Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Trabajo de Fin de Grado

Grado en Ingeniería Informática

Rastreando evidencia digital: Metodologías de trabajo y análisis en informática forense

Tracking Digital Evidence: Work Methodologies and Analysis in Forensic Computing

Carla Oval Torres

La Laguna, 11 de julio de 2024

Dña. **Pino Caballero Gil**, Catedrática de Universidad adscrita al Departamento de Ingeniería Informática y de Sistemas en el área de Ciencias de la Computación e Inteligencia Artificial de la Universidad de La Laguna, como tutora

Dña. **Candelaria Hernández Goya**, profesora Titular de Universidad adscrita al Departamento de Ingeniería Informática y de Sistemas en el área de Ciencias de la Computación e Inteligencia Artificial de la Universidad de La Laguna, como cotutora

C E R T I F I C A (N)

Que la presente memoria titulada:

"*Rastreando evidencia digital: Metodologías de trabajo y análisis en informática forense*" ha sido realizada bajo su dirección por Dña. **Carla Oval Torres**, con N.I.F. 45941706B.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 10 de julio de 2024.

Agradecimientos

A Irene Cotillas Torres, por su valiosa guía y apoyo durante la elaboración de este trabajo, y por todos los conocimientos que me ha transmitido sobre esta área en la que es experta.

A mi tutora Pino Caballero Gil y a mi cotutora Candelaria Hernández Goya que con su disposición y recursos, han hecho posible la elaboración y presentación de este trabajo.

A aquellos profesores de la Universidad de La Laguna y de la Escuela Superior de de Ingeniería y Tecnología que me han dado la motivación para continuar a pesar del arduo camino.

A los compañeros de carrera y de estudio que se han convertido en amigos, y que han hecho más ameno el recorrido.

A mi familia y amigos cercanos, por su aliento y por estar siempre ahí.

A Helena García Díaz, Norberto Medina Rodríguez, Adrián Fleitas de la Rosa y sus familias, por su apoyo, amor y amistad, que han sido invaluables y han marcado mi camino y mi vida.

Gracias a todos por haber contribuido a hacer posible que haya llegado hasta aquí.

Licencia

Resumen

El presente trabajo se centra en explorar el campo de la informática forense, una disciplina crucial en la resolución de delitos e incidentes digitales. La investigación comienza contextualizando la informática forense y estableciendo sus objetivos, respaldados por casos reales donde esta disciplina ha sido esencial.

Se aborda el marco legal como componente fundamental, abordando definiciones de delitos informáticos, tipos y ejemplos específicos, así como las leyes nacionales e internacionales pertinentes. Se analiza la ley en materia de protección de datos al respecto, la evidencia digital y sus criterios de admisibilidad en juicio, las exigencias de la cadena de custodia, los derechos y deberes de los peritos forenses, y la jurisdicción en casos de delitos informáticos.

Una sección significativa del trabajo explora las metodologías actuales en informática forense, detallando las fases de un análisis forense, la existencia y mitigación de las técnicas antiforenses, la importancia de la cadena de custodia y su admisibilidad en un juicio y otras metodologías relevantes actualmente en el campo.

Para enriquecer aún más la investigación, se incluye un estudio de caso práctico sobre el análisis de una máquina previamente infectada donde se ha manipulado la evidencia, como se haría en una consultoría, utilizando la imagen forense del disco duro (Windows 10) de dicha máquina. Se proporcionará una traza completa haciendo un esquema gráfico de cómo hemos infectado la máquina como prueba de concepto (PoC), del proceso de infección y de todos los artefactos del sistema, destacando la metodología y herramientas empleadas y los resultados obtenidos, con lecciones aprendidas y conclusiones derivadas de esta experiencia.

Con este proyecto se pretende abordar las metodologías usadas en la informática forense en el contexto actual, discutiendo las implicaciones y desafíos para los peritos forenses, y se ofrecen perspectivas futuras en este campo dinámico.

Palabras clave: Informática forense, delitos informáticos, evidencia digital, marco legal, protección de datos, cadena de custodia, peritos forenses, metodologías, análisis forense, técnicas antiforenses, estudio de caso, imagen forense, prueba de concepto, artefactos del sistema, herramientas forenses, implicaciones, desafíos, perspectivas futuras.

