñas guardadas junto al sitio web donde se han introducido esas credenciales.

Si vamos a la página de inicio de sesión veremos que nos rellena los campos mediante la función de autocompletar, por lo que si pulsamos la tecla F12 para acceder a las herramientas de desarrollo del navegador y tratamos de modificar el código HTML de la página de login podemos cambiar el tipo del campo de texto para que revele la contraseña a simple vista.

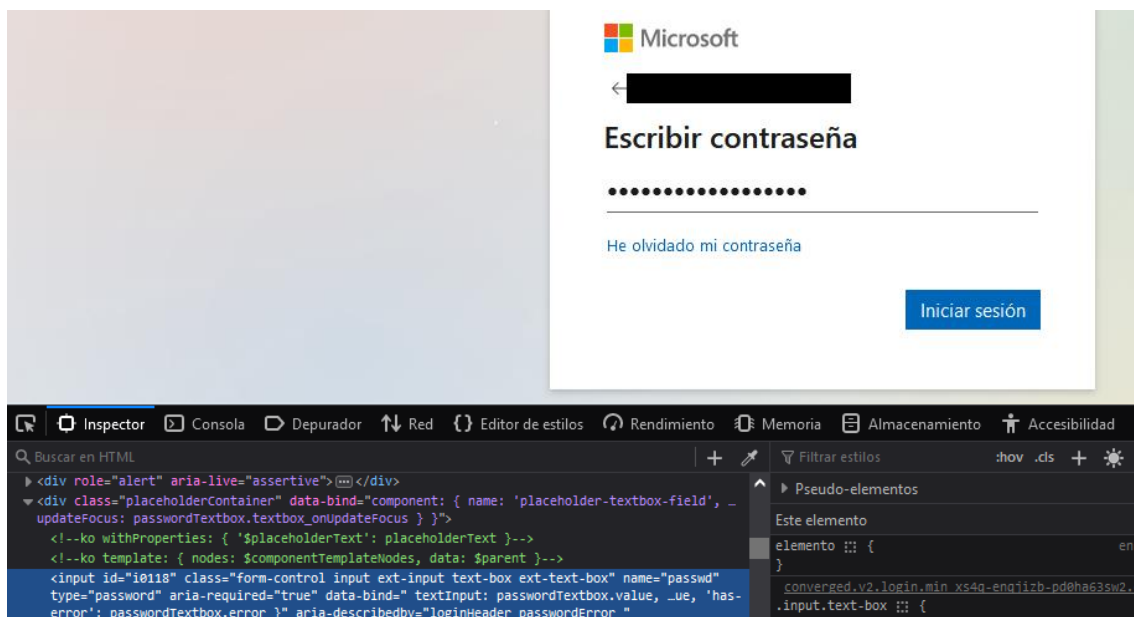


Ilustración 49: Contraseña oculta en login de Microsoft

Un login suele contar con 2 campos de texto, correspondiendo a un usuario y a una contraseña de acceso, cada uno siendo de un tipo diferente. El tipo del usuario es texto plano, y el tipo de la contraseña es texto plano con ocultación de los caracteres siendo reemplazados por asteriscos ("\*") o puntos ("•"). El elemento tiene un código HTML que es el siguiente:

```
<input type="text">  
<input type="password">
```

El primer campo de introducción de texto pertenece al usuario y el segundo a la contraseña. Ambos elementos tienen una variable designada en la que se guardan los valores introducidos por el usuario en el navegador. Desde la parte del cliente, es decir, desde el navegador se envían estos datos mediante un formulario al servidor, que es el que se encarga de procesar estos datos para dar acceso al usuario según si los datos introducidos son correctos o no en función de la comparación que este haga con sus propios datos y los proporcionados por el formulario de inicio de sesión.

Al modificar el código HTML desde las herramientas de desarrollo alteraremos su estado en la parte del cliente, es decir, desde la parte del navegador. Si seleccionamos el elemento de introducción de texto y cambiamos el valor del atributo *type* de *password* a *text* podemos revelar la contraseña ante nuestros ojos como se muestra en la Ilustración 50.

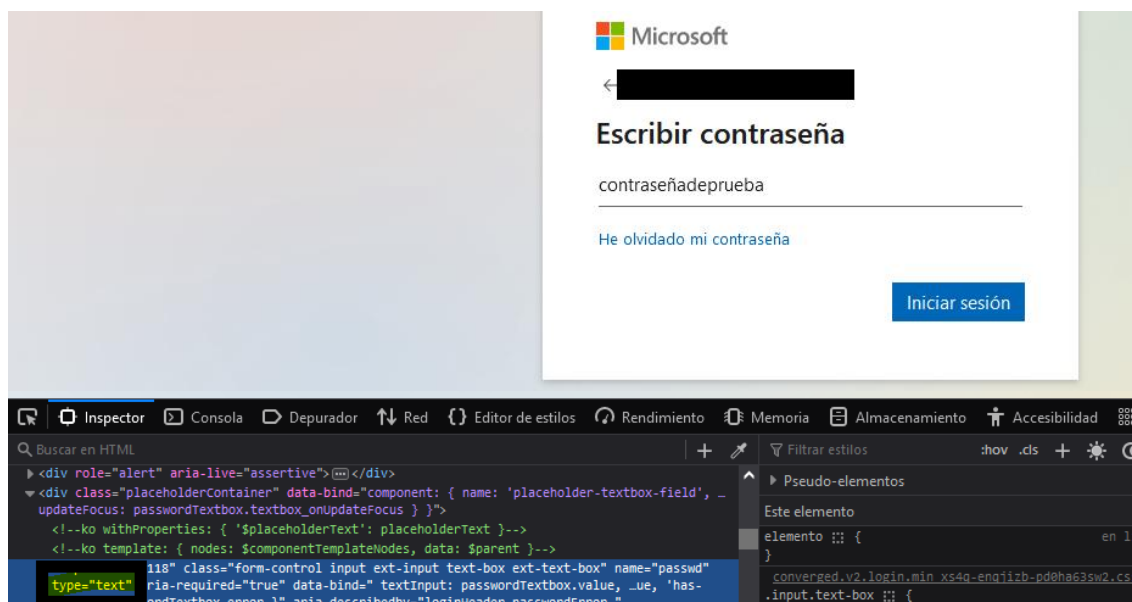


Ilustración 50: Contraseña visible en login de Microsoft

Mediante la recuperación de los pares usuario/contraseña se está permitiendo que se empleen esos datos para acceder a las cuentas personales del usuario que las haya guardado en el navegador, y si este usuario se trata de una persona que está siendo investigada por algún tipo de delito cibernético nos está proporcionando una llave que abre una puerta que esconde mucha información detrás.

Cabe destacar que en España y en la mayoría de los países, el acceso no autorizado a cuentas de usuario o sistemas informáticos sin el consentimiento del titular de la cuenta es considerado un delito. Esto se aplica a todas las personas, incluidos los

criminales investigados por cualquier tipo de delito. Sin embargo, en el contexto de una investigación forense realizada por profesionales autorizados y debidamente autorizados, el acceso a cuentas de usuario o sistemas informáticos puede estar permitido bajo ciertas condiciones siendo única y exclusivamente con el propósito de recopilar pruebas relevantes para la investigación. En este caso solo se haría pública la información que se toma como una evidencia en la investigación dejando de lado toda aquella información no relevante y sin revelar. El resto de la información que resulte relevante se emplearía tratándola de manera confidencial entre aquellas personas que formen parte de la investigación de forma que no trascienda una vez finalice la investigación o mientras esta siga en curso.

Además de estas consideraciones hoy en día es muy común el uso de sistemas de doble autenticación para iniciar sesión en las cuentas de usuario de multitud de servicios. Este es un método de seguridad que requiere que los usuarios proporcionen dos formas diferentes de verificación antes de permitir el acceso a una cuenta o sistema conocido como 2FA (2 Factor Authentication). Este enfoque aumenta significativamente la seguridad al agregar una capa adicional de protección más allá de la simple contraseña. La idea clave detrás de la autenticación de doble factor es que incluso si alguien descubre tu contraseña, no podrá acceder a tu cuenta a menos que también tenga acceso al segundo factor de autenticación, que suele ser más difícil de obtener. Se basa en la premisa de que para autenticarse se requiere de 2 elementos:

- Algo que sabes, como una contraseña o un PIN
- Algo que tienes, como un dispositivo físico

Los métodos comunes de autenticación suelen ser códigos de verificación por SMS, aplicaciones de autenticación que genera códigos de verificación que cambian cada cierto tiempo, llaves de seguridad físicas como tarjetas o dispositivos USB, o biometría como huellas dactilares o reconocimiento facial.

### **5.1.6 Recuperación y análisis de datos de navegación con Browser History Examiner**

Mediante este programa recuperaremos los datos del historial de navegación y de la memoria caché del navegador. Los navegadores web almacenan gran cantidad de información que emplean para su funcionamiento, ya sea por cuenta propia como por decisión del usuario, y esta herramienta nos permitirá averiguar de qué trata esta información.

Cuando ejecutamos el programa nos muestra una ventana emergente en la que nos pregunta si queremos generar un nuevo archivo de datos del historial o bien queremos cargar uno ya existente como se muestra en la ilustración 51:

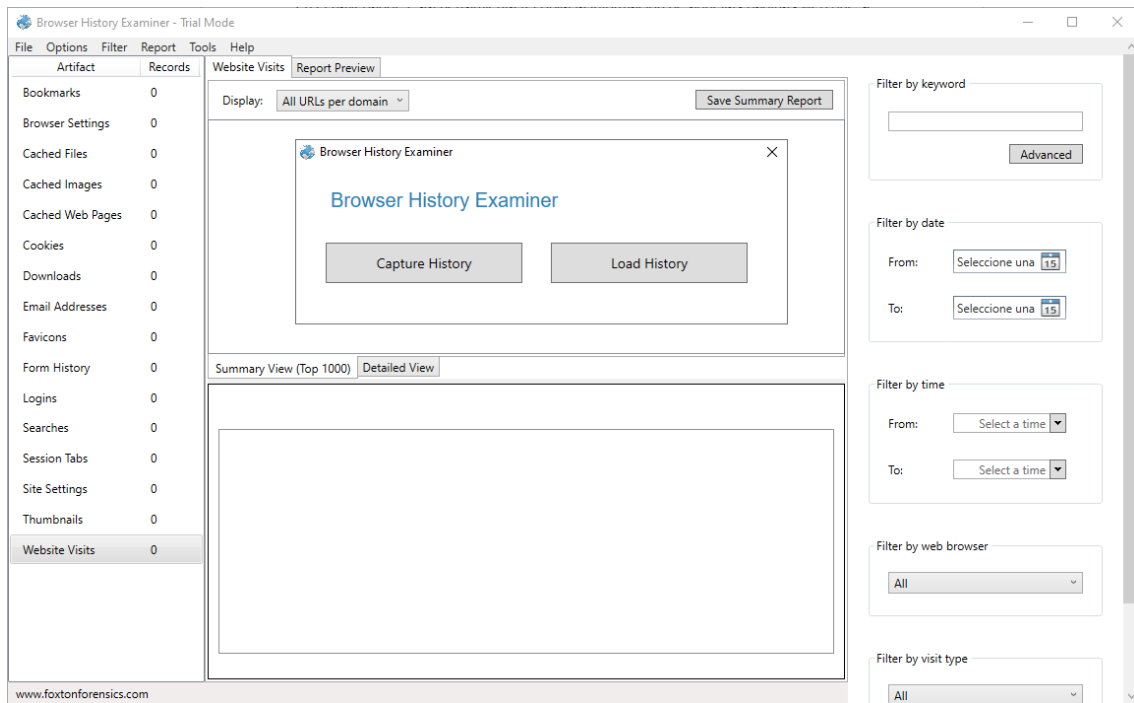


Ilustración 51: Ventana de inicio de Browser History Examiner

Una vez seleccionamos la opción de capturar el historial nos mostrará las opciones de captura. En este caso seleccionaremos capturar el historial de este ordenador, pero nos da la opción de seleccionar la captura de un disco lógico, es decir, de una partición del disco duro que tenemos montado en la máquina, e incluso de un ordenador accediendo remotamente a través de internet si este se encuentra en la misma red.

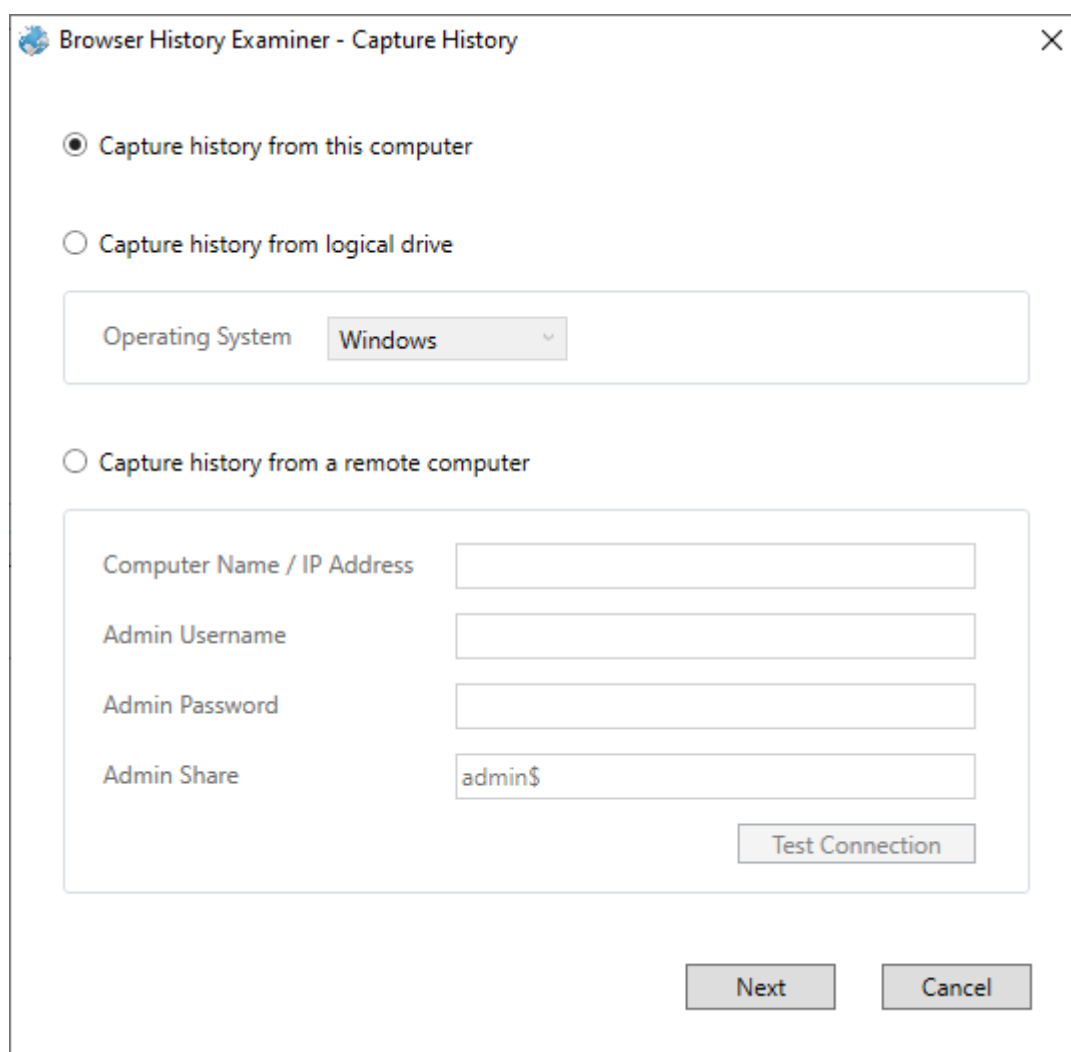


Ilustración 52: Opciones de captura

Tras escoger la opción de capturar el historial de este ordenador deberemos escoger el perfil del usuario del sistema del cual capturaremos los datos de exploración del navegador, marcando todos aquellos navegadores de los que queramos recuperar información y seleccionando una ruta de destino de la captura. Podemos escoger capturar la caché, el historial o ambas.

También dispone de una opción de recuperar los datos de exploración que hayan sido borrados recuperándolos desde las *Shadow Copies* (copias sombra o instantáneas) que son copias de seguridad de los volúmenes o de los archivos del sistema. Lamentablemente esta opción se trata de una funcionalidad de la versión de pago del programa, ya que en este caso estamos empleando la versión de prueba que nos permite realizar 25 capturas sin necesidad de activar el programa con una licencia de pago.

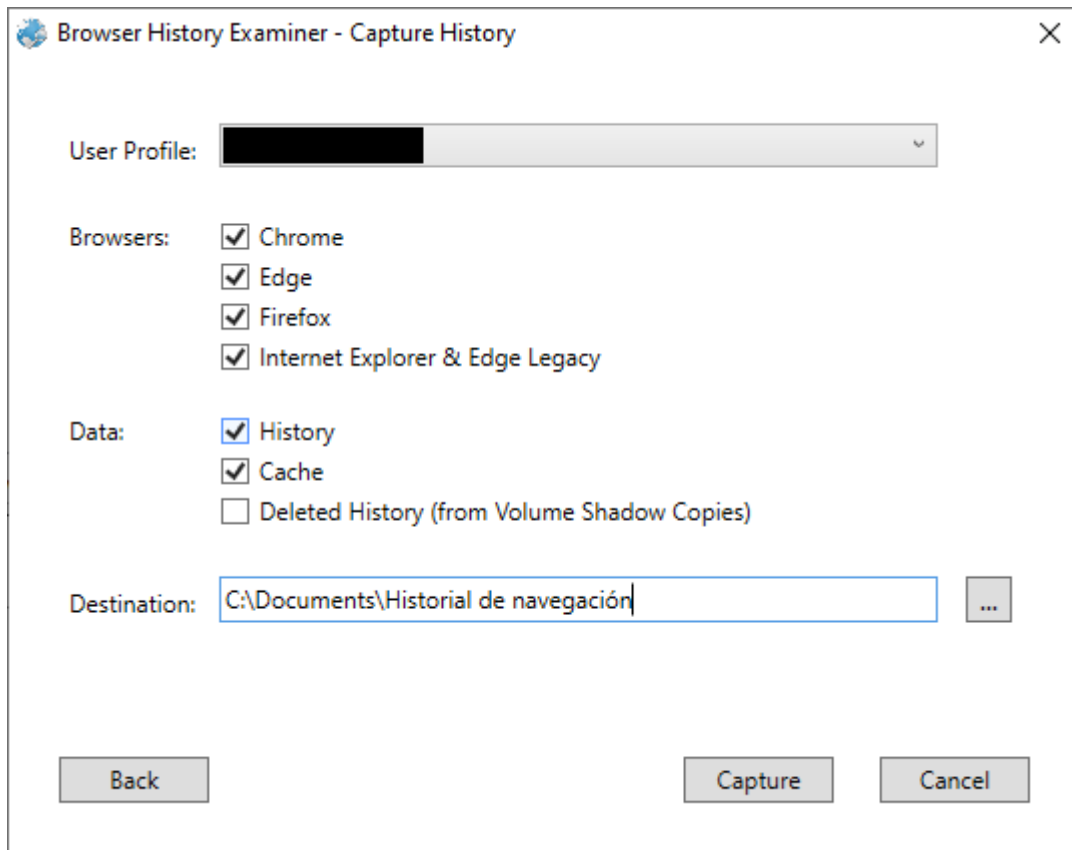


Ilustración 53: Opciones de captura avanzadas

Una vez hagamos click en el botón “*Capture*”, comenzará la captura de los datos:

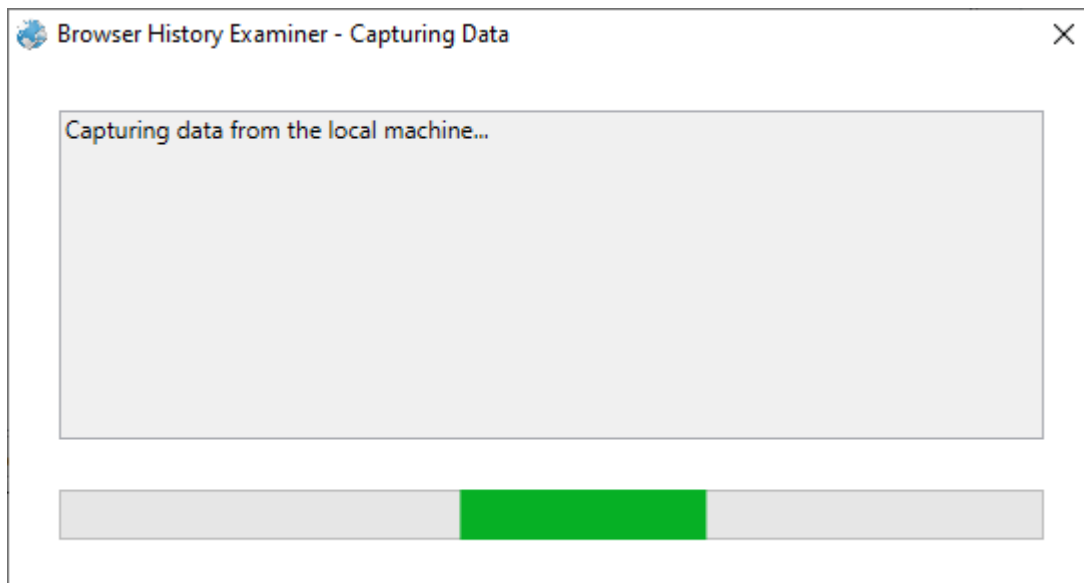


Ilustración 54: Captura de datos

Seleccionaremos cargar los datos recién capturados como muestra la Ilustración 55.