Abstract

This paper focuses on exploring the field of forensic computing, a crucial discipline in resolving digital crimes and incidents. The research begins by contextualizing forensic computing and establishing its objectives, supported by real cases where this discipline has been essential.

The legal framework is addressed as a fundamental component, covering definitions of cybercrimes, specific types and examples, as well as relevant national and international laws. Data protection law is analyzed in relation to digital evidence and its admissibility criteria in court, chain of custody requirements, the rights and duties of forensic experts, and jurisdiction in cases of cybercrimes.

A significant section of the paper explores current methodologies in forensic computing, detailing the phases of forensic analysis, the existence and mitigation of anti-forensic techniques, the importance of chain of custody and its admissibility in court, and other relevant methodologies currently in the field.

To further enrich the research, a practical case study is included, focusing on the analysis of a previously infected machine where evidence has been tampered with. This analysis is conducted in a consultancy-like manner, using a forensic image of the machine's hard drive (Windows 10). A complete trace will be provided by outlining how the machine was infected in graphical mode as a proof of concept (PoC), the infection process, and all system artifacts, highlighting the methodology and tools used and the results obtained, with lessons learned and conclusions drawn from this experience.

This project aims to address the methodologies used in forensic computing in the current context, discussing the implications and challenges for forensic experts, and offering future perspectives in this dynamic field.

Keywords: Forensic computing, cybercrimes, digital evidence, legal framework, data protection, chain of custody, forensic experts, methodologies, forensic analysis, anti-forensic techniques, case study, forensic image, proof of concept, system artifacts, forensic tools, implications, challenges, future perspectives.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

En aras de brindar una comprensión contextual exhaustiva sobre el ámbito principal de este trabajo, nos sumergiremos en un análisis detallado de los antecedentes y fundamentos que delinean la importancia y la relevancia de nuestra investigación.

1.1. ¿Qué es la informática forense?

La informática forense es una disciplina que se encarga de la aplicación de técnicas y métodos de investigación científica y analítica para recolectar, preservar, analizar y presentar evidencia digital con el objetivo de resolver casos criminales y disputas legales relacionadas con sistemas y redes informáticas [1] [2] [3].

Esta evidencia puede ser utilizada en procedimientos judiciales, auditorías, investigaciones de seguridad de la información, fraudes y otras actividades relacionadas con el derecho informático.

1.2. Contexto, justificación y objetivos

1.2.1. Situación actual de la informática forense

La disciplina forense en el ámbito de la informática ha evolucionado de manera muy rápida respecto a otras disciplinas, en respuesta al crecimiento vertiginoso de la tecnología y a la creciente dependencia en nuestra sociedad de los sistemas informáticos. La proliferación de cada vez más dispositivos y tecnologías ha ido a la par con los conflictos en el uso de las mismas, reafirmando cada vez más la necesidad de las soluciones que nos proporciona el análisis forense [4].

En la década de 1970, tras la llegada de los primeros ordenadores personales, se establece la fecha de referencia para el sistema de marcas de tiempo (timestamps) en formato Unix. Esta fecha es el punto de inicio desde el cual se cuentan los segundos transcurridos para representar fechas y horas en muchos sistemas operativos y aplicaciones, donde la fecha más antigua es el 1 de enero de 1601 (navegadores basados en Chromium) o en 1 de enero de 1970 (Mozilla). La fecha en formato unix cuenta los segundos que han pasado desde el uno de enero de 1970 a medianoche, para hacer la traducción en un formato de fecha UTC (+ 1 o +2).

La informática forense dio sus primeros pasos, con un comienzo modesto centrado en el análisis de sistemas informáticos para la recuperación y extracción de datos debido a errores inesperados, ya fueran técnicos o humanos, principalmente en empresas con sistemas centralizados. Durante este periodo, existía poco o ningún interés o esfuerzo en el desarrollo de la especialidad forense en la sociedad [5].

Más tarde, en la década de 1980, concretamente entre 1984 y 1996, comenzaron los que se vienen considerando los primeros años de la era moderna de la informática forense, donde se presenció la aparición de nuevos crímenes informáticos, aumentando estos también considerablemente en número. Este incremento fue caracterizado y propiciado por el uso cada vez más extendido de los ordenadores para uso personal y de las redes de uso privado, además de la estandarización de formatos de ficheros, llevando en consecuencia al aumento significativo de incidentes informáticos. Durante este periodo, los expertos comenzaron a especializarse en la investigación de estos delitos, respondiendo a la creciente complejidad y sofisticación de las amenazas cibernéticas, y a una necesidad en aumento en el ámbito judicial, marcando el inicio de la evolución exponencial que experimentaría la disciplina en las siguientes décadas. En este periodo se crea la Agencia Española de Protección de Datos (AEPD) en 1986, para velar por la privacidad y protección de datos personales en España [6] [7].

Las décadas de 1990 y los 2000, concretamente entre 1997 y 2007, son consideradas la era dorada de la informática forense, ya que fue durante este periodo cuando se consolidó el reconocimiento social e institucional de la informática forense. Esto es evidenciado por el desarrollo de herramientas forenses específicas destinadas a facilitar y mejorar la capacidad de investigar delitos relacionados con la informática, y por la creación de nuevas unidades especializadas en las fuerzas de seguridad para abordar crímenes informáticos.

Entre estas últimas destacan en la primera década, ambas creados en 1996:

- La Brigada Central de Investigación Tecnológica (BCIT) [8].
- El Grupo de Delitos Telemáticos (GDT) [9], integrado en la Unidad Central Operativa de la Guardia Civil.

También surgieron en la segunda década, tras el cambio de milenio:

- El Centro Criptológico Nacional (CCN) [10].
- El Instituto Nacional de Tecnologías de la Comunicación (INTECO) que en 2014, se transformó en el Instituto Nacional de Ciberseguridad (INCIBE) [11] [12].
- El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional (CCN-CERT) [13].
- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) [14] [15].

Dentro de la década del 2000, entre 2007 y 2009, se presenció el comienzo de un proceso cada vez más evidente de globalización de las amenazas cibernéticas, caracterizado por un marcado aumento de delitos informáticos transfronterizos, ya que las nuevas

tecnologías de la información habían diluido muchas de las barreras que antes limitaban a los ciberatacantes. Durante este periodo, se estableció una colaboración internacional significativa en la lucha contra el cibercrimen. El incremento en la sofisticación y alcance de las amenazas digitales impulsó esta necesidad de una cooperación más estrecha entre países y organizaciones para abordar de manera efectiva los desafíos emergentes en el ámbito cibernético y el desarrollo de mecanismos de ciberdefensa, siendo grandes preocupaciones especialmente los delitos relacionados con el crimen organizado, el espionaje industrial y la privacidad de la información [16].

En la actualidad, se ha seguido esta tendencia, pues el crecimiento exponencial de los incidentes cibernéticos ha sido impulsado por la creciente conectividad y acceso a la tecnología, resultando en delitos más frecuentes y sofisticados [17] [18] [19] [20].

Este escenario ha motivado el desarrollo de tecnologías forenses avanzadas, que incluyen herramientas especializadas y técnicas para investigar dispositivos complejos. Además, se enfrentan al surgimiento de mecanismos contra la recuperación de evidencias, como es el caso de las técnicas antiforenses, cada vez más sofisticadas, utilizadas para evadir la detección. La expansión de los campos de aplicación demuestra que la informática forense consolidándose como una disciplina crucial en la gestión de incidentes digitales en la era actual,con cada vez más retos por delante, que la presentan como herramienta indispensable para nuestra sociedad y nuestro día a día .

1.2.2. Estudio estadístico de la incidencia de la ciberdelincuencia

Según datos públicos del ministerio del interior, en el año 2011 se cometieron 37.458 ciberdelitos en España. En el último informe del OEDI del ministerio [19] en 2022, ha ascendido esta cifra a 305.477 delitos. Como podemos ver en la gráfica siguiente (figura 1.1), cada año aumentan los delitos informáticos que se cometen en territorio español.