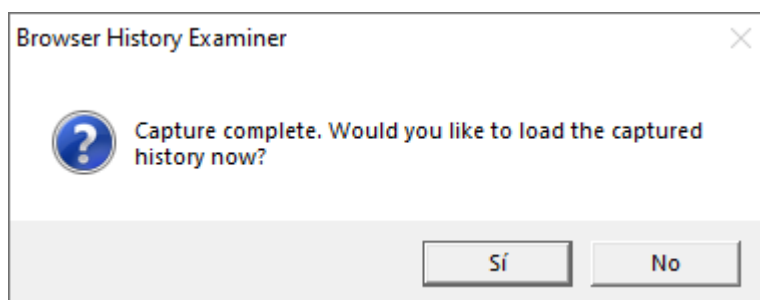


Ilustración 55: Carga del historial

Después de esto comenzará la carga y el procesamiento de los datos detallando el proceso conforme carga como se muestra en la Ilustración 56.

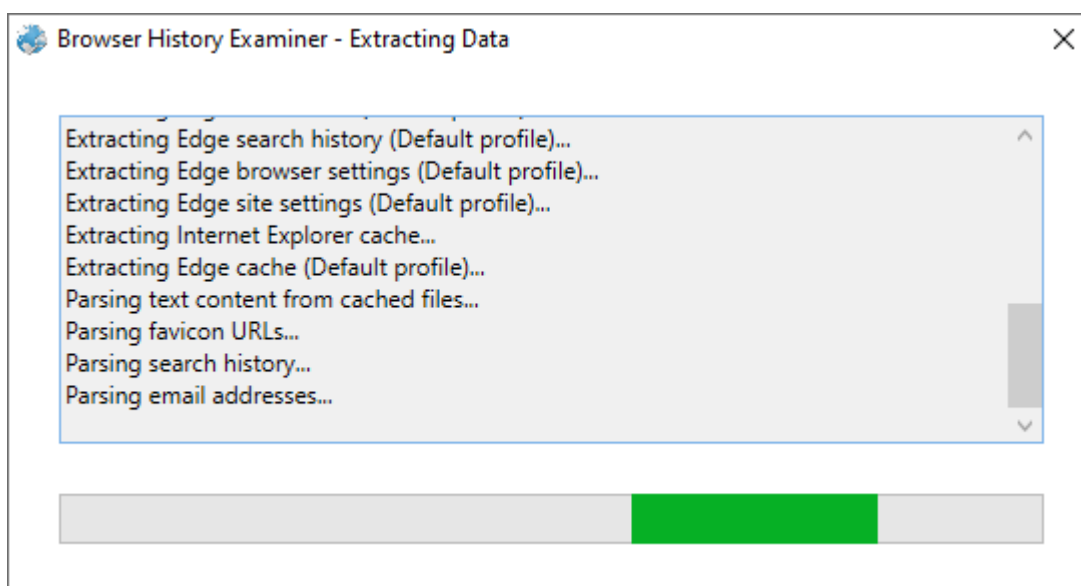


Ilustración 56: Extracción de datos de navegación

Tras la extracción de los datos del archivo de captura el programa nos mostrará la ventana principal con los datos recopilados en todas sus categorías. Entrando en materia veremos las pestañas de información más relevantes según la información que recopilan.

En primer lugar, veremos los marcadores del navegador, que se tratan de las URL de las páginas web que el usuario del navegador ha decidido almacenar en la memoria a modo de acceso directo a esa página web por si desea acceder a ella más tarde. En la Ilustración 57 vemos marcadores de webs de Microsoft acerca del uso de comandos o de software distribuido por la compañía, de ciertos estándares ISO relacionados con el peritaje informático o del portal de máquinas virtuales del DSIC que es proporcionado a los alumnos de la ETSINF en la UPV con el fin de emplearlas para las prácticas de algunas asignaturas.

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact	Records	Date Added	Last Modified	Title	URL	Web Browser (Profile)
Bookmarks	57					Edge (Default)
Browser Settings	14					Edge (Default)
Cached Files	10840	11/05/2023 21:05:58		Disk2vhd - Sysintern	https://learn.microsoft.com/en-us/sysintern	Edge (Default)
Cached Images	3496	22/07/2023 13:07:07		Get-FileHash (Micro	https://learn.microsoft.com/es-es/powerst	Edge (Default)
Cached Web Pages	236					Edge (Default)
Cookies	23	30/04/2023 16:15:07		Estándares nacionale	https://peritoinformaticocolegiado.es/blog	Edge (Default)
Downloads	33	30/04/2023 16:29:16		ISO 71505/2013-1. S	https://peritosinformaticos.es/iso-71505-2	Edge (Default)
Email Addresses	5	30/04/2023 16:29:24		ISO 71505/2013-2. B	https://peritosinformaticos.es/iso-71505-2	Edge (Default)
		30/04/2023 16:42:30		ISO 71505/2013-3. F	https://peritosinformaticos.es/iso-71505-2	Edge (Default)
		30/04/2023 16:13:44		ISO 71506/2013. Me	https://peritosinformaticos.es/iso-71506-2	Edge (Default)
		01/05/2023 10:20:14		Portal DSIC Cloud	https://portal-ng.dsic.upv.es/login/?next=	Edge (Default)

Ilustración 57: Marcadores del navegador

Podemos visualizar información acerca de la configuración interna del navegador. La Ilustración 58 muestra la cuenta de usuario de Outlook con la que se ha iniciado sesión en el navegador, la ruta donde se guardan los archivos descargados desde el navegador y otras configuraciones como la sincronización de los marcadores, extensiones, contraseñas, preferencias del usuario, entre otros.

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact	Records	Name	Value	Web Browser (Profile)
Bookmarks	57			
Browser Settings	14	Account Email (0)	[REDACTED]@outlook.com	Edge (Default)
		Account Name (0)		Edge (Default)
Cached Files	10840	Default File Save Directory	Downloads	Edge (Default)
Cached Images	3496	Last File Select Directory	Downloads	Edge (Default)
Cached Web Pages	236	Last Sync Time	25/07/2023 20:05:43	Edge (Default)
Cookies	23	Profile Creation Time	15/06/2021 13:51:00	Edge (Default)
Downloads	33	Profile Last Engagement Time	25/07/2023 19:04:00	Edge (Default)
Email Addresses	5	Sync Autofill	Yes	Edge (Default)
Favicons	92	Sync Bookmarks	Yes	Edge (Default)
Form History	37	Sync Extensions	Yes	Edge (Default)
		Sync Passwords	Yes	Edge (Default)
		Sync Preferences	Yes	Edge (Default)
		Sync Tabs	Yes	Edge (Default)
		Sync Typed URLs	Yes	Edge (Default)

Ilustración 58: Configuración del navegador

Veremos también las imágenes almacenadas en caché, especificando la ruta de la cual se han obtenido. Podemos observar una gran cantidad de imágenes provenientes de la web de MSN de Microsoft, así como de la web de la Agencia Tributaria del Gobierno de España como se muestra en la Ilustración 59.

## Análisis forense de la huella digital de un usuario en sistemas informáticos

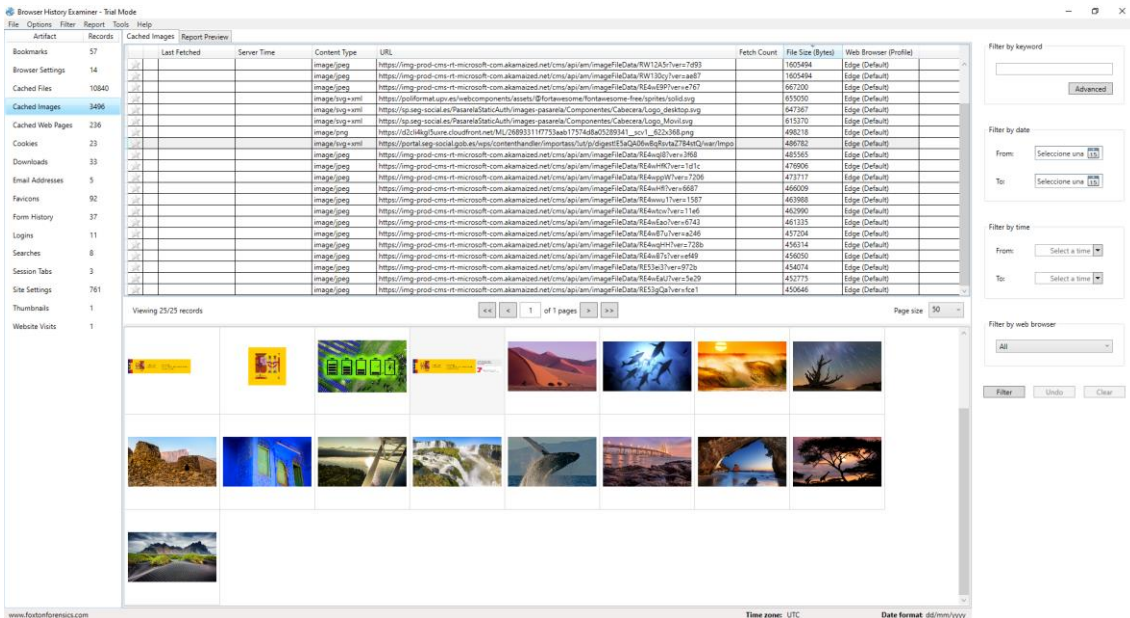


Ilustración 59: Imágenes en caché

Es posible visualizar las páginas almacenadas en caché como muestra la Ilustración 60.

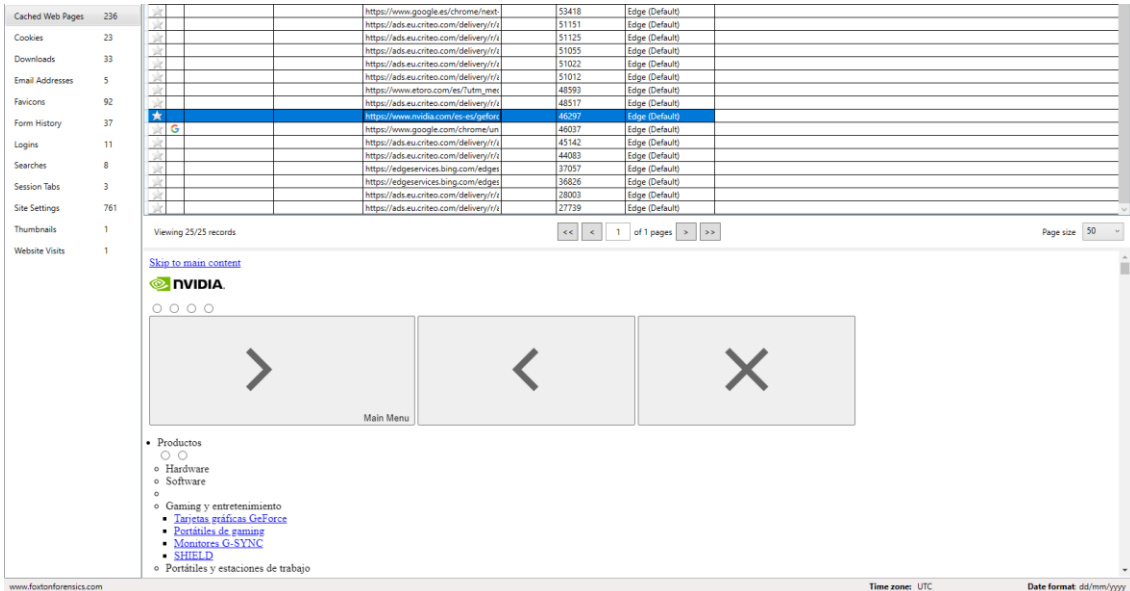


Ilustración 60: Páginas en caché

En este caso visualizamos una página web de Nvidia, empresa dedicada principalmente al diseño de tarjetas gráficas. También se puede apreciar que la mayoría de las páginas almacenadas en caché se tratan de anuncios del navegador de los motores de búsqueda Bing y Google.

En la Ilustración 61 veremos las cookies almacenadas y su contenido.

Artifact	Records	Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser
Bookmarks	57	13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	MUID	348FD582537D6F9F2481C70552566603	Edge Legacy
Browser Settings	14	24/07/2023 16:07:40	www.bing.com/	24/07/2023 16:07:40	09/03/2024 18:08:26	MUID	348FD582537D6F9F2481C70552566603	Edge Legacy
Cached Files	10840	13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	EDGE_V	1	Edge Legacy
Cached Images	3496	13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	SRCHID	AF=NOFORM	Edge Legacy
Cached Web Pages	236	13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	SRCHUID	V=2&GUID=CC9576AA89DC41E2A594F21E717A58A0&dmchq=1	Edge Legacy
		13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	SRCHUSR	DOB=20230213	Edge Legacy
		13/02/2023 18:08:26	bing.com/	13/02/2023 18:08:26	09/03/2024 18:08:26	SRCHHPGUSR	SRCHLANG=es	Edge Legacy
Cookies	23	25/07/2023 20:07:04	win-rar.com/	25/07/2023 20:07:04	24/07/2024 20:07:04	jsrr	#HofwvENACEBMMCCCLshhggp97zr5cmgMghoMsk6SugU97LGP3ZFR%2FOZBZChLcn4DAA2VwDv%3D	Edge Legacy
		11/05/2023 21:05:16	win-rar.com/	11/05/2023 21:05:16	10/05/2025 21:05:16	jsr	GA1.2.466047862.1679405706	Edge Legacy
Downloads	33	24/07/2023 16:07:40	bing.com/	24/07/2023 16:07:40	25/07/2023 04:07:39	SUID	M	Edge Legacy

Ilustración 61: Cookies del navegador

También podremos ver los archivos descargados desde el navegador además de su ruta de descarga. Como podemos ver en la Ilustración 62, nos encontramos con un certificado digital, el ejecutable del cliente P2P qbittorrent y algunos archivos PDF, siendo uno de ellos contenido sensible al contener datos de carácter personal como los datos de la Seguridad Social de un individuo.

Artifact	Records	Date Created	File Name	Status	Date Accessed	Date Expires	Size	Web Browser
Downloads	33	17/01/2023 19:35:33	[redacted].ciudadano	Complete	17/01/2023 19:35:33		3608	Edge (Default)
		17/01/2023 19:32:44	[redacted].ciudadano	Complete	17/01/2023 19:32:44		3608	Edge (Default)
		10/12/2022 21:01:30	Downloads\qbittorrent_4.5.0_y64_setup.exe	Complete	10/12/2022 21:01:30		29241578	Edge (Default)
Email Addresses	5	09/12/2022 20:09:28	Downloads\Seguridad social.pdf	Complete	09/12/2022 20:09:28		109042	Edge (Default)
		06/12/2022 19:45:21	Downloads\Tablero en blanco.pdf	Complete	06/12/2022 19:45:21		115692	Edge (Default)
Favicons	92	06/12/2022 19:05:39	Downloads\Tablero en blanco.pdf	Complete	06/12/2022 19:05:39		115705	Edge (Default)
Form History	37	01/12/2022 17:14:42	Downloads\ [redacted]	Complete	01/12/2022 17:14:42		2840657	Edge (Default)

Ilustración 62: Descargas del navegador

Por otra parte, es posible recuperar direcciones de correo electrónico de varias fuentes, como caché, historial de navegación o configuración del navegador.

Artifact	Records	Last Used	Email Address	Domain	Source	Web Browser (Profile)
Bookmarks	57	12/01/2023 16:58:18	[redacted]@gmail.com		Form History	Edge (Default)
Browser Settings	14	22/06/2022 16:34:07	[redacted]@gmail.com		Form History	Edge (Default)
Cached Files	10840		[redacted]@outlook.com	graph.microsoft.co	Cache	Edge (Default)
Cached Images	3496		bootstrap@5.3.0-alpha1	cdn.jsdelivr.net	Cache	Edge (Default)
Cached Web Pages	236		[redacted]@outlook.com		Browser Setting	Edge (Default)
Cookies	23					
Downloads	33					
Email Addresses	5					

Ilustración 63: Direcciones de correo

En la Ilustración 63 vemos todas las direcciones de correo que se han recuperado, además de indicar la fuente de la cual provienen.

Del mismo modo que se almacenan los marcadores también se almacena su *favicon*, que se trata del icono que aparece acompañando a las páginas web para facilitar su identificación en las pestañas, marcadores, buscador, etc.



En la ilustración 64 podemos ver los iconos de Lowi, Steam y la Generalitat Valenciana, con sus respectivas URL de las cuales se ha descargado este icono:

Artifact	Records	Favicons	Report Preview
Bookmarks	57		
Browser Settings	14		
Cached Files	10840		
Cached Images	3496		
Cached Web Pages	236		
Cookies	23		
Downloads	33		
Email Addresses	5		
Favicons	92		

URL	Page URL	Expires	Last Updated	Web Browser (Profile)
http://192.168.0.	http://192.168.0.			Edge (Default)
http://192.168.0.	http://192.168.0.			Edge (Default)
https://store.stea	https://store.stea			Edge (Default)
https://store.stea	https://store.stea			Edge (Default)
https://labora.gv	https://labora.gv			Edge (Default)
https://labora.gv	https://labora.gv			Edge (Default)

Ilustración 64: Favicons

Son recuperables algunos datos que se han introducido en formularios web. La Ilustración 65 muestra direcciones de correo, un NIF, nombres de usuario, respuestas a preguntas de seguridad para recuperación de cuentas de usuario, códigos de autenticación de un solo uso y hasta el IBAN de una cuenta bancaria.

Artifact	Records	Form History	Report Preview
Bookmarks	57		
Browser Settings	14		
Cached Files	10840		
Cached Images	3496		
Cached Web Pages	236		
Cookies	23		
Downloads	33		
Email Addresses	5		
Favicons	92		
Form History	37		
Logins	11		
Searches	8		
Session Tabs	3		
Site Settings	761		
Thumbnails	1		
Website Visits	1		

Field Name	Value	First Used	Calculated Domain (First Used)	Last Used	Calculated Domain (Last Used)	Times Used	Web Browser (Profile)
t	7hu3jk	21/03/2023 19:21:45		21/03/2023 19:21:45		1	Edge (Default)
t	5	21/03/2023 17:31:42		21/03/2023 17:31:42		1	Edge (Default)
t	8pqp	04/03/2023 23:00:34		04/03/2023 23:00:34		1	Edge (Default)
nif	[REDACTED]	17/01/2023 19:31:58		17/01/2023 19:31:58		1	Edge (Default)
codigo0	43LJ9	17/01/2023 19:31:58		17/01/2023 19:31:58		1	Edge (Default)
codigo1	v7te6	17/01/2023 19:31:58		17/01/2023 19:31:58		1	Edge (Default)
cke_167_textinput	19	14/01/2023 18:08:00		14/01/2023 18:08:00		1	Edge (Default)
cke_170_textinput	45	14/01/2023 18:07:19		14/01/2023 18:08:00		1	Edge (Default)
cke_167_textinput	7	14/01/2023 18:07:19		14/01/2023 18:07:19		1	Edge (Default)
login-username	[REDACTED]@gmail.com	12/01/2023 16:58:18		12/01/2023 16:58:18		1	Edge (Default)
balance_return_iban(ibn)	65	21/11/2022 18:29:31		21/11/2022 18:29:31		1	Edge (Default)
cke_113_textinput	4	19/10/2022 16:55:06		19/10/2022 17:21:16		3	Edge (Default)
cke_110_textinput	7	19/10/2022 17:20:55		19/10/2022 17:21:16		2	Edge (Default)
cke_110_textinput	4	19/10/2022 17:19:58		19/10/2022 17:20:18		2	Edge (Default)
cke_113_textinput	8	19/10/2022 17:19:58		19/10/2022 17:20:18		2	Edge (Default)
cke_110_textinput	38	19/10/2022 16:55:06		19/10/2022 16:55:06		1	Edge (Default)
uid_21	364483	09/10/2022 18:04:09		09/10/2022 18:04:09		1	Edge (Default)
username	[REDACTED]	05/10/2022 07:49:57		05/10/2022 07:49:57		1	Edge (Default)
username	[REDACTED]	05/10/2022 06:46:07		05/10/2022 06:46:17		1	Edge (Default)
username	[REDACTED]	26/09/2022 18:10:40		26/09/2022 11:19:04		2	Edge (Default)
battletag	[REDACTED]	14/09/2022 18:44:54		14/09/2022 18:44:54		1	Edge (Default)
answer	[REDACTED]	14/09/2022 18:42:12		14/09/2022 18:42:12		1	Edge (Default)
authcode	[REDACTED]	29/07/2022 18:10:54		29/07/2022 18:10:54		1	Edge (Default)
homeIP1	192	29/06/2022 23:26:26		29/06/2022 23:26:26		1	Edge (Default)
homeIP2	168	29/06/2022 23:26:26		29/06/2022 23:26:26		1	Edge (Default)

Ilustración 65: Datos de formularios

Para finalizar con la información relevante, se pueden visualizar los inicios de sesión en las diferentes URL que se han visitado con el navegador. En estas se almacena la URL a la que se accede, el navegador desde el que se ha accedido a esa URL y el usuario con el que se inicia la sesión. En la Ilustración 66 podemos ver que se ha iniciado sesión en varios servicios de la UPV, la plataforma Steam, GitHub, PayPal, el escritorio remoto de Google y la página de configuración de un router.

Artifact	Records	Logins	Report Preview
Bookmarks	57		
Browser Settings	14		
Cached Files	10840		
Cached Images	3496		
Cached Web Pages	236		
Cookies	23		
Downloads	33		
Email Addresses	5		
Favicons	92		
Form History	37		
<b>Logins</b>	<b>11</b>		
Searches	8		

Ilustración 66: Inicios de sesión

Tras recopilar la información de uso del navegador nos podemos dar cuenta de la cantidad de información que estos pueden llegar a almacenar sin que el usuario lo sepa. Esta información puede tratarse tanto de datos cifrados como las cookies o bien pueden tratarse de datos de carácter personal como cuentas bancarias o números de identificación personal. Estos últimos al ser datos de carácter personal nos permiten tener identificado al usuario ya que un DNI y una cuenta de banco son fácilmente identificables por las autoridades pertinentes, siempre y cuando el tratamiento de estos datos personales por parte del perito informático sea con fines de investigación y el tratamiento de estos sea legítimo, siempre justificado con el correspondiente informe para justificar su inocencia en el acceso a estos datos.

### 5.1.7 Visualización de metadatos con ExifTool

Gracias a esta herramienta de línea de comandos podemos ver los metadatos de los archivos que queramos analizar. Este programa es compatible con una gran cantidad de formatos de archivo diferentes, pero este es empleado mayormente con imágenes y documentos de texto, ya que de estos se puede obtener una gran cantidad de metadatos en comparación a otros tipos de archivo. Por ese motivo vamos a analizar los metadatos de este tipo de archivos y la información que recopilamos.

Para ejecutar una instancia del programa deberemos emplear la consola del sistema para abrir el ejecutable con ella. No obstante, con eso no basta, ya que cada ejecución del programa debe de ir acompañada de argumentos, y como mínimo debe de ser el nombre del archivo y su formato. Hay que mencionar que este programa también permite la modificación, agregación y borrado de metadatos, pero no usaremos los comandos designados para estas tareas, ya que el objetivo es mostrar la información de los metadatos de la imagen y mantenerlos intactos.

Por ejemplo, si quisiéramos visualizar los metadatos de una imagen en formato .jpg escribiríamos el comando de la siguiente manera:

```
exiftool.exe -lang es -t imagen.jpg
```

Donde el lenguaje es español, el archivo se llama imagen y el formato de salida es en tabla. Este comando se ejecuta directamente desde la ruta donde se encuentra el archivo ejecutable `exiftool.exe` y los archivos a analizar. Tras este ejemplo veamos la información de archivos reales como el de la imagen que se muestra en la Ilustración 67.

```
C:\Users\      \Desktop\exiftool>exiftool.exe -lang es -t IMG_20230826_225330.jpg
Versión ExifTool      12.65
Nombre Archivo      IMG_20230826_225330.jpg
Ubicación del Fichero      .
Tamaño Archivo      4.0 MB
Fecha Actualización      2023:08:26 22:53:31+02:00
Fecha y Hora de Acceso      2023:08:26 22:55:48+02:00
Fecha y Hora de Creación      2023:08:26 22:55:47+02:00
Permisos      -rw-rw-rw-
Tipo Archivo      JPEG
File Type Extension      jpg
MIME Type      image/jpeg
Exif Byte Order      Big-endian (Motorola, MM)
Unidad de Resolución de X e Y      Pulgada
Marca      Xiaomi
Modelo      M2012K11AG
```

Ilustración 67: Análisis de imagen con ExifTool

En detalle podemos observar en la Ilustración 67 que la ubicación del fichero que es la misma que la del programa representada por un punto, que indica que se encuentra en el directorio actual. Podemos ver las fechas de actualización, creación y acceso del archivo, además de los permisos que tiene para los usuarios del sistema que son de lectura y escritura para propietario, grupo y otros usuarios. Al tratarse de una imagen podemos recopilar datos más interesantes como la marca y el modelo del dispositivo con el que se ha realizado la fotografía, que en este caso es un móvil Xiaomi modelo M2012K11AG.

Como podemos ver en la Ilustración 68, también se obtienen datos de configuración de la cámara en el momento de tomar la imagen como la distancia focal, si se ha disparado flash, el tipo de captura, apertura de la lente, balance de blancos, entre otros. Otros datos de interés son la fecha de captura de la imagen y su tamaño en alto y ancho de imagen que en este caso corresponde a una imagen del tamaño de 3000x4000 píxeles.



```

Distancia Focal Objetivo      4.7 mm
Flash      Flash no disparado, modo flash forzado
Fuente Luz      D65
Modo Medición Media ponderada al centro
Tipo Captura Escena      Estándar
Identificación Interoperabilidad      R98: Archivo binario DCF (sRGB)
Versión Interoperabilidad      0100
Distancia Focal en Película de 35 mm      26 mm
Apertura Lente Máxima      1.8
Fecha y Hora de Datos Digital      2023:08:26 22:53:30
Compensación Exposición      0
Alto Imagen      4000
Balance de Blancos      Automático
Fecha y Hora de Datos Original      2023:08:26 22:53:30
Luminosidad      -3.26
Ancho Imagen      3000
Modo Exposición      Exposición automática
Apertura      1.8

```

Ilustración 68: Metadatos imagen

Además de toda la información anterior es posible obtener datos de geolocalización si la foto se ha tomado con los ajustes de ubicación activados en el teléfono. Los datos para destacar son la fecha y hora GPS y las coordenadas GPS en latitud y longitud, que permiten saber el lugar aproximado donde se ha hecho la foto.

```

Longitud Este u Oeste      Longitud Oeste
Referencia Altitud      Nivel del Mar
Hora GPS (reloj atómico)      20:53:27
Nombre del Método de Procesado GPS      CELLID
Fecha GPS      2023:08:26
Resolución Imagen Horizontal      72
Resolución Imagen Vertical      72
Thumbnail Offset      5670
Thumbnail Length      16955
Compresión      JPEG (estilo antiguo)
Ancho Imagen      3000
Alto Imagen      4000
Proceso de codificación      Baseline DCT, Huffman coding
Número de Bits Por Muestra      8
Componentes de Color      3
Ratio Submuestreo de Y a C      YCbCr4:2:0 (2 2)
Apertura      1.8
Tamaño de la Imagen      3000x4000
Megapixels      12.0
Scale Factor To 35 mm Equivalent      5.5
Tiempo de Exposición      1/20
Create Date      2023:08:26 22:53:30.684
Date/Time Original      2023:08:26 22:53:30.684
Modify Date      2023:08:26 22:53:30.684
Miniatura      (Binary data 16955 bytes, use -b option to extract)
Altitud 108 m Above Sea Level
Fecha y Hora GPS      2023:08:26 20:53:27Z
Latitud      N
Longitud      W
Circle Of Confusion      0.005 mm
Angulo de Visión      69.4 deg
Longitud Focal (Conversión a 35 mm)      4.7 mm (35 mm equivalent: 26.0 mm)
GPS Position      W
Distancia Hiperfocal      2.29 m
Light Value      2.6

```

Ilustración 69: Coordenadas GPS en metadatos



Pasemos ahora a analizar los metadatos de un documento de texto.

En la Ilustración 70 la información para destacar son las fechas de creación, último acceso y actualización del documento, sus permisos de archivo, el título del documento, el creador del documento, el último usuario que ha modificado el documento, la compañía a la que pertenece, la aplicación con la que ha sido creado, si el documento está protegido, si está compartido con otros usuarios, si parte de una plantilla, y el número de líneas, párrafos y de caracteres contando los espacios.

Los creadores y los usuarios se muestran con su nombre completo, por lo que esto puede llevar a identificar o a poder saber más de una persona conociendo su nombre y la compañía para la que trabaja con unas simples búsquedas en internet.

```
C:\Users\ \Desktop\exiftool>exiftool.exe -lang es -t U0702141.docx
Versión ExifTool 12.65
Nombre Archivo U0702141.docx
Ubicación del Fichero .
Tamaño Archivo 1858 kB
Fecha Actualización 2023:08:13 18:46:31+02:00
Fecha y Hora de Acceso 2023:08:30 18:35:07+02:00
Fecha y Hora de Creación 2023:08:30 18:32:20+02:00
Permisos -rw-rw-rw-
Tipo Archivo DOCX
File Type Extension docx
MIME Type application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version 20
Zip Bit Flag 0x0006
Compresión Zip Deflated
Zip Modify Date 1980:01:01 00:00:00
Zip CRC 0xf27430e3
Zip Tamaño Comprimido 521
Zip Tamaño Descomprimido 3817
Zip File Name [Content_Types].xml
Título
Creador
Last Modified By
Número Revisión 2
Last Printed 2012:05:02 09:48:00Z
Fecha y Hora de Datos Digital 2023:08:13 16:46:00Z
Fecha y Hora de Cambio del Archivo 2023:08:13 16:46:00Z
Template Normal
Total Edit Time 0
Pages 39
Words 11234
Characters 61787
Application Microsoft Office Word
Doc Security Ninguno
Lines 514
Paragraphs 145
Scale Crop No
Heading Pairs Título, 1
Titles Of Parts
Company
Links Up To Date No
Characters With Spaces 72876
Shared Doc No
Hyperlinks Changed No
App Version 16.0000
ContentTypeId 0x010100FADE71AC1723FF488EC6D94255A5FB04
```

Ilustración 70: Metadatos documento de texto Word

También es posible extraer la información de los metadatos de un archivo redirigiendo la salida de la consola a un archivo externo con los siguientes comandos:

```

C:\Users\ \Desktop\exiftool>exiftool.exe -lang es -h IMG_20230826_225330.jpg > metadata.html
C:\Users\ \Desktop\exiftool>exiftool.exe -lang es -T IMG_20230826_225330.jpg > metadata.csv
C:\Users\ \Desktop\exiftool>exiftool.exe -lang es -t IMG_20230826_225330.jpg > metadata.txt
C:\Users\ \Desktop\exiftool>

```

Ilustración 71: Comandos de extracción de metadatos en diferentes formatos

Esta información se puede exportar en archivos con formato html, csv y txt. Los modificadores del comando hacen que la información se muestre en diferentes formatos usando -T y -h para formatear la salida del programa en tabla o código HTML respectivamente. La ejecución de los comandos anteriores crea los siguientes archivos:




	metadata	26/08/2023 23:05	Archivo de valores separados por comas de Microsoft Excel
	metadata	26/08/2023 23:04	Microsoft Edge HTML Document
	metadata	26/08/2023 23:05	Documento de texto

Ilustración 72: Extracción de metadatos en archivos de diversos formatos

Si los abrimos se muestran en su formato correspondiente. Por ejemplo, si abrimos el archivo HTML con un navegador este interpretará el código y generará una página estática con el siguiente aspecto:

C:/Users/ /Desktop/exiftool/metadata.html	
Versión ExifTool	12.65
Nombre Archivo	IMG_20230826_225330.jpg
Ubicación del Fichero	.
Tamaño Archivo	4.0 MB
Fecha Actualización	2023:08:26 22:53:31+02:00
Fecha y Hora de Acceso	2023:08:26 23:03:37+02:00
Fecha y Hora de Creación	2023:08:26 22:55:47+02:00
Permisos	-rw-rw-rw-
Tipo Archivo	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Unidad de Resolución de X e Y	Pulgada
Marca	Xiaomi
Modelo	M2012K11AG
Orientación de Imagen	0° (arriba/izquierda)
Fecha y Hora de Cambio del Archivo	2023:08:26 22:53:30

Ilustración 73: Metadatos en formato HTML

Como conclusión, esta herramienta nos permite obtener grandes cantidades de información de archivos personales como son las imágenes digitales y los documentos de texto, por lo que resulta muy interesante para profundizar en una investigación forense dado que nos proporciona datos de carácter personal como nombre y apellidos, empresa, incluso la ubicación GPS en el momento de la toma de una imagen.

Esto ha llegado a ser un problema para algunos famosos que han llegado a subir una imagen en su domicilio compartiendo sus metadatos de posicionamiento GPS, motivo por el que cualquier persona que pudiese descargarse el archivo de esa red social y que dispusiera de los conocimientos mínimos necesarios para analizar y extraer los metadatos del archivo podría averiguar dónde vive su famoso favorito, pero no obstante esto es un problema de privacidad para cualquier usuario. Esto cada vez es menos habitual ya que por políticas de las redes sociales estas se suben sin compartir los metadatos incluso si la foto ha sido tomada con la ubicación activada en el teléfono y la ubicación GPS ha sido registrada, por lo que al subir una foto o compartirla con nuestros contactos solamente recibirán la imagen y esta solo contendrá los metadatos imprescindibles.

En la Ilustración 74 se muestran los metadatos que alberga una imagen compartida por WhatsApp.

```
C:\Users\      \Desktop\exiftool>exiftool.exe "Imagen de WhatsApp.jpg"
ExifTool Version Number      : 12.65
File Name                    : Imagen de WhatsApp.jpg
Directory                    : .
File Size                    : 357 kB
Zone Identifier              : Exists
File Modification Date/Time   : 2023:08:30 20:26:19+02:00
File Access Date/Time        : 2023:08:30 20:30:17+02:00
File Creation Date/Time      : 2023:08:30 20:29:00+02:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 2048
Image Height                  : 1536
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                    : 2048x1536
Megapixels                    : 3.1
```

*Ilustración 74: Metadatos imagen de WhatsApp*

Con esto queda demostrado que no se transfieren metadatos con información más allá de la necesaria a ningún otro usuario al que le enviemos una imagen personal a través de WhatsApp.

### 5.1.8 Volcado de memoria RAM con AccessData FTK Imager/AVML (Acquire Volatile Memory for Linux) y extracción de información con Volatility

Para llevar a cabo esta tarea emplearemos tres herramientas, que serán AccessData FTK Imager, AVML [23] y Volatility.

Como el volcado de memoria es otra de las funcionalidades del programa utilizaremos AccessData FTK Imager en Windows para obtener la imagen de la información de la memoria RAM en un momento concreto. Esto consiste en copiar el contenido de la memoria principal en un fichero que después podrá ser analizado para extraer la información del estado de la máquina en el momento en el que se ha realizado este volcado de memoria.

En el caso de AVML se trata de una herramienta portable de Microsoft que es compatible con sistemas Linux. Esta herramienta se emplea para la adquisición de imágenes de memoria sin necesidad de saber el sistema operativo objetivo, por lo que es compatible con varias distribuciones de Linux como Ubuntu, Centos, RedHat, Debian, entre otras.

Una vez tengamos nuestro archivo de volcado podremos analizar los datos mediante la potente herramienta de línea de comandos Volatility. Esta herramienta nos permite extraer gran variedad de información de las imágenes de memoria como por ejemplo de procesos en ejecución, información del sistema o hashes de las contraseñas de los usuarios del sistema.

Podemos realizar un volcado de memoria tanto en Linux como en Windows. Hace falta destacar que el análisis de los archivos de volcado se realiza en ambos sistemas con Volatility, pero la obtención de la imagen de memoria se hace con herramientas diferentes en cada sistema.

Para obtener el volcado de memoria en Windows ejecutamos el programa AccessData FTK Imager y en el menú desplegable *File* seleccionamos la opción de *Capture Memory*.

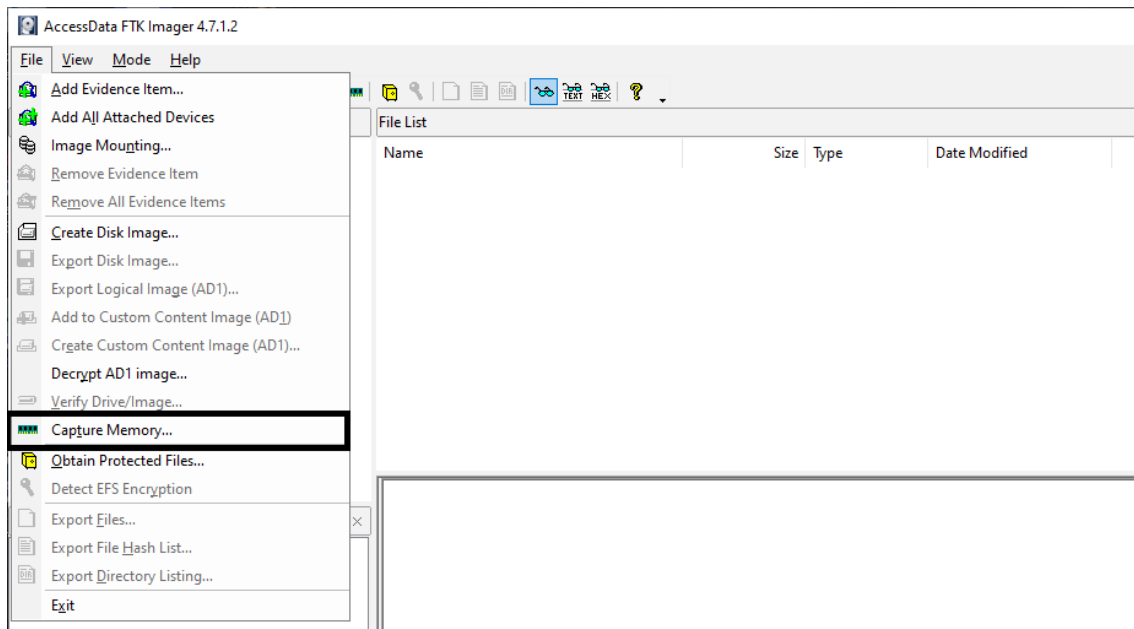


Ilustración 75: Volcado de memoria con AccessData FTK Imager

Seleccionamos la ruta en la que se guardará el archivo de volcado y el nombre del archivo. Tras esto pulsaremos en el botón de *Capture Memory* para comenzar el proceso.

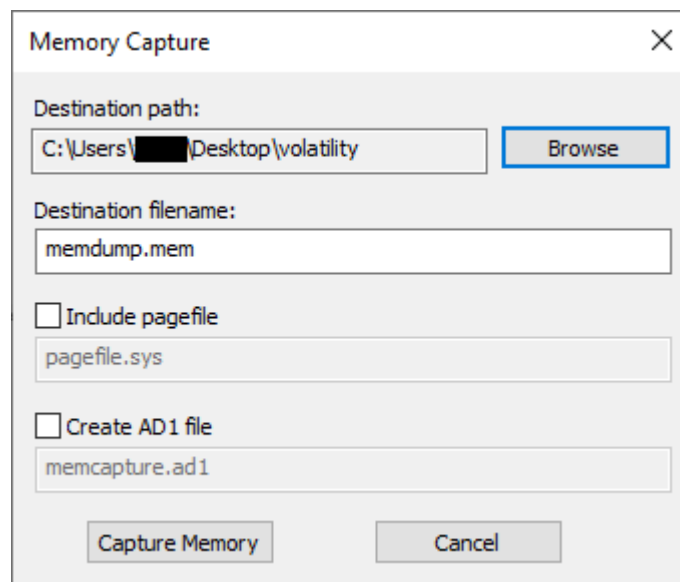


Ilustración 76: Captura de memoria

Una vez iniciado el proceso la duración dependerá de la capacidad de la CPU y de la cantidad de memoria RAM que disponga el sistema. Cuando finalice el proceso cerramos la ventana y ya disponemos de nuestra imagen de memoria.