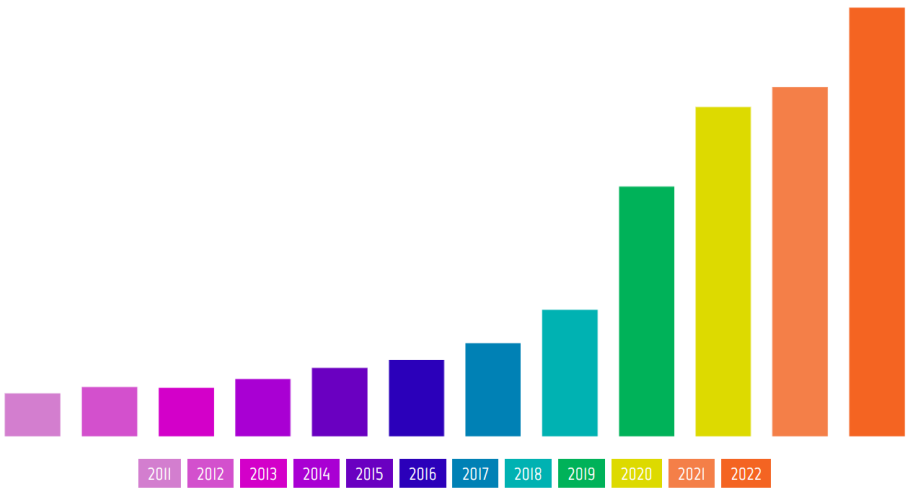


Figura 1.1: Actividad cibercriminal anual entre 2011-2022 en España [19]

Si desglosamos estos datos por tipología del delito (figura 1.2), se pueden observar tanto la tendencia al aumento del total de delitos anualmente, como las categorías con más incidencia, entre los cuales estarían, con mucha diferencia sobre los demás, los delitos de fraude informático seguidos de los delitos de amenazas y coacciones.

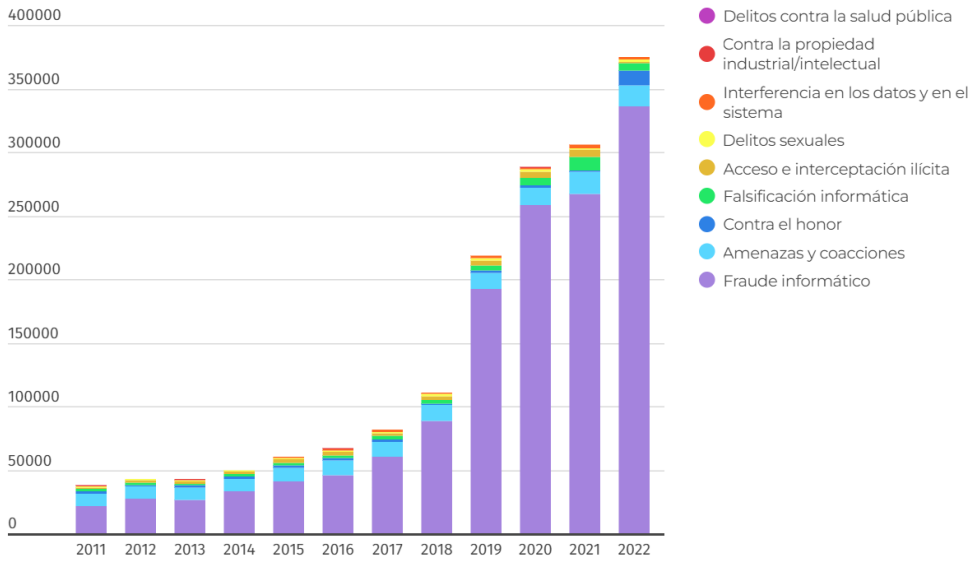


Figura 1.2: Actividad cibercriminal anual por tipología entre 2011-2022 en España [19]

Esta tendencia se ratifica en los informes anuales de cibercriminalidad del INCIBE, cuyos datos son obtenidos del Sistema Estadístico de Criminalidad (SEC), que nos aportan muchos datos estadísticos relevantes y curiosos sobre la incidencia en la población de la cibercriminalidad [17] [18] [19] [20].

Según estos datos, existe un rango concreto mantenido durante el tiempo en el cual el mayor número de víctimas de delitos informáticos se encuentra en el rango de edad de entre los 26-40 años, decreciendo ligeramente en rangos posteriores, siendo este rango el que posee una más alta incidencia. Esta distribución tan peculiar puede estar motivada por un mayor uso de la tecnología en los primeros rangos de edades, y sin embargo un mayor conocimiento de la misma que contribuye a evitar las estafas más comunes, junto con una exposición no tan frecuente en los rangos más alejados con un menor conocimiento general de la tecnología, resultando en una proporción en base a uso, que nos indica que las personas de los rangos de mayor edad, pese a no usar tanto la tecnología, suelen caer más fácilmente en los engaños de los criminales, sobre todo en casos de ingeniería social, y por tanto suelen suponer víctimas con más frecuencia, haciendo que proporcionalmente al grupo más joven, la incidencia en este grupo etario sea mucho mayor [21].