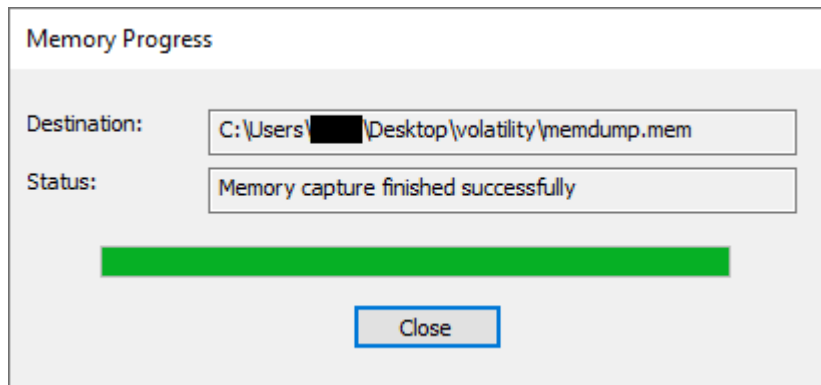


Ilustración 77: Captura de memoria finalizada

Para obtener la imagen de memoria en Linux en primer lugar adquiriremos AVML. Para ello nos descargaremos los archivos del repositorio oficial de GitHub mediante la herramienta wget, que nos permitirá recuperar esos archivos del repositorio.

Una vez hayamos descargado los archivos comprobamos que se encuentren en la ruta actual como se muestra en la ilustración 78:

```

user@ubuntu:~$ wget https://github.com/microsoft/avml/releases/download/v0.9.0/avml
--2023-09-03 20:34:42-- https://github.com/microsoft/avml/releases/download/v0.9.0/avml
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/190660866/d0ed95a5-a1fd-4996-9ada-333aa736a2ef?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230903%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230903T183442Z&X-Amz-Expires=300&X-Amz-Signature=db7a41847f06ee1719ac8f1f9f7378532e26b347dd495492e6782038f97a1c4c&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=190660866&response-content-disposition=attachment%3Bfilename%3Ddavml&response-content-type=application%2Foctet-stream [following]
--2023-09-03 20:34:42-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/190660866/d0ed95a5-a1fd-4996-9ada-333aa736a2ef?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230903%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230903T183442Z&X-Amz-Expires=300&X-Amz-Signature=db7a41847f06ee1719ac8f1f9f7378532e26b347dd495492e6782038f97a1c4c&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=190660866&response-content-disposition=attachment%3Bfilename%3Ddavml&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4558304 (4.3M) [application/octet-stream]
Saving to: 'avml'

avml                               100%[=====] 4.35M  --.-KB/s  in 0.1s

2023-09-03 20:34:43 (31.2 MB/s) - 'avml' saved [4558304/4558304]

user@ubuntu:~$ ls
avml Desktop Documents Downloads Music Pictures Public snap Templates Videos

```

Ilustración 78: descarga de AVML

Para que nos permita ejecutar el programa debemos darle permisos de ejecución al archivo con el comando:

```
chmod +x avml
```



```

user@ubuntu:~$ ls -l
total 4452
-rw-rw-r-- 1 user user 4558304 Oct  3  2022 avml
drwxr-xr-x 2 user user   40 Jul 22 14:10 Desktop
drwxr-xr-x 2 user user   60 Jul 22 15:08 Documents
drwxr-xr-x 2 user user   40 Jul 22 14:10 Downloads
drwxr-xr-x 2 user user   40 Jul 22 14:10 Music
drwxr-xr-x 2 user user   40 Jul 22 14:10 Pictures
drwxr-xr-x 2 user user   40 Jul 22 14:10 Public
drwx----- 4 user user   80 Jul 22 14:11 snap
drwxr-xr-x 2 user user   40 Jul 22 14:10 Templates
drwxr-xr-x 2 user user   40 Jul 22 14:10 Videos
user@ubuntu:~$ chmod +x avml
user@ubuntu:~$ ls -l
total 4452
-rwxrwxr-x 1 user user 4558304 Oct  3  2022 avml
drwxr-xr-x 2 user user   40 Jul 22 14:10 Desktop
drwxr-xr-x 2 user user   60 Jul 22 15:08 Documents

```

Ilustración 79: Otorgando permisos de ejecución a AVML

Una vez el programa disponga de los permisos de ejecución podemos ejecutarlo con permisos de supersusuario con el comando:

```
sudo ./avml mem.mem
```

Tras ejecutar el programa se generará un archivo llamado mem.dump, y podemos comprobar su existencia listando los elementos de la carpeta como muestra la ilustración 80:

```

user@ubuntu:~$ sudo ./avml mem.mem
user@ubuntu:~$ ls
avml Desktop Documents Downloads mem.mem Music
Pictures Public snap Templates Videos

```

Ilustración 80: Creación de imagen de memoria

Tras haber obtenido el volcado de memoria en ambos sistemas nos vamos a centrar en obtener información del volcado de memoria en Windows, ya que la información que vamos a obtener es bastante similar y con mostrar el uso de la herramienta en un sistema es suficiente para proporcionar una visión general del uso de la herramienta y de lo que podemos hacer con ella.



Para ejecutar el programa hemos de situarnos en la ubicación del archivo con la consola del sistema, y una vez hecho esto ejecutaremos el programa mediante la siguiente sintaxis:

```
py vol.py -f memdump.mem comando
```

donde el volcado se llama memdump y su extensión es .mem, y el comando será el elegido para mostrar la información seleccionada.

Existen una gran cantidad de comandos para usar con este entorno de trabajo, y es por eso por lo que destacaremos unos cuantos por su utilidad.

En primer lugar, emplearemos el comando `pslist`, que mostrará la lista de los procesos en ejecución en el momento de la captura de memoria como muestra la Ilustración 81.

```
C:\Users\ \Desktop\volatility>py vol.py -f memdump.mem windows.pslist
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xb204abade1e0 331	-	N/A	False	2023-08-23 08:27:51.000000	N/A	Disabled	
220	4	Registry	0xb204ad4e6000 4	-	N/A	False	2023-08-23 08:27:46.000000	N/A	Disabled	
748	4	smss.exe	0xb204b7bc00c0 2	-	N/A	False	2023-08-23 08:27:51.000000	N/A	Disabled	
756	860	csrss.exe	0xb204bce7a340 13	-	0	False	2023-08-23 08:27:55.000000	N/A	Disabled	
1508	860	wininit.exe	0xb204bdd1a000 1	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1516	1500	csrss.exe	0xb204bdd13340 14	-	1	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1604	1508	services.exe	0xb204bdd94000 7	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1612	1508	lsass.exe	0xb204bdd4d0c0 16	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1744	1604	svchost.exe	0xb204bde3e000 16	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1780	1508	fontdrvhost.ex	0xb204bde72000 5	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1836	1500	winlogon.exe	0xb204bde7b100 6	-	1	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1880	1836	fontdrvhost.ex	0xb204bdec0000 5	-	1	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1940	1604	svchost.exe	0xb204bdeca000 11	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1980	1604	svchost.exe	0xb204bdf73000 5	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
820	1836	LogonUI.exe	0xb204bdf9b000 0	-	1	False	2023-08-23 08:27:57.000000	2023-08-23 08:28:09.000000	Disabled	Disabled
1040	1836	dwm.exe	0xb204bdfef00c0 39	-	1	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1156	1604	svchost.exe	0xb204bf641000 3	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1224	1604	svchost.exe	0xb204bf66a000 6	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1256	1604	svchost.exe	0xb204bf675000 4	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	
1264	1604	svchost.exe	0xb204bf679000 2	-	0	False	2023-08-23 08:27:57.000000	N/A	Disabled	

Ilustración 81: Comando `pslist` (Volatility)

Como podemos observar en la Ilustración 81 este comando muestra una lista de los procesos con información relevante como el identificador de proceso (PID), el identificador del proceso padre o proceso creador del proceso (PPID), el nombre del proceso, fecha de creación, fecha de salida del proceso y el *offset* o dirección de inicio de la memoria en la que se encuentra ubicado el proceso.

Esta información puede ser un poco difícil de visualizar de un simple vistazo, ya que podemos darnos cuenta de que unos procesos cuelgan de otros, por lo que al estar todo a la misma altura es difícil de diferenciar a simple vista. Es por eso por lo que existe el comando `pstree` que cumple con el cometido del comando anterior y además de eso lo muestra con estructura de árbol separando por subniveles como muestra la Ilustración 82.





```
C:\Users\ \Desktop\volatility>py vol.py -f memdump.mem windows.pstree
Volatility 3 Framework 2.4.1
Progress: 100.00
PDB scanning finished
PID PPID ImageFileName OffSet(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xb204abade1c0 331 - N/A False 2023-08-23 08:27:51.000000 N/A
* 220 4 Registry 0xb204ad4e6080 4 - N/A False 2023-08-23 08:27:46.000000 N/A
* 748 4 smss.exe 0xb204b7bc0c0 2 - N/A False 2023-08-23 08:27:51.000000 N/A
756 860 csrss.exe 0xb204bce7a340 13 - 0 False 2023-08-23 08:27:55.000000 N/A
1508 860 wininit.exe 0xb204bdd1a080 1 - 0 False 2023-08-23 08:27:57.000000 N/A
* 1604 1508 services.exe 0xb204bdd94080 7 - 0 False 2023-08-23 08:27:57.000000 N/A
** 8784 1604 aswidsagent.exe 0xb204c1e670c0 27 - 0 False 2023-08-23 08:28:01.000000 N/A
** 11784 1604 SearchIndexer.exe 0xb204c2e53080 71 - 0 False 2023-08-23 08:28:03.000000 N/A
*** 5064 11784 SearchProtocolHost.exe 0xb204ca8e70c0 0 - 1 False 2023-08-23 10:48:27.000000 2023-08-23 10:50:04.000000
*** 16976 11784 SearchProtocolHost.exe 0xb204c63b7340 6 - 0 False 2023-08-23 11:28:21.000000 N/A
*** 764 11784 SearchFilterHost.exe 0xb204c3370080 4 - 0 False 2023-08-23 11:20:21.000000 N/A
** 9232 1604 KinectManagementService.exe 0xb204c18a6080 3 - 0 False 2023-08-23 08:28:03.000000 N/A
** 9240 1604 lghub_updater.exe 0xb204c1862080 36 - 0 False 2023-08-23 08:28:03.000000 N/A
** 9248 1604 svchost.exe 0xb204c2005080 1 - 0 False 2023-08-23 08:28:03.000000 N/A
** 12832 1604 svchost.exe 0xb204c34d80c0 6 - 0 False 2023-08-23 08:28:04.000000 N/A
** 2604 1604 svchost.exe 0xb204bfb1080 3 - 0 False 2023-08-23 08:27:58.000000 N/A
```

Ilustración 82: Comando pstree (Volatility)

La Ilustración 81 y 82 muestran la misma información de los procesos, pero en este caso la 82 muestra la misma información con otro formato, añadiendo un asterisco (\*) por cada nivel de proceso.

Si nos paramos a analizar los procesos almacenados en la memoria RAM podemos observar en la ilustración 82 que el proceso wininit.exe inicia la ejecución del proceso services.exe, que se trata del controlador de servicios de Windows, que a su vez lanza otros procesos en el arranque de la máquina como aswidsagent.exe que se trata de los servicios del antivirus Avast que a su vez lanza otros procesos.

Del proceso services.exe con PID 1604 también cuelgan otros procesos como SearchFilterHost.exe que es el motor de indexación de archivos del sistema que nos permite realizar las búsquedas desde la barra de búsqueda de Windows.

También cuelgan otros procesos como KinectManagementService.exe que se trata del servicio instalado con los controladores de Kinect para Windows que se encargan de controlar este periférico, lghub\_updater.exe es el servicio de actualización del programa Logitech G HUB para periféricos de la marca Logitech, y RtkAudService.exe que se trata de los controladores de audio de la firma Realtek.

Destacamos también el programa del sistema svchost.exe, que se trata de un servicio de Windows que se encarga de cargar archivos DLL (Dinamic Link Library) que son bibliotecas contenedoras de recursos que emplean los programas siendo compartidos por estos reduciendo el tamaño de los ejecutables.

Otro ejemplo de procesos se muestra en la Ilustración 83.

```
1836 1500 winlogon.exe 0xb204bde7b180 6 - 1 False 2023-08-23 08:27:57.000000 N/A
* 1880 1836 fontdrvhost.exe 0xb204bdec0800 5 - 1 False 2023-08-23 08:27:57.000000 N/A
* 1040 1836 dmw.exe 0xb204bdf0e0c0 39 - 1 False 2023-08-23 08:27:57.000000 N/A
* 4316 1836 userinit.exe 0xb204c0450080 0 - 1 False 2023-08-23 08:27:59.000000 2023-08-23 08:28:22.000000
** 4364 4316 explorer.exe 0xb204c04da080 212 - 1 False 2023-08-23 08:27:59.000000 N/A
*** 13824 4364 lghub.exe 0xb204c2e32280 27 - 1 False 2023-08-23 08:28:12.000000 N/A
**** 13440 13824 lghub.exe 0xb204c1a7b080 37 - 1 False 2023-08-23 08:28:13.000000 N/A
**** 8176 13824 lghub.exe 0xb204c1a83080 9 - 1 False 2023-08-23 08:28:13.000000 N/A
**** 9052 13824 lghub_system_t 0xb204c1a790c0 71 - 1 False 2023-08-23 08:28:13.000000 N/A
***** 14744 9052 lghub_agent.exe 0xb204c3ae5080 102 - 1 False 2023-08-23 08:28:13.000000 N/A
*** 9348 4364 WIMWORD.EXE 0xb204c14450c0 133 - 1 False 2023-08-23 10:34:44.000000 N/A
**** 15664 9348 ai.exe 0xb204c6e11080 19 - 1 False 2023-08-23 10:34:45.000000 N/A
*** 13132 4364 RtkAudService.exe 0xb204c1da6080 7 - 1 False 2023-08-23 08:28:11.000000 N/A
*** 5812 4364 SecurityHealth.exe 0xb204c1d1a080 1 - 1 False 2023-08-23 08:28:11.000000 N/A
*** 7988 4364 FTK Imager.exe 0xb204c0ecf0c0 19 - 1 False 2023-08-23 11:18:27.000000 N/A
*** 14716 4364 OUTLOOK.EXE 0xb204c51d9080 159 - 1 False 2023-08-23 09:01:25.000000 N/A
**** 14648 14716 ai.exe 0xb204c5fe2080 19 - 1 False 2023-08-23 09:01:27.000000 N/A
**** 2496 14716 msdgedwebview2.exe 0xb204c536a2c0 41 - 1 False 2023-08-23 09:01:32.000000 N/A
```

Ilustración 83: Procesos lanzados por winlogon.exe

En esta ilustración podemos ver que el proceso winlogon.exe ha lanzado otros procesos, a destacar el proceso de userinit.exe. El primer proceso se encarga de cargar el perfil de usuario, y el segundo se ejecuta al iniciar sesión cargando la interfaz, el explorador de archivos (explorer.exe) y otros procesos importantes. Desde el explorador de archivos se han lanzado otros procesos como el software Logitech G HUB (lghub.exe), Microsoft Word (WINWORD.EXE), el programa de los drivers de audio Realtek (RtkAudUService.exe), el cliente de escritorio Outlook (OUTLOOK.EXE), un servicio del navegador Edge que se usa para ejecutar contenido web en apps nativas (msedgewebview2.exe) e incluso el programa AccessData FTK Imager que hemos instalado en el equipo para crear la imagen de la memoria RAM entre otras funciones (FTKImager.exe).

```

** 10048      1604      svchost.exe      0xb204c23a02c0  4      -      0      False      2023-08-23 08:28:03.000000      N/A
** 2884 1604      NVDisplay.Cont  0xb204bfac30c0  9      -      0      False      2023-08-23 08:27:58.000000      N/A
*** 3096      2884      NVDisplay.Cont  0xb204bfc020c0  43     -      1      False      2023-08-23 08:27:58.000000      N/A
*** 2068      2884      dbInstaller.ex  0xb204bfb22800  0      -      0      False      2023-08-23 08:27:58.000000      2023-08-23 08:27:58.000000
** 4936 1604      svchost.exe      0xb204c06b4080  7      -      0      False      2023-08-23 08:27:59.000000      N/A
** 848 1604      svchost.exe      0xb204bf729080  1      -      0      False      2023-08-23 08:27:57.000000      N/A
** 5460 1604      AvastSvc.exe     0xb204c0a3a080  245    -      0      False      2023-08-23 08:27:59.000000      N/A
*** 6772      5460      aswEngSrv.exe   0xb204c123c2c0  65     -      0      False      2023-08-23 08:28:00.000000      N/A
** 2392 1604      svchost.exe      0xb204bd620080  5      -      0      False      2023-08-23 08:27:57.000000      N/A
** 12644     1604      svchost.exe     0xb204c34bf080  1      -      0      False      2023-08-23 08:28:04.000000      N/A
** 8552 1604      gameinputsvc.e  0xb204c17e4080  3      -      0      False      2023-08-23 08:28:03.000000      N/A

```

Ilustración 84: Procesos lanzados por svchost.exe

En la Ilustración 84 podemos observar que existen varios subprocesos svchost.exe que se encargan de cargar los DLL como hemos comentado anteriormente, pero estos cuelgan del mismo proceso services.exe ya que su PPID corresponde al 1604 que es el PID de services.exe, por lo que este proceso es el padre de todos los subprocesos svchost.exe lanzados.

Algunos lanzan controladores gráficos de Nvidia, en concreto el Nvidia Control Panel que es una herramienta que nos permite controlar las opciones gráficas de la tarjeta gráfica de nuestro ordenador, otros lanzan servicios del antivirus Avast necesarios para su funcionamiento, y otros lanzan gameinputsvc.exe que se trata del servicio GameInput de Windows y se encarga de manejar la entrada de dispositivos de juego como mandos o joysticks haciendo que su entrada sea compatible con el sistema y los juegos que se ejecuten en el sistema.



Pasamos a emplear el comando `info`, que mostrará información del sistema como se muestra en la ilustración:

```
C:\Users\ \Desktop\volatility>py vol.py -f memdump.mem windows.info
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf80473a00000
DTB 0x1ad000
Symbols file:///C:/Users/ /Desktop/volatility/volatility3/symbols/windows/ntkrnlmp.pdb/06564D3477822C7D97F04852CBD5AFD6-1.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8047460f400
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 4
SystemTime 2023-08-23 11:21:35
NTSystemRoot C:\WINDOWS
NTProductType NtProductWinNt
NTMajorVersion 10
NTMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Mon Nov 22 18:02:49 2004
```

Ilustración 85: Información del sistema

En la Ilustración 85 podemos observar información acerca del sistema como la hora del sistema, el número de procesadores, si se trata de un sistema con una arquitectura de 64 o 32 bits, o la raíz del sistema Windows.

Para finalizar emplearemos el comando `hashdump` para obtener los hashes de las contraseñas de los usuarios de la máquina como muestra la Ilustración 86:

```
C:\Users\ \Desktop\volatility>py vol.py -f memdump.mem windows.hashdump
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
User rid lmhash nthash
Administrador
Invitado
DefaultAccount
WDAGUtilityAccount EJEMPLO_HASH
21232f297a57a5a743894a0e4a801fc
```

Ilustración 86: Hashes de contraseñas

Como se tratan de hashes de contraseñas personales estas se han ocultado y se ha empleado un hash de ejemplo para ilustrar qué podemos hacer con estos hashes. Al tratarse de un hash este no se puede “desencriptar” por así decirlo, pero sí que podemos comparar este hash con una tabla de hashes pregenerados con las contraseñas más comunes. Esto consiste en buscar este valor hash en una base de datos de hashes pregenerados a partir de contraseñas ya existentes y buscar coincidencias exactas como si tratásemos de realizar un ataque por fuerza bruta

basado en diccionario para averiguar la contraseña que corresponde al valor hash que hemos recuperado mediante Volatility.

Si introducimos el valor obtenido en una web de búsqueda de hashes como hashes.com esta web buscará el hash introducido y buscará coincidencias en su base de datos.



Ilustración 87: Búsqueda de hashes en hash.com

Al tratarse de un hash de una contraseña débil y común este valor hash es fácilmente encontrado en la base de datos de la web, cuyo valor corresponde a la contraseña “admin” que podría ser la típica contraseña de un usuario de administrador por defecto.

De esta manera podemos recuperar contraseñas a partir de su valor hash mediante búsqueda de comparaciones en un diccionario de claves hash de contraseñas pregeneradas que nos permitirá acceder a las cuentas de los usuarios del sistema que está siendo analizado.

### 5.1.9 Recuperación y análisis de datos de dispositivos de almacenamiento con Autopsy

Para esta tarea nos serviremos de la herramienta Autopsy que será la encargada de recuperar todos los archivos del disco duro que sea objeto de análisis.

En este caso concreto analizaremos el sistema de archivos de un disco duro de una máquina Windows, ya que al tratarse del disco duro de mi ordenador personal que llevo usando durante más de un año cuya capacidad es de 1TB podremos encontrar información de sobra que podremos analizar y de la que podremos extraer información. Podríamos analizar también un disco duro que contenga datos de un sistema operativo Linux, pero el objetivo que se alcanzaría es el mismo, salvo por la particularidad de que la máquina Linux que he estado empleando para poblarla de datos nos daría resultados un poco pobres si la comparamos con los posibles resultados que nos dé el análisis del disco duro de la máquina Windows, ya que este disco duro tiene una mayor capacidad y ha almacenado más datos a lo largo un periodo de tiempo mayor.

Cabe destacar que podemos analizar un disco duro perteneciente a otro sistema diferente al que alberga la herramienta Autopsy siempre y cuando dispongamos de la imagen de disco virtual. Esto implica que podemos analizar un disco duro de un sistema Windows mediante la herramienta Autopsy siendo ejecutada en un sistema Linux y viceversa.

Para emplear todas las herramientas de la misma forma analizaremos el disco duro del sistema Windows que ha sido montado en la máquina virtual Windows del entorno de laboratorio desde la propia máquina virtual donde tenemos la herramienta Autopsy instalada.

Comenzaremos abriendo el programa y veremos la siguiente ventana de bienvenida:

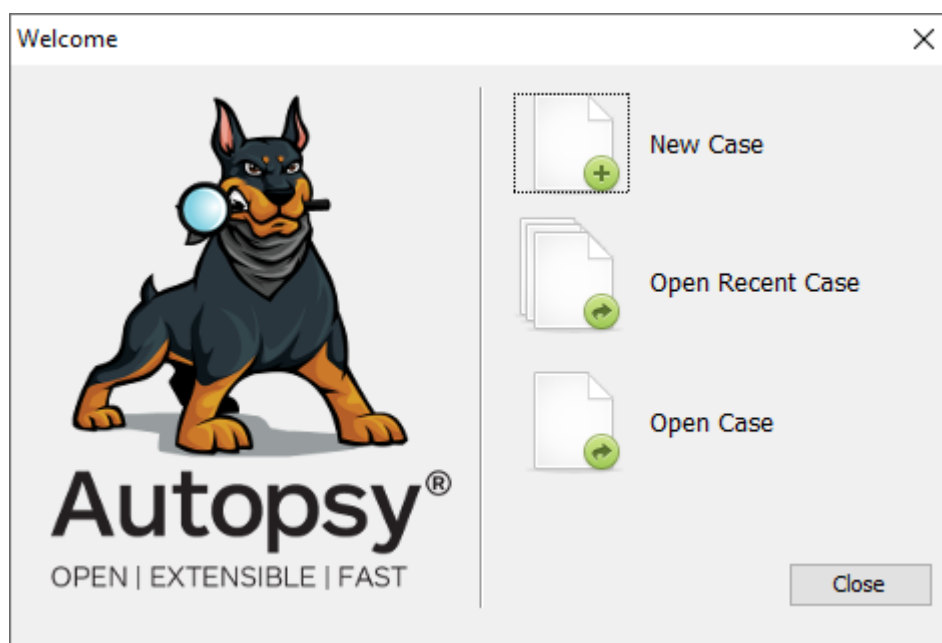


Ilustración 88: Welcome Autopsy

Seleccionaremos la opción de crear un nuevo caso, que nos abrirá otra ventana en la que deberemos de rellenar la información del caso como muestra la Ilustración 89.

New Case Information

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name: Disco Duro

Base Directory: C:\Documents\Autopsy

Case Type:  Single-User  Multi-User

Case data will be stored in the following directory:

C:\Documents\Autopsy\Disco Duro

< Back Next > Finish Cancel Help

Ilustración 89: Información del caso

En esta ocasión llamaremos al caso “Disco duro” y seleccionaremos la ruta base del directorio donde se almacenarán todos los archivos del caso. Es un caso de un usuario único del sistema.

En la siguiente pestaña encontraremos un formulario con información adicional que debería de rellenarse con la información del perito informático que está llevando a cabo la investigación. Para nuestro caso podemos rellenarlo con nuestros datos, o bien dejarlo en blanco porque no van a ser necesarios como muestra la Ilustración 90.

**New Case Information**

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: Recovery

Examiner

Name: [ ]

Phone: [ ]

Email: [ ]

Notes: [ ]

Organization

Organization analysis is being done for: Not Specified [v] Manage Organizations

< Back Next > Finish Cancel Help

Ilustración 90: Información adicional

A continuación, se nos abrirá otra ventana donde seleccionaremos cómo vamos a organizar los datos una vez el programa los extraiga, seleccionando la primera opción correspondiente a “Generar un nuevo nombre de host basado en el nombre de la fuente de datos” como se muestra en la Ilustración 91.

**Recuperacion - Autopsy 4.20.0**

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Add Data Source**

**Steps**

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

**Select Host**

Hosts are used to organize data sources and other data.

Generate new host name based on data source name

Specify new host name [ ]

Use existing host [ ]

< Back Next > Finish Cancel Help

Ilustración 91: Organización de datos

Una vez hecho esto seleccionaremos el tipo de fuente de datos que vamos a analizar, y escogeremos la opción de disco local:

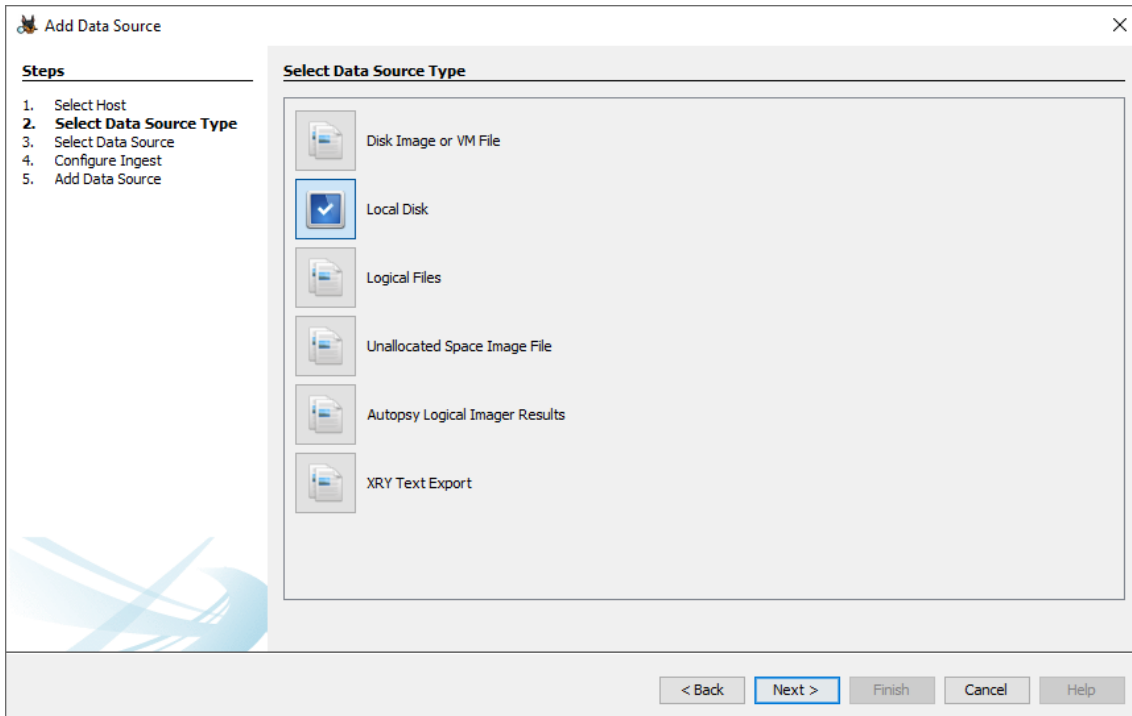


Ilustración 92: Selección de fuente de datos

Una vez dentro de las opciones seleccionaremos el disco duro que analizaremos, que se trata del "Drive 0" como se puede ver en la Ilustración 93. El resto de las opciones se dejan con sus valores predeterminados, ya que la zona horaria es un dato que viene dado por el propio sistema operativo.

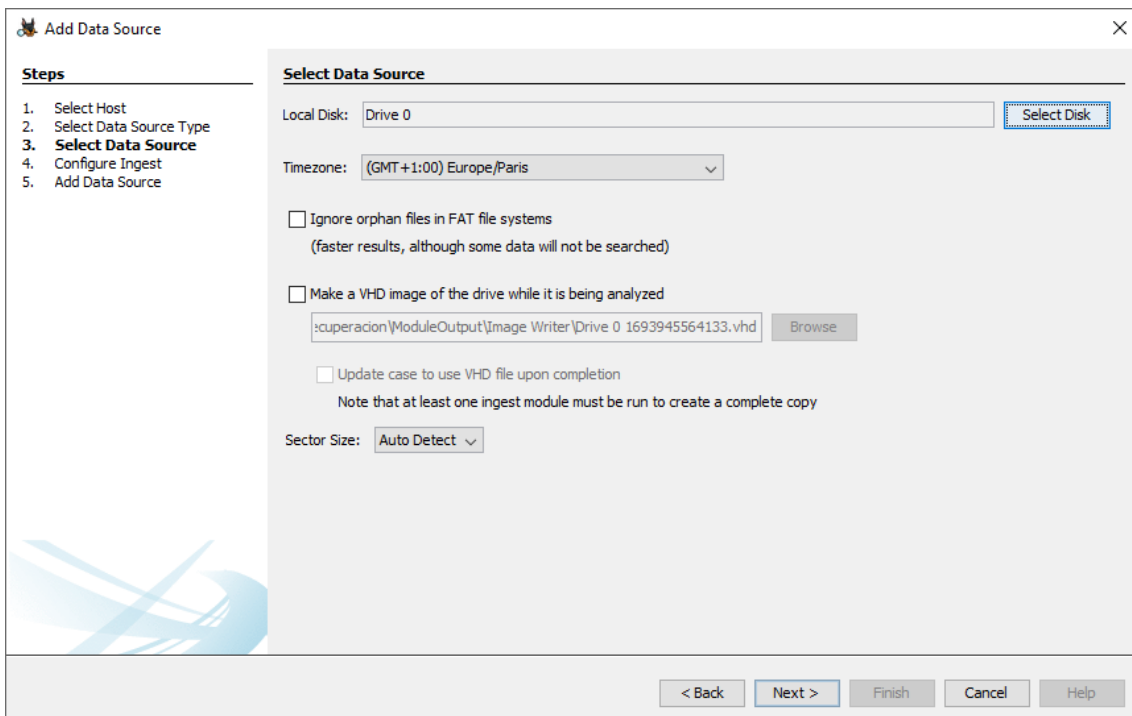


Ilustración 93: Selección de fuente de datos



Es importante destacar que este software tiene la capacidad de generar una imagen de disco en formato VHD mientras se está analizando, lo cual es interesante pero no emplearemos para nuestro caso.

Después seleccionaremos los módulos de Autopsy como muestra la ilustración:

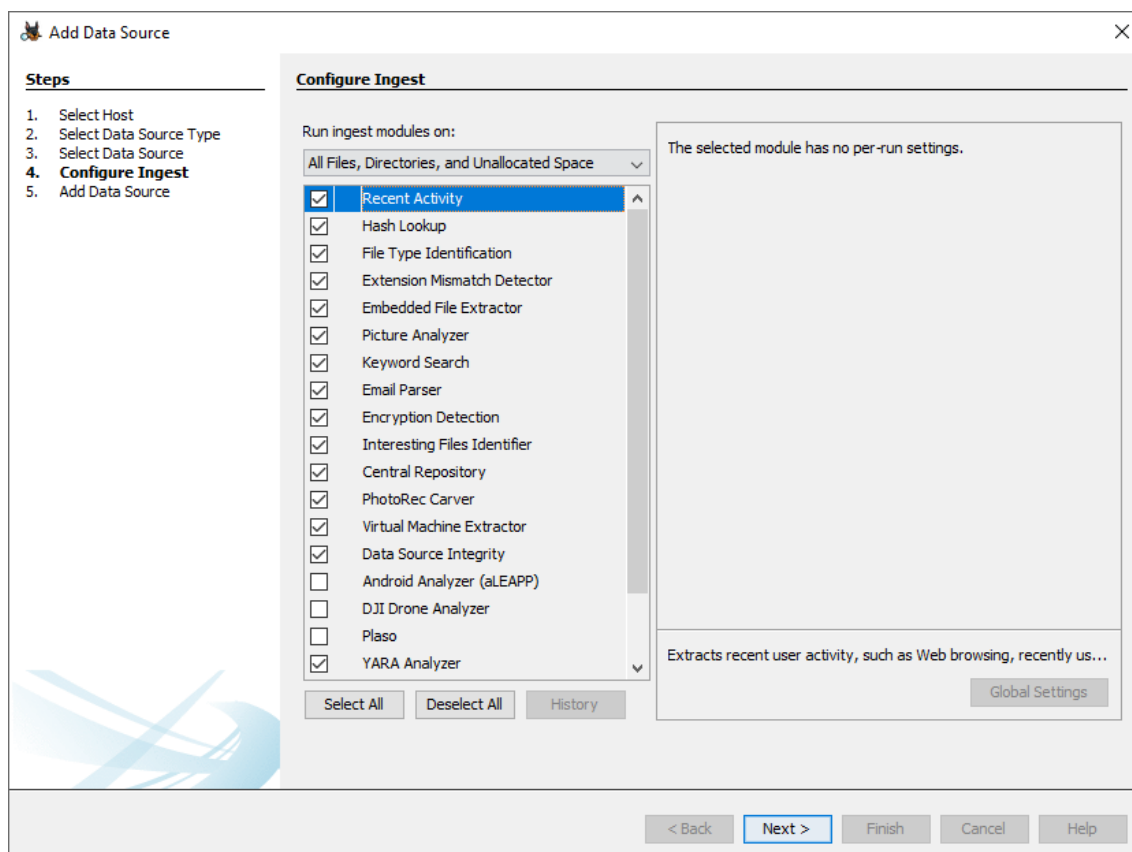


Ilustración 94: Módulos seleccionados para el análisis

Se hace hincapié en que Autopsy permite instalar módulos de terceros de fuentes abiertas para su uso en el programa, pero para nuestro caso los módulos que vienen instalados por defecto con Autopsy son más que suficientes para analizar el disco duro. Estos módulos seleccionados tienen aportan funcionalidades como ver la actividad reciente del usuario con los archivos, identificar los tipos de archivo, un analizador de imágenes, buscador de palabras clave, identificador de archivos interesantes, entre otros.

Hay que añadir que el módulo de extracción de máquinas virtuales no sería indispensable de importar para el análisis, ya que se plantea el siguiente escenario: Al haberse montado el entorno de trabajo en la máquina física con sistema operativo Windows se está creando una copia exacta de la máquina física mediante la creación de una máquina virtual en la cual cargamos una imagen de disco que constituye una copia exacta de la unidad de disco que contiene los datos del sistema operativo. Lo que hay que tener en cuenta es que la imagen de disco se ha creado antes que la construcción del entorno de laboratorio con el fin de emplear esta imagen de disco y cargarla en la máquina virtual, por lo cual no va a haber ningún lugar en el sistema de archivos en el que Autopsy pueda rebuscar para recuperar información de máquinas

virtuales ya que estas no tienen cabida en el sistema que estamos analizando debido al momento en el que se ha generado la imagen de disco virtual.

Tras esta aclaración se podrá iniciar el proceso de obtención de los datos haciendo click en el botón de “Siguiente”.

Una vez se inicia el proceso de escaneo del disco duro el programa comienza a recuperar los archivos mostrando el estado del proceso como muestra la Ilustración 95.

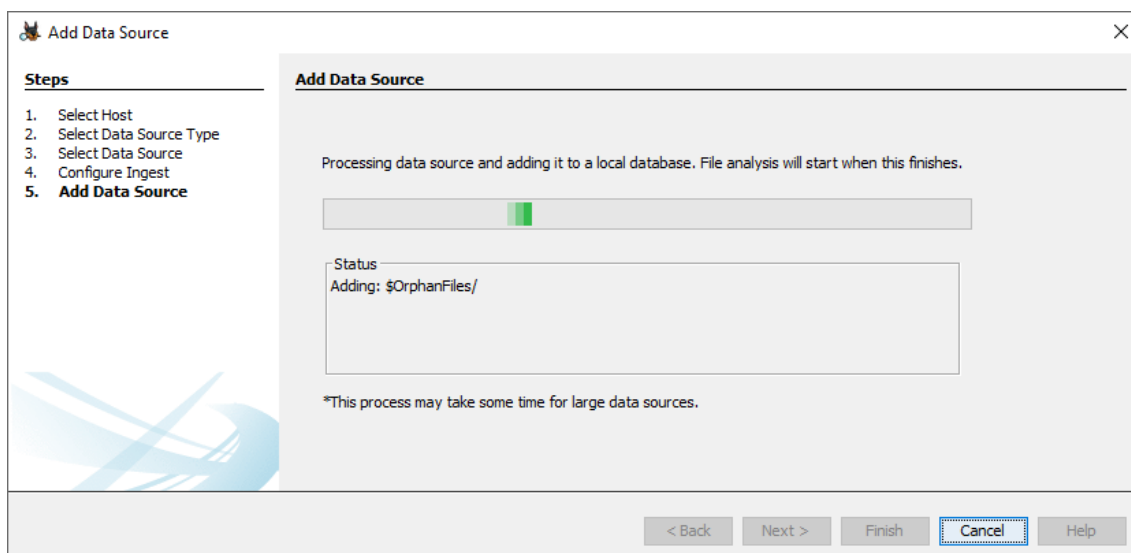


Ilustración 95: Proceso de extracción de datos

La duración del proceso depende de la capacidad del disco duro, la cantidad de datos almacenados y la potencia de cómputo de la máquina. Al ejecutarse en una máquina virtual con 4 CPU asignados y 4GB de memoria RAM este proceso ha durado más de una hora. Si se hubiese seleccionado como fuente de datos la propia imagen de disco en vez del disco local como se mostraba en la Ilustración 92 este proceso se podría haber realizado en una máquina física directamente instalando el programa en el sistema operativo host y no en las máquinas virtuales que este alberga, por lo que el proceso hubiese sido mucho más rápido si se hubiese realizado en una máquina con 32GB de RAM y un procesador con 12 núcleos, que se corresponde con el triple de procesadores de los que dispone la máquina virtual y ocho veces más memoria RAM asignada.

Para seguir empleando todas las herramientas de la misma forma se ha escogido la opción de ejecutar el programa en la máquina virtual y analizar el disco local (que es literalmente la imagen de disco que hemos montado en la máquina virtual) y lo importante es que el proceso de extracción ha sido finalizado con éxito y ha recuperado todos los archivos del disco duro, por lo que ya podemos comenzar a analizarlos y ver la información que contienen.

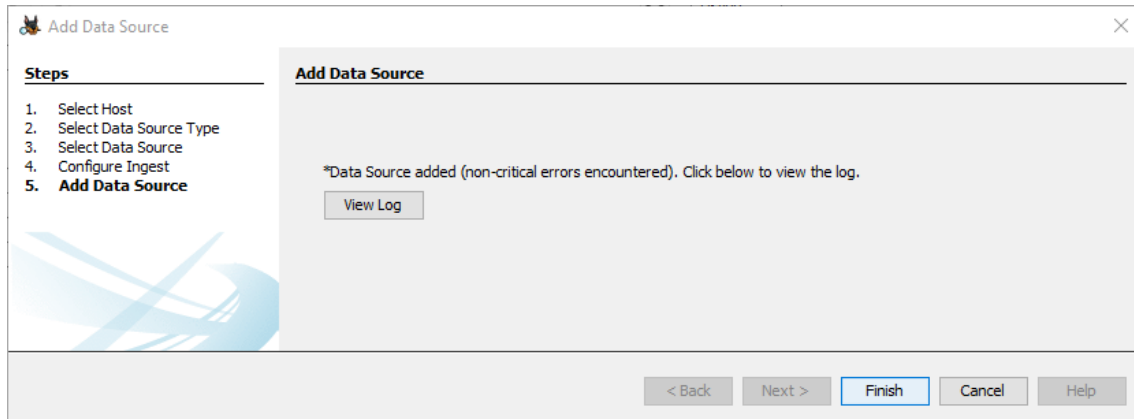


Ilustración 96: Proceso de extracción finalizado

En un primer vistazo veremos la pantalla principal del caso que se muestra en la Ilustración 97. En ella veremos una gran cantidad de datos agrupados por categorías las cuales definen de forma clara y concisa la información que nos encontraremos al abrir estos conjuntos. Si nos fijamos en los nombres de los agrupamientos podemos observar que la herramienta a través de sus módulos ha sido capaz de extraer datos de navegación, programas en ejecución, caché web de navegadores, que son datos que hemos recuperado en apartados anteriores con otras herramientas. Esto se debe a que Autopsy realmente es una interfaz de usuario que recopila una gran cantidad de herramientas de recuperación de datos de fuente abierta, por lo que podemos considerarla la herramienta “definitiva” en cuanto a recuperación de datos.

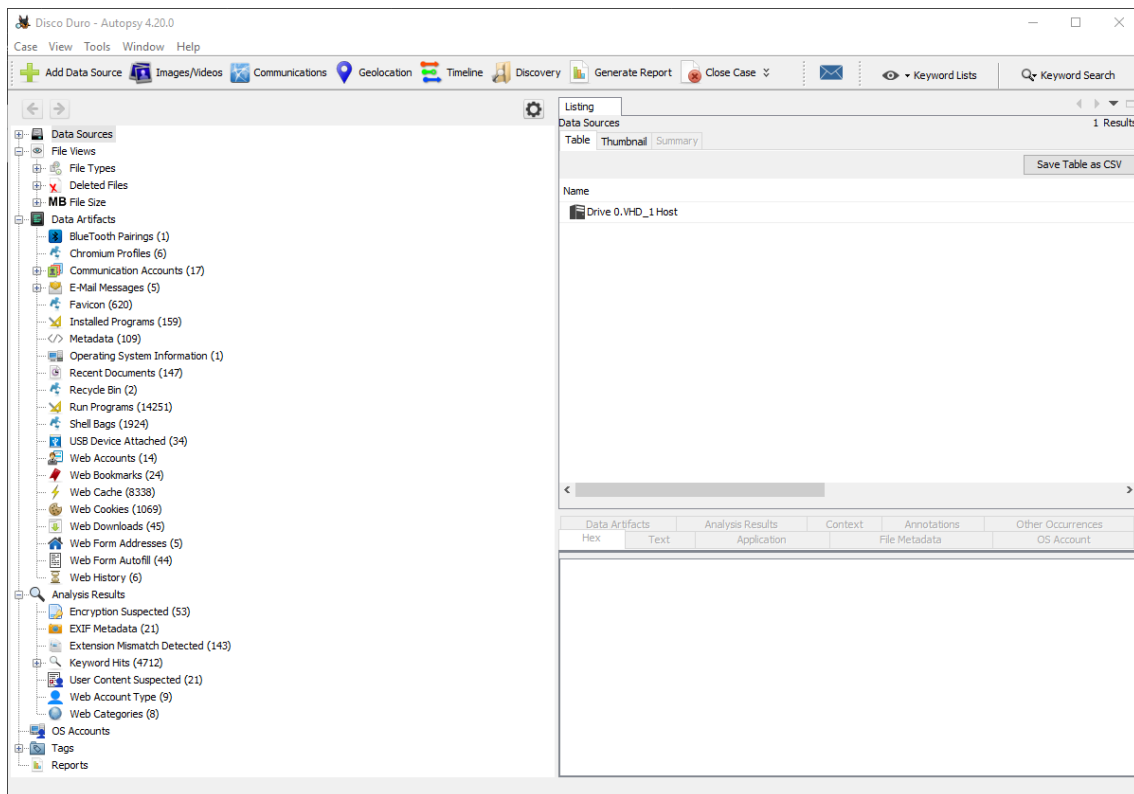


Ilustración 97: Ventana principal del caso

Si comenzamos a examinar los archivos recuperados podemos ver los archivos por tipo de archivo y por extensión. El menú desplegable muestra las principales extensiones de archivo como son imágenes, videos, audio o bases de datos como podemos ver en la Ilustración 98. Para el caso de las imágenes se han encontrado más de 10.000 elementos. A modo de ejemplo se puede observar una de ellas en la Ilustración 98.

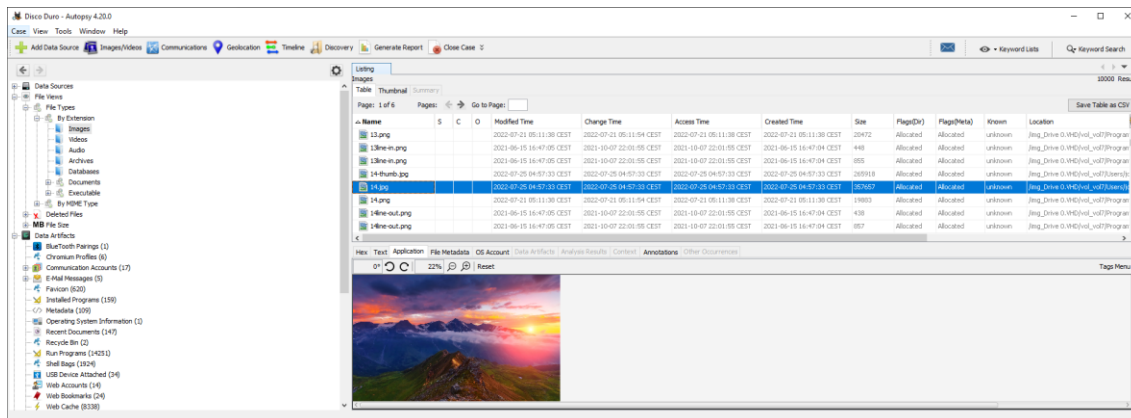


Ilustración 98: Imagen recuperada

Podemos ver una previsualización de la imagen y sus datos como sus datos de acceso, creación y modificación, tamaño del archivo y su ubicación. En este caso se trata de una imagen recuperada de la carpeta Roaming, por lo que esta debe de pertenecer a los datos de alguna aplicación, y posiblemente se trate de algún fondo de pantalla.

En el caso de los videos podemos encontrar archivos temporales de aplicaciones como la versión de escritorio de WhatsApp. En este caso se observa un video que, aunque no se haya descargado para ser almacenado WhatsApp lo ha descargado como un archivo temporal para que este video sea reproducido en el ordenador del usuario, por lo que inevitablemente debe de descargarlo como un archivo temporal. Su previsualización nos hace ver que se trata de un video de un coche de rally saltando por encima de una pendiente como vemos en la Ilustración 99.