Por otro lado, en cuanto a los cibercriminales, los datos apuntan mucho más drásticamente a este mismo rango de entre 26-40 años, no siendo tan ligero el descenso en rangos posteriores, lo que tiene sentido si pensamos que para ser víctima, se acrecientan las posibilidades con el desconocimiento de la tecnología, y sin embargo, a la hora de cometer un delito informático, el conocimiento sobre las tecnologías de la información, e incluso amplia experiencia y conocimientos técnicos son necesarios y requeridos.

1.2.3. Casos reales donde ha sido crucial esta disciplina

El peritaje forense en toda su amplitud, ha esclarecido la verdad de los hechos en cuanto a criminología se refiere en innumerables casos de diversa naturaleza, con un impacto mediático a nivel nacional e internacional. Y aunque existen más casos de los que podemos abarcar en este trabajo, algunos ejemplos donde la informática forense fue especialmente relevante se incluyen a continuación.

El caso del asesino BTK (Bind, Torture, Kill) 1974-2005 [22] [23] o el posterior caso Guttman (1991).

Destacan casos de desapariciones como el caso Déborah (2002) [24], el de Madeleine McCann (2007) [25], el sonado caso de Diana Quer (2016) [26] [27] [28], o el caso de Marta del Castillo (2009) [29] [30].

En el ámbito de los delitos de hacking, malware y phishing, etc, podríamos mencionar los casos de Sony Pictures Hack (2014) [31], WannaCry (2017) [32] [33], o el más cercano Caso del Phishing de Correos (2019) [34]. Todos estos casos están más relacionados con nuestro caso práctico, en particular el caso de WannaCry, ya que analizamos un ransomware.

Por otro lado, el análisis forense se ha empleado también en casos de fraude, estafa, filtración y robo de información, como los casos de la quiebra de Enron (2001) [35] [36] [37], el caso de Wikileaks (2009), Chelsea Manning (2010) y Edward Snowden (2013), el Yahoo Data Breach (2013-2014), el Caso del Pequeño Nicolás (2014), la Operación Púnica (2014) o los Papeles de Panamá (2016) [38].

Incluso se emplea en casos de tráfico, terrorismo o crimen organizado como el desmantelamiento de Ross Ulbricht y Silk Road (2013), el caso Irán-Contras (1995) [39].

1.2.4. Objetivos y justificación del presente trabajo

Visto el encuadre anterior sobre la importancia e historia de la disciplina y la magnitud y aumento de los casos existentes a lo largo del tiempo, nuestro objetivo primordial en este proyecto es investigar el ámbito de la informática forense, comprendiendo tanto sus fundamentos teóricos como su contexto y utilidad ante la creciente necesidad de esta disciplina en cada vez más áreas de nuestra vida y nuestra sociedad. Esta exploración nos dotará de los conocimientos esenciales para abordar de manera más accesible y cercana, y con conocimiento de causa, el enfoque práctico y técnico de nuestro caso de estudio, que sería el colofón final de nuestro trabajo.

Capítulo 2

Marco legal de la informática forense

A continuación abordaremos el marco legal en el que navegan los peritos a la hora de realizar análisis forenses digitales.

2.1. Definición de delito informático

Un delito informático puede ser definido como “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas” [40].

Nos gusta esta definición, ya que a pesar de ser genérica, dada la variedad de delitos diferentes que existen, es imposible abarcarlos todos si empezamos a especificar detalles, y podemos aplicarla a cualquier delito que se nos ocurra [41].

2.2. Tipos de delitos informáticos

Debido a la dificultad anteriormente mencionada, definir una clasificación estática con lo cambiante que es el mundo de los delitos informáticos, donde constantemente aparecen nuevas tecnologías y amenazas, es una tarea ardua.