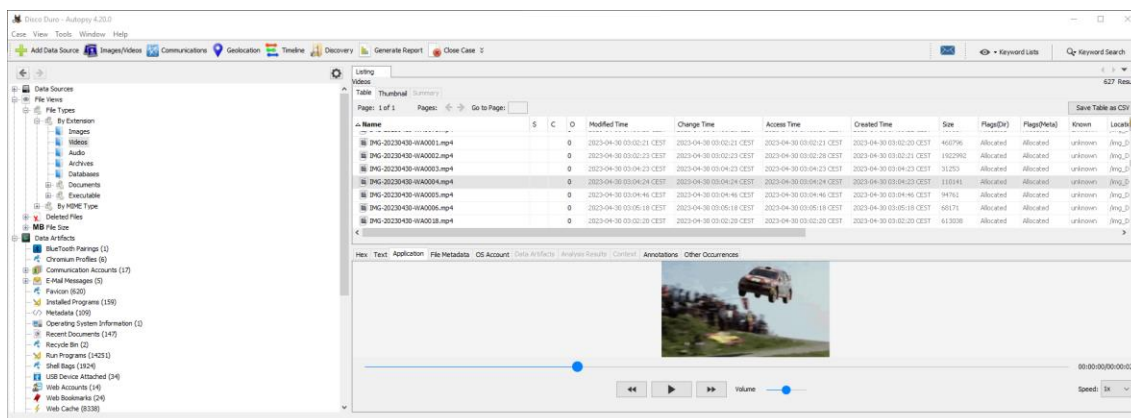


Ilustración 99: Video recuperado



# Análisis forense de la huella digital de un usuario en sistemas informáticos

En el caso de los audios es exactamente igual, mostrando un tono de alarma.

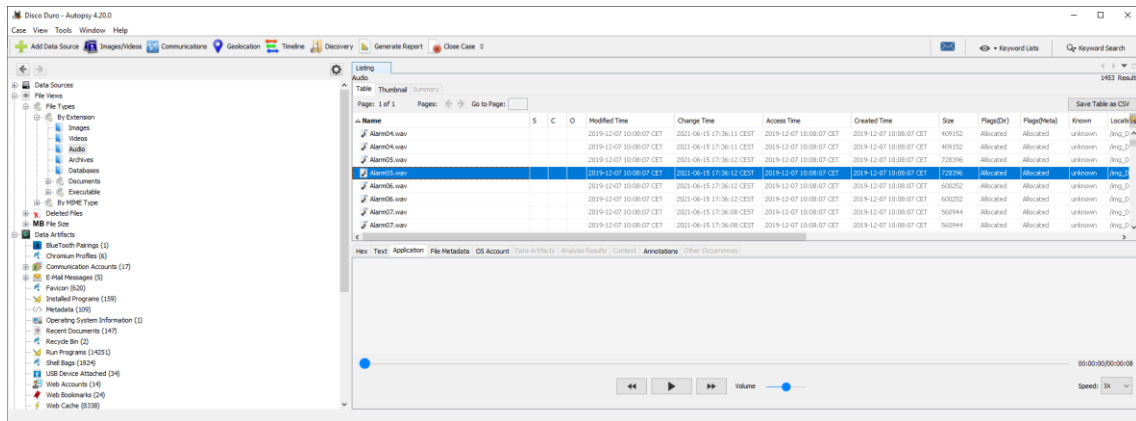


Ilustración 100: Audios recuperados

Si visualizamos los archivos se tratan de archivos temporales de archivos que han sido descomprimidos, siendo el caso de un paquete de lenguaje para el idioma Inglés de Estados Unidos.

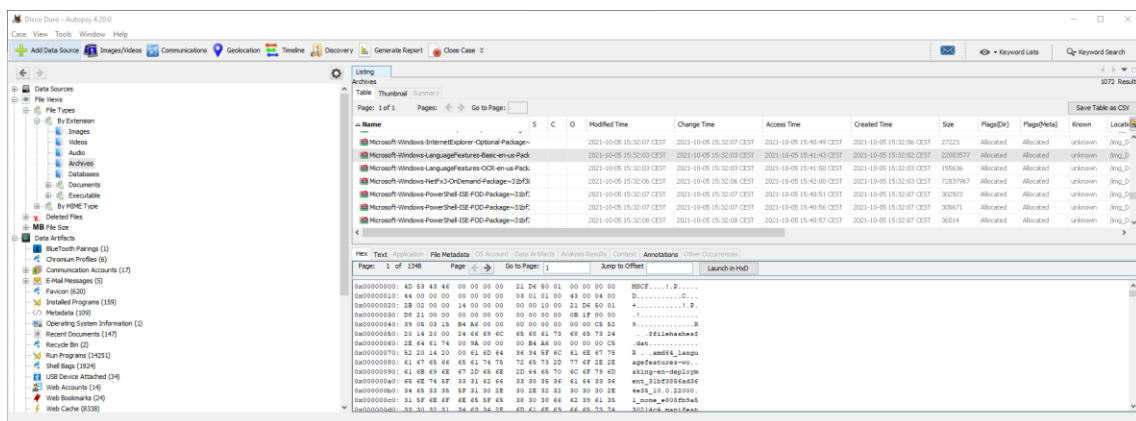


Ilustración 101: Archivos comprimidos recuperados

Una vez teniendo claro cómo se estructura esta información pasaremos a mostrar información relevante de entre todos los grupos de archivos.

En el apartado de documentos se han encontrado archivos con información sensible, como por ejemplo informes laborales, nóminas, presentaciones de PowerPoint con información confidencial acerca de unas instalaciones en las que el usuario ha desempeñado acciones laborales, trabajos académicos, recetas médicas, cuadros horarios, currículums, contratos y convenios firmados y certificados de titularidad bancaria. No será necesario mostrar cada uno de ellos por separado, pero se mostrarán algunos en concreto por el carácter de la información que estos contienen

Destacamos la nómina de la Ilustración 102 en la que se pueden ver datos de la empresa y el trabajador, como nombres completos, números de la Seguridad Social, y números de identificación fiscal.

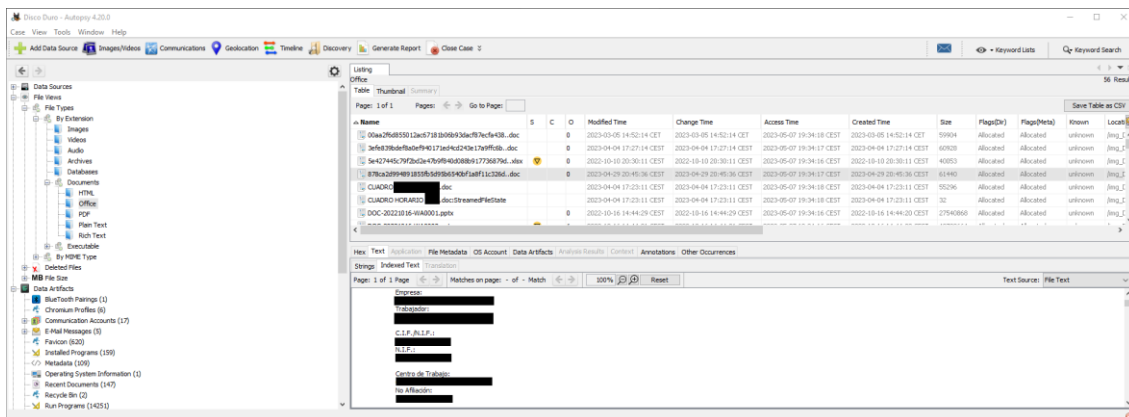


Ilustración 102: Nómina

Del certificado de titularidad bancaria mostrado en la Ilustración 103 destacamos nombre completo, número de identificación fiscal y número de cuenta bancaria.

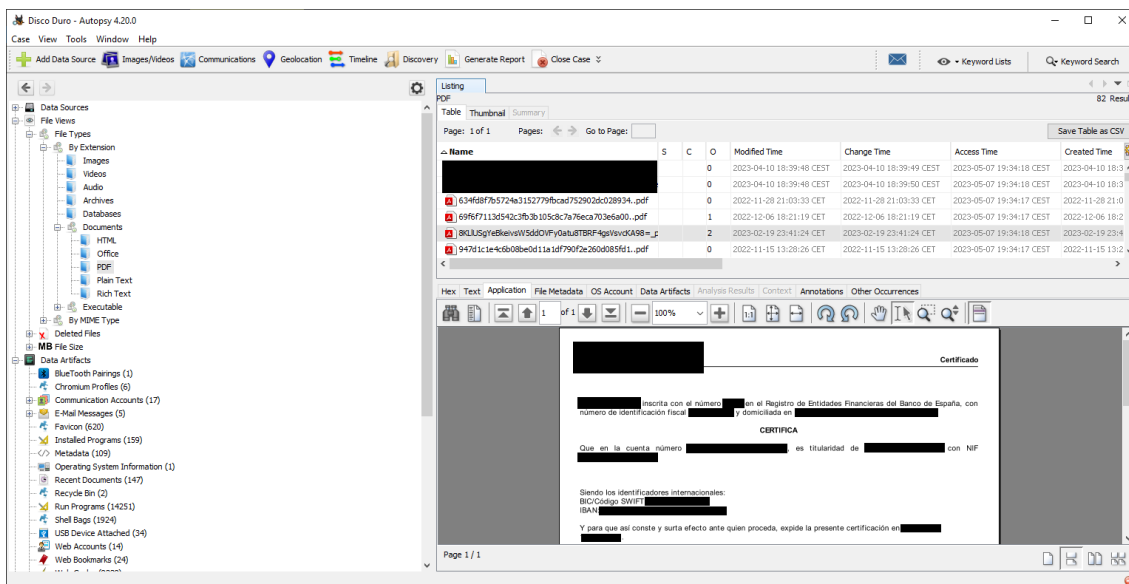


Ilustración 103: Certificado de titularidad bancaria

Además de estos datos presentes en el disco duro del sistema también podremos visualizar archivos borrados que Autopsy ha recuperado.

Por ejemplo, en la Ilustración 104 se ha recuperado una captura de pantalla del videojuego de conducción.



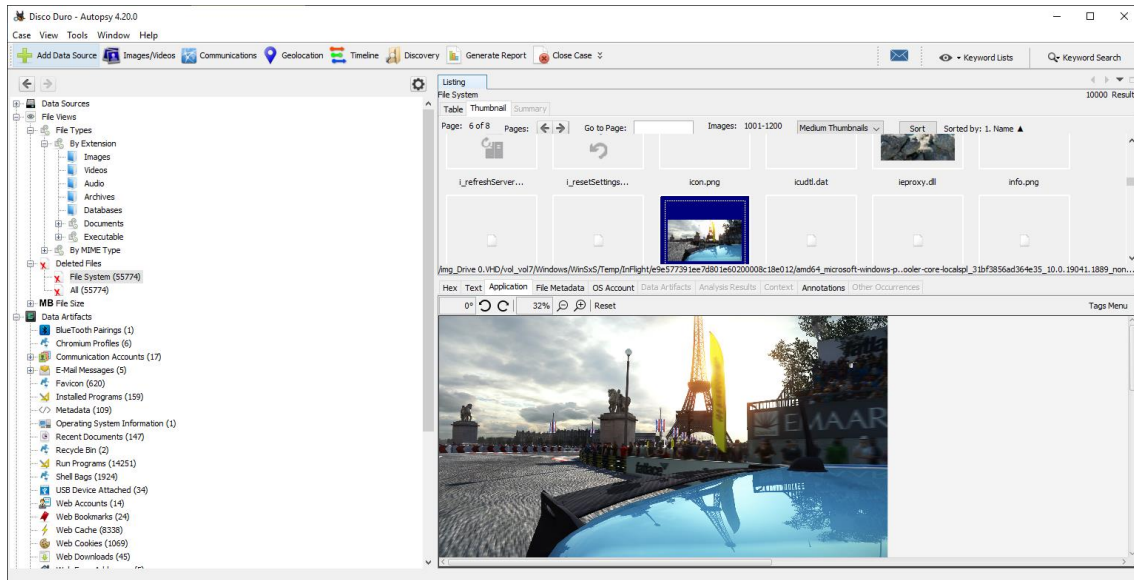


Ilustración 104: Imagen borrada recuperada

En el apartado de los artefactos de datos podremos encontrar muchas categorías que nos proporcionarán información acerca de los dispositivos BlueTooth vinculados con el sistema, perfiles de navegadores basados en Chromium, cuentas de correo electrónico, programas instalados, documentos recientes, contenido sin eliminar en la papelera de reciclaje, programas ejecutados en el sistema, dispositivos USB conectados al equipo, cuentas de usuario, marcadores del navegador, descargas del navegador, entre otros.

Destacamos los perfiles en los navegadores Edge y Chrome que proporcionan información acerca de los nombres de usuario que son direcciones de correo que muestra la Ilustración 105.

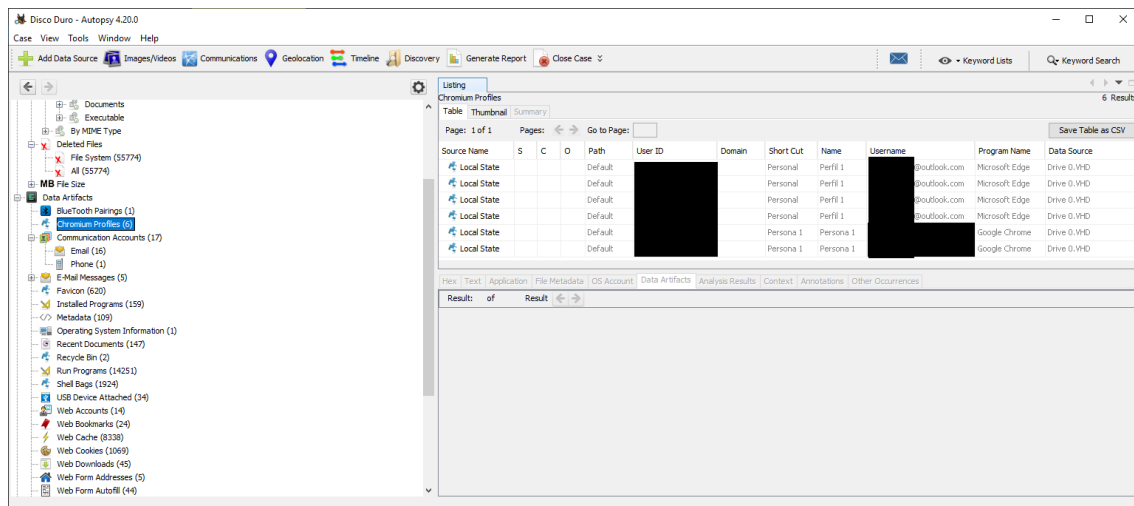


Ilustración 105: Perfiles del navegador



Se han recuperado correos electrónicos de diversas fuentes como archivos con extensión .eml que corresponde a mensajes de correo electrónico o del administrador de cuentas del sistema (SAM, *System Account Manager*) como se puede ver en la Ilustración 106.

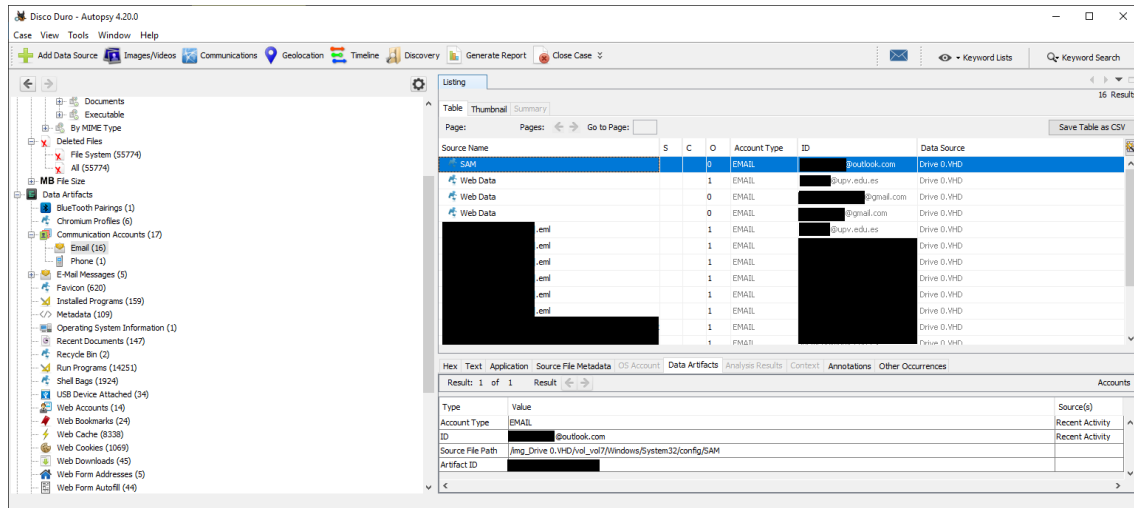


Ilustración 106: Direcciones de correo

Como ejemplo se muestran algunos programas instalados en la Ilustración 107. Se tratan de controladores gráficos de Nvidia, antivirus Avast, aplicaciones de Office, entre otros.

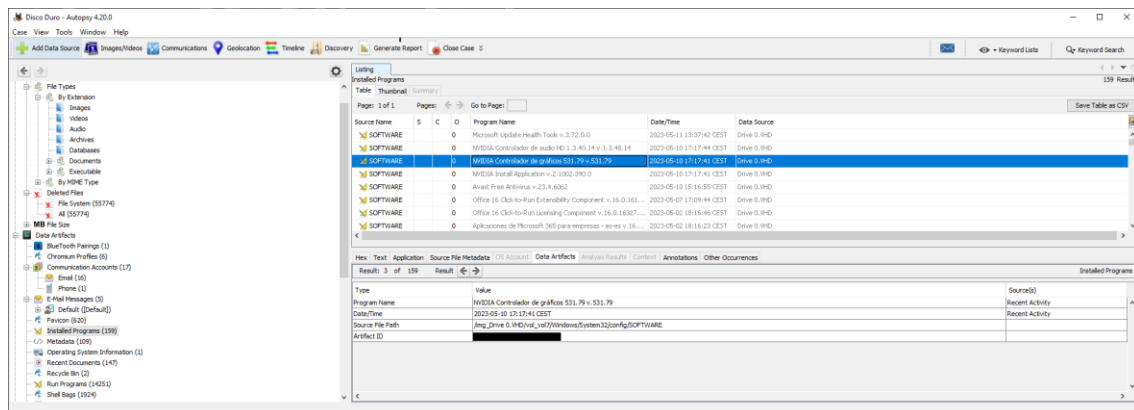


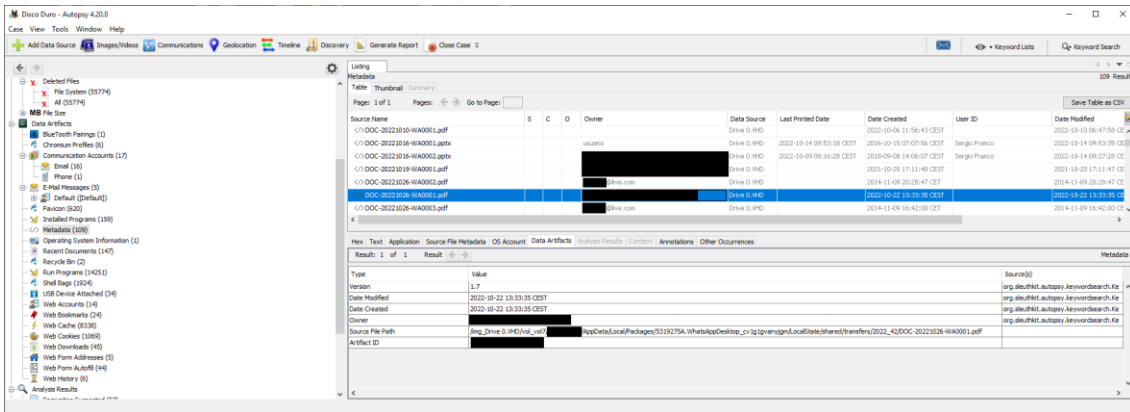
Ilustración 107: Programas instalados

El módulo de análisis de metadatos se encarga de buscar los metadatos en los archivos y ordenarlos por categoría como estos documentos clasificados por propietario de la Ilustración 108. En este caso concreto se ilustra un documento en formato PDF recuperado de la aplicación WhatsApp de escritorio.





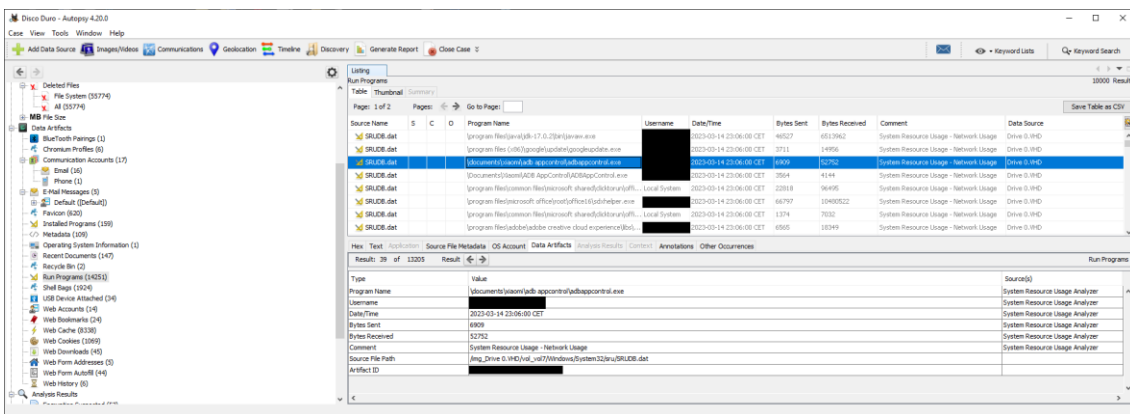
## Análisis forense de la huella digital de un usuario en sistemas informáticos



Source Name	S	C	D	Owner	Date Source	Last Printed Date	Date Created	User ID	Date Modified
DOC-20221016-WA001.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-16 06:47:59 CE
DOC-20221016-WA001.pdf					Drive 0:WHD		2022-10-14 09:53:18 CEST		2022-10-14 09:53:35 CE
DOC-20221016-WA002.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST	Sergio Franco	2022-10-14 09:53:35 CE
DOC-20221016-WA002.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-14 09:53:35 CE
DOC-20221016-WA002.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-14 09:53:35 CE
DOC-20221016-WA002.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-14 09:53:35 CE
DOC-20221016-WA003.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-14 09:53:35 CE
DOC-20221016-WA003.pdf					Drive 0:WHD		2022-10-16 11:56:43 CEST		2022-10-14 09:53:35 CE

Ilustración 108: Archivos clasificados por metadatos

Disponemos de acceso a un registro que recopila todos los programas que se han ejecutado en el sistema como muestra la ilustración 109. Destacamos la ejecución del programa Adb App Control, que se trata de una herramienta de desarrollo empleada para la gestión de las aplicaciones en los teléfonos Android.



Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment	Data Source
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	48027	603962		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	3711	14956		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	1900	52752		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	3564	4144		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	22818	56495		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	64979	1040022		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	1174	2032		Drive 0:WHD
System Resource Usage - Network Usage		2022-03-14 23:06:00 CET	4555	10349		Drive 0:WHD

Ilustración 109: Programas ejecutados en el sistema

Y para finalizar se muestra la lista de los dispositivos USB conectados al sistema que se ha recuperado del archivo SYSTEM de los registros de Windows. En el detalle de la Ilustración 110 observamos que se ha conectado por USB un disco duro externo de la marca Western Digital.

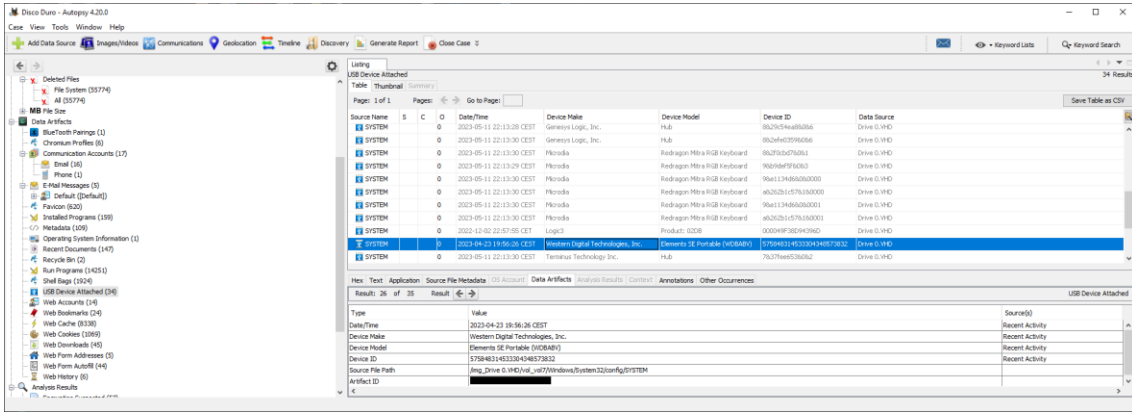


Ilustración 110: Dispositivos USB conectados al equipo

Si quisiéramos exportar cualquier dato de los recuperados en el análisis simplemente deberemos de hacer click derecho sobre el fichero y seleccionar la opción de exportar que nos abrirá una ventana de guardado de archivos como la que muestra la Ilustración 111.

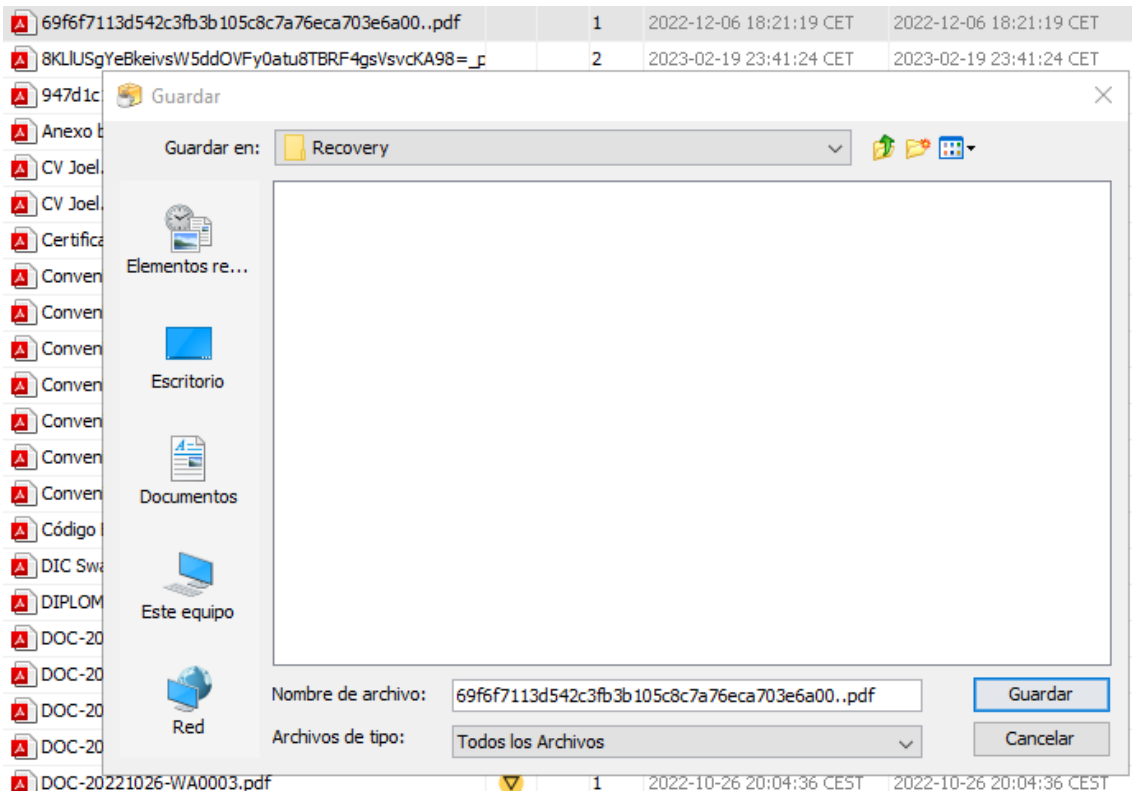


Ilustración 111: Exportación de archivos del análisis

Como función adicional a destacar si hacemos click en el icono de Geolocalización ubicado en la barra de herramientas del programa nos abrirá una ventana en la que nos mostrará los datos de aquellos archivos que contengan metadatos con coordenadas GPS y los ubicará en el mapa como se aprecia en la Ilustración 112.



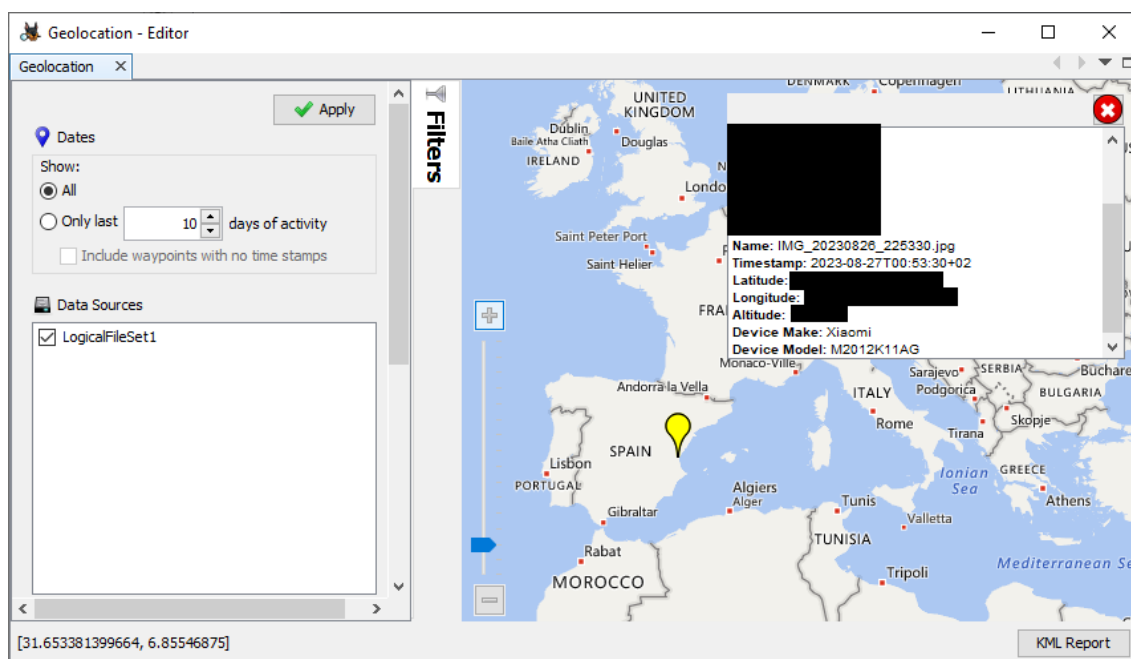


Ilustración 112: Metadatos de geolocalización

Tras mostrar estos ejemplos de información recuperada queda constancia de la potencia de esta herramienta en cuanto al análisis y la recuperación de archivos. La cantidad de archivos recuperados es enorme al igual que sus tipos y la información que contienen. Se ha tratado de escoger ejemplos significativos de los que se ha podido extraer información relevante con el fin de demostrar las utilidades de esta herramienta y de la información recuperada por esta.

Como conclusión podemos definir a Autopsy como una herramienta muy completa para la recuperación y el análisis de datos, ya que con su escaneo profundo del disco duro ha recuperado una gran cantidad de archivos de los cuales hemos podido obtener datos que podrían ser muy relevantes en cualquier investigación forense, ya que hemos podido extraer datos de propietarios de archivos con nombres personales, datos fiscales, cuentas bancarias, imágenes eliminadas del sistema de archivos y otros ejemplos anteriormente mostrados. Cabe destacar que muchos de los módulos de Autopsy han recogido la misma información que otros programas de uso individual como Browser History Examiner, por lo que esta recopilación de utilidades basada en módulos de programa la hace la herramienta perfecta para cualquier tipo de análisis de datos digitales a cualquier nivel de profundidad que nos propongamos llegar.

## 5.2 Preservación de información

En este apartado veremos cómo la criptografía nos permite preservar la información asegurando la integridad de los archivos una vez han sido obtenidos y tener total certeza de que estos no han sido modificados por agentes externos. Veremos los mecanismos que se pueden emplear y las herramientas propias del sistema operativo que nos hacen posible esta tarea, por lo que no será necesario el

uso de herramientas adicionales debido a que para esta demostración cumplen con el objetivo que se persigue.

Se emplearán técnicas de criptografía como la generación de valores hash de los archivos recuperados como evidencias en el proceso de recuperación y análisis de información garantizando así la preservación de estos archivos como una evidencia sólida que se mantiene intacta a lo largo de todo el proceso judicial.

### 5.2.1 Función hash criptográfica

Una función hash es un método criptográfico para generar una clave que sea considerada como un identificador unívoco de un fichero. Estas funciones solo funcionan en un sentido, ya que transforman datos de entrada como puede ser un fichero de texto en una serie de caracteres de salida de longitud fija. Esta salida es a lo que llamamos hash. Al ser una función unidireccional es muy sencillo calcular el valor hash a partir de un conjunto de datos de entrada, pero es prácticamente imposible poder hacer el proceso a la inversa de tal forma que se pueda recuperar el conjunto de datos de entrada original a partir del valor hash que se ha generado mediante la función.

El hash se utiliza para verificar si los datos han sido modificados o corrompidos. Cuando se envían o almacenan datos, se puede calcular el hash antes y después de transmitir o almacenar los datos, y luego comparar los dos valores para asegurarse de que los datos no hayan sido alterados en el proceso garantizando así su integridad. Esto nos va a permitir garantizar que los archivos obtenidos en la fase de extracción se puedan conservar sin modificaciones durante todo el proceso de investigación, desde que son recuperados hasta que son presentados como prueba.

Es importante destacar que, aunque los algoritmos de hash son muy útiles para la verificación y la seguridad, no son perfectos. En algunos casos, pueden ocurrir colisiones, donde dos conjuntos de datos diferentes generan el mismo valor hash. Sin embargo, los algoritmos de hash modernos están diseñados para minimizar la probabilidad de colisiones y ofrecer un alto grado de seguridad y confiabilidad como puede ser el algoritmo SHA-256 que genera salidas de 64 caracteres en formato hexadecimal de tal forma que la cantidad de valores distintos que puede generar es del orden de  $2^{256}$  y eso hace extremadamente improbable que ocurra una colisión comparando el hash de un archivo cuando se trata de asegurar la integridad de los datos.

Tanto en sistemas Linux como en sistemas Windows disponemos de herramientas propias del sistema con las cuales podemos llevar a cabo esta tarea, como son la Terminal de Linux y la PowerShell de Windows. En ambos casos usaremos el mismo algoritmo para generar el valor hash, que será SHA-256.

Para nuestro caso práctico crearemos un fichero de texto con el editor de texto nano llamado mensaje.txt y le dotaremos de contenido. Basta con escribir una frase simple como la que se emplea en la Ilustración 111.

```
GNU nano 7.2          mensaje.txt *
Este mensaje es privado. El contenido del mensaje no debe de ser modificado.
```

Ilustración 113: Contenido del archivo



Una vez hemos generado el fichero y hemos guardado los cambios generamos su hash. En Linux nos iremos a la ruta del archivo que hemos generado y escribiremos el siguiente comando para generar el hash:

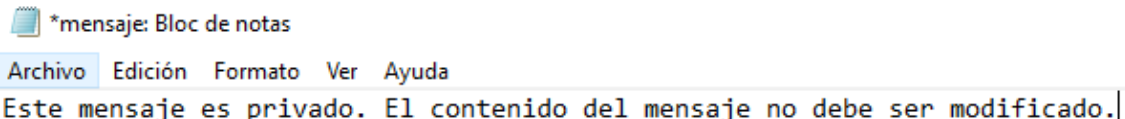
```
sha256sum mensaje.txt
```

La salida nos devuelve el valor hash que corresponde a la cadena hexadecimal y el nombre del archivo del que se ha generado el hash como se observa en la ilustración:

```
user@ubuntu:~/Documents$ nano mensaje.txt
user@ubuntu:~/Documents$ sha256sum mensaje.txt
a53772fcd203b8ed32d89b7166540e976bfb45cf40497cd72596d90984ca5a1b mensaje.txt
```

Ilustración 114: Hash de mensaje.txt

En el caso de Windows generamos el archivo de texto con el editor de texto Bloc de notas y guardamos los cambios que hemos hecho en el fichero.



\*mensaje: Bloc de notas

Archivo Edición Formato Ver Ayuda

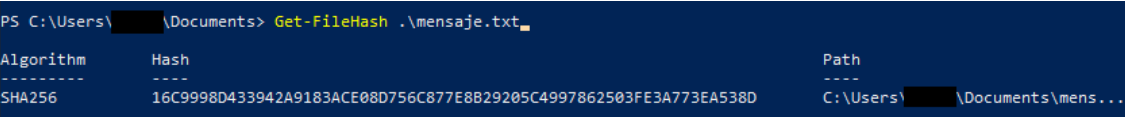
Este mensaje es privado. El contenido del mensaje no debe ser modificado.

Ilustración 115: Contenido del archivo

Posteriormente abriremos una consola de PowerShell. Nos dirigimos a la ruta del archivo y ejecutamos el siguiente comando:

```
Get-FileHash .\mensaje.txt
```

Este comando devuelve una salida especificando el algoritmo utilizado, el valor hash en hexadecimal y la ruta absoluta del archivo como vemos en la ilustración:



```
PS C:\Users\████████\Documents> Get-FileHash .\mensaje.txt
Algorithm Hash Path
-----
SHA256 16C9998D433942A9183ACE08D756C877E8B29205C4997862503FE3A773EA538D C:\Users\████████\Documents\mens...
```

Ilustración 116: Hash de mensaje.txt

Habiendo obtenido previamente el valor hash de los archivos vamos a modificarlos ligeramente para generar de nuevo los valores hash, que serán distintos a los obtenidos anteriormente cuando el fichero no se había modificado. En las ilustraciones se muestra el contenido del archivo tras su modificación en ambos sistemas:

```

GNU nano 7.2                                mensaje.txt *
Este mensaje es privado, el contenido del mensaje no debe de ser modificado.

mensaje: Bloc de notas
Archivo Edición Formato Ver Ayuda
Este mensaje es privado, el contenido del mensaje no debe ser modificado.

```

Ilustración 117: Mensaje modificado

Repetimos la ejecución de los comandos y generamos el segundo hash, pudiendo compararlos frente a frente como podemos observar en las ilustraciones:

```

user@ubuntu:~/Documents$ nano mensaje.txt
user@ubuntu:~/Documents$ sha256sum mensaje.txt
a53772fcd203b8ed32d89b7166540e976bfb45cf40497cd72596d90984ca5a1b mensaje.txt
user@ubuntu:~/Documents$ nano mensaje.txt
user@ubuntu:~/Documents$ sha256sum mensaje.txt
4a23e15caed237882eb0be7f9713641878c17618bc1f8a2f5cceb4f93507c4f3 mensaje.txt
user@ubuntu:~/Documents$

```

Ilustración 118: Comparación hash Linux

```

PS C:\Users\██████\Documents> Get-FileHash .\mensaje.txt
Algorithm Hash Path
-----
SHA256 16C9998D433942A9183ACE08D756C877E8B29205C4997862503FE3A773EA538D C:\Users\██████\Documents\mens...

PS C:\Users\██████\Documents> Get-FileHash .\mensaje.txt
Algorithm Hash Path
-----
SHA256 AC6BA06FF480C3CAC0CCCD3482DDACA4677509E5568FFB4DBAB8AA6F272288ED C:\Users\██████\Documents\mens...

```

Ilustración 119: Comparación hash Windows

Como podemos observar el valor hash de los archivos una vez han sido modificados ha cambiado. A pesar de que en este caso se ha modificado el contenido del archivo sin alterar el significado se puede verificar que el archivo ha sido modificado ya que los 2 valores hash no coinciden. Si se tratase del mismo archivo sin modificaciones posteriores ambos hashes serían idénticos independientemente del nombre del archivo ya que solamente compara el contenido del archivo para generar la clave.

Cabe destacar que para poder realizar esta comparación debe de generarse el primer hash y guardarse la salida de estos comandos en un fichero de texto aparte, de tal manera que podamos disponer de este hash una vez queramos verificar la integridad del archivo en cuestión generando el segundo hash y comparándolo con el primero para ver si son idénticos y el archivo se mantiene intacto, o bien son diferentes y el archivo ha sido modificado tras la generación del primer hash y no mantiene su integridad.

A pesar de que existen programas complejos que disponen de varios algoritmos de generación de claves y otras características avanzadas no se ha considerado oportuno su uso debido a que para la ejemplificación y puesta en práctica no es necesario contar con otras alternativas debido a que la complejidad de uso de los comandos mostrados anteriormente se reduce al mínimo y el resultado final es igual de efectivo en el contexto de uso en el cual podríamos emplear otras herramientas más complejas



y no tan difíciles de usar, que si bien abarcan mucho más y aportan otras funcionalidades extra además de la función que ya cumplen los comandos todo aquello que ofrecen adicionalmente no resulta de interés para este caso particular.

Esta simple y rápida generación y comparación de valores hash que se ha realizado empleando herramientas propias del sistema es crucial para garantizar la integridad de una evidencia a lo largo de todo el proceso que dure una investigación forense. De esta manera podremos comprobar que la evidencia analizada, los datos originales y la evidencia presentada se tratan del mismo archivo sin ninguna modificación garantizando así la cadena de custodia.

## 6. Conclusiones

---

En este capítulo se recogen las conclusiones alcanzadas tras el desarrollo del proyecto y los resultados alcanzados, se proporciona una reflexión de las implicaciones del proyecto con la legislación y normativas que afectan a la informática forense y finalmente se relaciona el proyecto con los estudios cursados por el alumno.

### 6.1 Grado de cumplimiento de los objetivos

El principal objetivo de este proyecto ha sido realizar un análisis forense de un sistema operativo con el propósito de identificar y sacar a la luz la huella digital de un usuario de dicho sistema. Este objetivo se ha materializado en dos sistemas reales, uno Linux y otro Windows, que han sido objeto de análisis en un entorno de laboratorio creado específicamente para este fin. Tras los resultados obtenidos podemos llegar a la conclusión de que se ha alcanzado el objetivo de mostrar esta huella digital mediante el uso de herramientas de análisis y extracción de datos, aplicando en cada caso técnicas propias del campo de la informática forense.

Como es lógico no se han mostrado todos los registros del sistema ni se han analizado todos los archivos del usuario, sino que se han seleccionado ciertos datos en concreto de los que hemos podido obtener información relevante del usuario o del propio sistema operativo. Es decir, nos hemos enfocado en ejemplos concretos de datos para ejemplificar el formato que tienen, mostrar el tipo de información que aportan y deducir el uso particular que el usuario ha hecho del sistema. Entre estos ejemplos se incluyen registros de actividad, archivos empleados por el usuario, programas instalados en el sistema, procesos en ejecución y otros hallazgos significativos. Estos ejemplos proporcionan evidencia sólida de la capacidad del análisis forense para revelar la huella digital de un usuario.

La identificación de las fuentes de información en el sistema operativo han demostrado ser elementos cruciales en este proceso. Elementos como el sistema de archivos, el registro del sistema y los registros de eventos se han revelado como pilares fundamentales para rastrear la actividad del usuario y entender su relación con el sistema. Cada sistema operativo tiene sus peculiaridades respecto a dichas fuentes de información, que han quedado patentes durante el desarrollo del proyecto y se han recogido en esta memoria.

Se han aplicado técnicas forenses concretas a lo largo del desarrollo del proyecto. La preservación de la evidencia, el análisis de los datos obtenidos y el uso de herramientas especializadas han sido técnicas críticas para alcanzar estos resultados. En particular, se ha logrado capturar y aislar de forma completa la máquina objeto de estudio, para trabajar sobre ella en un entorno de laboratorio basado en máquinas virtuales garantizando que durante el análisis realizado la máquina original queda intacta y no se aplican modificaciones sobre ella. La copia del sistema objeto de estudio en una imagen de disco puede considerarse una evidencia en sí misma además de poder preservarse como una copia de seguridad de la máquina original.



Para demostrar la identificación e interpretación de la huella digital, hemos presentado ejemplos y evidencias concretos obtenidos a partir del análisis forense de un sistema Linux y otro Windows. Estos ejemplos incluyen registros de actividad, acceso a archivos específicos y otros hallazgos de información relevante que respaldan con firmeza nuestra capacidad para obtener la huella digital del usuario y comprenderla tras su análisis. En este caso, al tratarse de sistemas de uso personal del propio alumno no ha sido necesario un proceso de deducción de las acciones del usuario del sistema, ya que, desde el principio, a la hora de recuperar y analizar los datos ya se sabía lo que se iba a encontrar. De hecho, los sistemas objeto de análisis estaban instalados en el ordenador personal del alumno para su uso cotidiano, incluyendo actividades lúdicas, educativas o laborales. Es por ello que, en el transcurso de la memoria, se han ocultado explícitamente ciertos datos sensibles, que desvelarían información de carácter personal.

Por otro lado, el proyecto ha tenido en cuenta las implicaciones legales relacionadas con la informática forense, y las ha expuesto en la memoria. Sin embargo, en este caso no ha sido necesario aplicar las normativas habituales en este tipo de procesos, al tratarse del análisis de los sistemas personales del propio alumno, y no de un tercero. En este último caso sí habría sido necesario contemplar dicha legislación, incluyendo entre muchos otros una orden judicial para investigar un sistema concreto, regulaciones sobre acceso a datos sensibles como datos médicos, fiscales o financieros, y los derechos de privacidad de un individuo o una entidad que garantizan que el acceso a los datos personales se haga de forma legal y ética. Sin embargo, como decíamos arriba, en virtud de dichos derechos de privacidad, en la memoria se han censurado ciertos datos, tales como *hashes* de contraseñas del sistema, nombres completos, direcciones de correo personales, números de identificación fiscal y datos de cuentas bancarias. Durante el proyecto se ha identificado y mostrado su formato para ilustrar las capacidades de las herramientas de análisis, pero en la memoria se han ocultado para mantener la privacidad del autor.

En resumen, pensamos que este proyecto ha evidenciado que el análisis forense de las fuentes de información del sistema operativo es una herramienta esencial para desentrañar la huella digital de un usuario en un sistema informático.

## 6.2 Relación con los estudios cursados

El proyecto realizado tiene relación con los conocimientos adquiridos en las asignaturas “Fundamentos de sistemas operativos”, “Administración de sistemas”, “Seguridad en redes y sistemas informáticos” y “Sistemas y servicios en red”, como se detalla a continuación.

“Fundamentos de sistemas operativos” ha sido esencial para adquirir las habilidades necesarias para el manejo de sistemas Linux mediante la consola de comandos Terminal.

“Administración de sistemas” ha sido clave para cubrir la administración del sistema Windows, el conocimiento de las directivas de seguridad del sistema y el manejo de la consola cmd y PowerShell para uso avanzado del sistema.

“Seguridad en redes y sistemas informáticos” ha otorgado los conocimientos esenciales de seguridad en sistemas informáticos y sus prácticas se realizaron en un entorno de máquinas virtuales que se encontraban en la misma red, por lo que el montaje del entorno de trabajo ha sido posible en gran parte por estos contenidos vistos en la asignatura.

Además de esto se han adquirido las siguientes competencias transversales durante los estudios cursados y han sido aplicadas a la realización de este proyecto:

- CT\_09 - Pensamiento crítico
- CT\_11. Aprendizaje permanente
- CT\_13 - Instrumental específica

En particular, la competencia instrumental específica se incluye ya que en el proyecto se han empleado herramientas específicas para la tarea de recuperación, análisis y visualización de los datos. Por otro lado, el pensamiento crítico ha sido esencial a la hora de aplicar los métodos y técnicas empleados, y en la tarea de descifrar la información que nos pueden proporcionar los datos obtenidos durante el análisis.



## 7. Bibliografía

---

[1] « Constitución Española | Boletín Oficial del Estado ». [En línea].

Disponible en:

<https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>

[Accedido: may-2023]

[2] « Reglamento General de Protección de Datos | Boletín Oficial del Estado ». [En línea].

Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

[Accedido: jun-2023]

[3] « Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal | Boletín Oficial del Estado ». [En línea].

Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

[Accedido: may-2023]

[4] « Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones | Boletín Oficial del Estado ». [En línea].

Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>

[Accedido: may-2023]

[5] « Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales | Boletín Oficial del Estado ». [En línea].

Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

[Accedido: may-2023]

[6] « Estatuto de los Trabajadores | Boletín Oficial del Estado ». [En línea].

Disponible en: [https://www.boe.es/biblioteca\\_juridica/abrir\\_pdf.php?id=PUB-DT-2023-139](https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DT-2023-139)

[Accedido: may-2023]

[7] « Normativas Aplicables por el Perito Informático | GlobátiKa ». [En línea].

Disponible en: <https://peritosinformaticos.es/category/normativas-aplicables-por-el-perito-informatico>

[Accedido: may-2023]

[8] « FTK® Imager | Exterro ». [En línea].

Disponible en: <https://www.exterro.com/ftk-imager>

[Accedido: jul-2023]

[9] « Registry Viewer | Exterro ». [En línea].

Disponible en: <https://www.exterro.com/ftk-product-downloads/registry-viewer-2-0-0>

[Accedido: jul-2023]

[10] « ExifTool by Phil Harvey | ExifTool ». [En línea].

Disponible en: <https://exiftool.org>

[Accedido: jul-2023]

[11] « The Volatility Foundation - Open Source Memory Forensics | The Volatility Foundation ». [En línea].

Disponible en: <https://www.volatilityfoundation.org>

[Accedido: jul-2023]

[12] « Recover lost passwords stored in your Web browser | NirSoft ». [En línea].

Disponible en: [https://www.nirsoft.net/utils/web\\_browser\\_password.html](https://www.nirsoft.net/utils/web_browser_password.html)

[Accedido: jul-2023]

[13] « Browser History Examiner | Foxtton Forensics ». [En línea].

Disponible en: <https://www.foxttonforensics.com/browser-history-examiner>

[Accedido: jul-2023]

[14] « Autopsy | Digital Forensics ». [En línea].

Disponible en: <https://www.autopsy.com>

[Accedido: jul-2023]

[15] « VM VirtualBox | Oracle ». [En línea].

Disponible en: <https://www.virtualbox.org>

[Accedido: jul-2023]

[16] « Get Ubuntu | Ubuntu ». [En línea].

Disponible en: <https://ubuntu.com/download/desktop>

[Accedido: jul-2023]

[17] « Descargar imagen de disco de Windows 10 (archivo ISO) | Microsoft ». [En línea].

Disponible en: <https://www.microsoft.com/es-es/software-download/windows10>

[Accedido: jul-2023]

[18] « Disk2vhd - Sysinternals | Microsoft ». [En línea].

Disponible en: <https://learn.microsoft.com/es-es/sysinternals/downloads/disk2vhd>

[Accedido: jul-2023]

[19] « How to Make Disk Images in Linux with DD Command | Linux Hint ». [En línea].

Disponible en: <https://linuxhint.com/make-disk-images-dd-command-linux>

[Accedido: jul-2023]

[20] « QEMU disk image utility | QEMU ». [En línea].

Disponible en: <https://qemu-project.gitlab.io/qemu/tools/qemu-img.html>

[Accedido: jul-2023]

[21] « Download Python | Python.org ». [En línea].

Disponible en: <https://www.python.org/downloads>

[Accedido: jul-2023]

[22] « microsoft/avml - Acquire Volatile Memory for Linux | Microsoft ». [En línea].

Disponible en: <https://github.com/microsoft/avml>

[Accedido: jul-2023]

[23] « Historia de la Informática Forense timeline | Timetoast ». [En línea].

Disponible en: <https://www.timetoast.com/timelines/historia-de-la-informatica-forense-41d18e84-554f-4ea5-856a-01864e1d401e>

[Accedido: may-2023]

## ANEXO A

### OBJETIVOS DE DESARROLLO SOSTENIBLE

#### Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. <b>Fin de la pobreza.</b>				<b>X</b>
ODS 2. <b>Hambre cero.</b>				<b>X</b>
ODS 3. <b>Salud y bienestar.</b>				<b>X</b>
ODS 4. <b>Educación de calidad.</b>				<b>X</b>
ODS 5. <b>Igualdad de género.</b>				<b>X</b>
ODS 6. <b>Agua limpia y saneamiento.</b>				<b>X</b>
ODS 7. <b>Energía asequible y no contaminante.</b>				<b>X</b>
ODS 8. <b>Trabajo decente y crecimiento económico.</b>				<b>X</b>
ODS 9. <b>Industria, innovación e infraestructuras.</b>				<b>X</b>
ODS 10. <b>Reducción de las desigualdades.</b>				<b>X</b>
ODS 11. <b>Ciudades y comunidades sostenibles.</b>				<b>X</b>
ODS 12. <b>Producción y consumo responsables.</b>				<b>X</b>
ODS 13. <b>Acción por el clima.</b>				<b>X</b>
ODS 14. <b>Vida submarina.</b>				<b>X</b>
ODS 15. <b>Vida de ecosistemas terrestres.</b>				<b>X</b>
ODS 16. <b>Paz, justicia e instituciones sólidas.</b>	<b>X</b>			
ODS 17. <b>Alianzas para lograr objetivos.</b>				<b>X</b>



## **Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.**

De todos los objetivos de desarrollo sostenible que se mencionan anteriormente este trabajo está relacionado con:

- **Paz, justicia e instituciones sólidas**, ya que el análisis forense de sistemas operativos y la identificación de la huella digital son esenciales para promover la justicia y construir instituciones sólidas. Este tipo de trabajo contribuye a la capacidad de las instituciones y organismos de aplicación de la ley para investigar y resolver delitos informáticos, lo que a su vez contribuye a mantener la paz y la seguridad en el entorno digital.

Principalmente este proyecto cumple con este objetivo de desarrollo sostenible debido a que el análisis forense de sistemas operativos contribuye directamente a la promoción de la justicia al ayudar en la identificación de huellas y pruebas digitales que pueden ser utilizadas en investigaciones y procesos judiciales. Estas pruebas pueden ser cruciales para demostrar la culpabilidad o inocencia de las partes involucradas, garantizando así que se haga justicia.

El proyecto contribuye al fortalecimiento de instituciones sólidas, en particular, aquellas relacionadas con la ciber seguridad y la aplicación de la ley en el entorno digital. Proporciona a estas instituciones las herramientas y los conocimientos necesarios para abordar los delitos informáticos de manera eficiente y efectiva, lo que a su vez mejora su capacidad para mantener la paz y la seguridad en la sociedad.