En el estudio estadístico previo se hace una clasificación genérica, pero ahondando un poco más, algunos ciberdelitos específicos y comunes que podemos nombrar son por ejemplo el uso de adware, spyware y malware (virus, troyanos, gusanos, etc.), la implantación de ransomware, el común (según datos previos) fraude en línea, que incluye por ejemplo el robo o suplantación de identidad (phishing) y diversos tipos de ingeniería social (grooming, sextorsión) donde podemos rozar en algunos casos la categoría de ciberacoso o ciberbullying. También existen los delitos de acceso no autorizado a sistemas informáticos (comúnmente denominados hacking), los ataques de denegación de servicio: Denial of Service (DoS) y Distributed DoS (DDoS), la infracción de derechos de autor o incluso el espionaje cibernético. Podríamos pasarnos todo el día indagando en esta lista, ya que por ejemplo la propia ingeniería social tiene muchos tipos según su proceder y objetivo, pero esta clasificación no es el tema principal que nos requiere en este trabajo [42] [43].

2.3. Leyes y regulaciones específicas

En esta disciplina en específico es muy importante seguir las normativas y regulaciones nacionales e internacionales, ya que al trabajar estrechamente con el ámbito legal, es a veces complejo discernir dónde acaba nuestra rama técnica y dónde lo relativo al derecho. Cualquier error puede afectar críticamente a la evidencia de un caso y por tanto al resultado del mismo y su sentencia.

2.3.1. Legislación nacional relacionada con la informática forense

A nivel nacional, existen una serie de leyes y normativas que han de ser conocidas por los peritos informáticos a la hora de llevar a cabo su labor.

Estas leyes son:

- La Constitución Española y los derechos fundamentales que otorga, siendo de particular interés los derechos a la seguridad jurídica y tutela judicial, al secreto de las comunicaciones, a la protección de datos, y a la vida privada, la intimidad y el honor [44].
- El marco legal que establece la Ley de Enjuiciamiento Civil, concretamente en sus artículos 299 y 340, donde exponen los medios de prueba (pudiendo ser estos medios informáticos) y las condiciones que debe cumplir un perito forense, respectivamente [45].
- La Ley de Enjuiciamiento Criminal de 14 de septiembre de 1882 también conocida como LECrim [46], que regulan la prueba pericial en el proceso penal en los artículos 456 a 485, y las obligaciones del perito en su artículo 335.3, que establece lo siguiente: *"El, o los, peritos abajo firmantes manifiestan, bajo promesa de decir verdad, que han actuado y, en su caso, actuarán con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conocen las sanciones penales en las que podrían incurrir si incumplieren su deber como perito."*
- La Ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico que regula aspectos como la prestación de servicios en línea, la contratación electrónica, la responsabilidad de los intermediarios en internet, la publicidad en línea, la protección de datos personales y la resolución de conflictos en línea, y protege a todos aquellos que intervienen en las relaciones ofrecidas por Internet estableciendo disposiciones legales para garantizar la seguridad jurídica en las transacciones electrónicas, promoviendo la confianza de los usuarios en el entorno digital y fomentado el desarrollo de la economía digital [47].
- La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, como su propio nombre indica, establece la obligación de los proveedores de servicios de telecomunicaciones de conservar los datos de tráfico y localización durante un período específico para facilitar en el caso de que la hubiere, la investigación, detección o prevención de delitos relacionados con las comunicaciones electrónicas [48].

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 9546CE (Reglamento general de protección de datos) que protege los derechos y la privacidad de las personas físicas en relación con el tratamiento de sus datos personales. Esta ley proporciona un marco legal integral que regula cómo las organizaciones deben recolectar, procesar y proteger los datos personales, asegurando así la transparencia, la seguridad y el control de los individuos sobre su información personal en un entorno digital, y los derechos de los mismos en cuanto a esta [49] [50].

- Y por último el Código penal (LO 10/1995 y última modificación en LO 1/2015), que recoge todas aquellas conductas y actividades tipificadas como delito, aplicables también a los delitos informáticos [51].

Además, recientemente el Instituto Nacional de Ciberseguridad de España (INCIBE), organismo dependiente de la Secretaría de Estado para el Avance Digital del Ministerio de Economía y Empresa, dentro de las funciones que tienen encomendadas para el desarrollo y aplicación de las políticas de ciberseguridad, ha compilado un documento con toda la legislación española que afecte a la la misma, al objeto de contribuir a mejorar el conocimiento y facilitar la aplicación de una normativa que afecta a una materia tan importante, pero a su vez tan cambiante. Este documento es el Código de Derecho de la Ciberseguridad del 3 de mayo de 2024, donde se ven incluidas las leyes anteriores [52].

2.3.2. Tratados internacionales sobre delitos informáticos

A nivel internacional, destaca el tratado europeo sobre ciberdelincuencia del Convenio de Budapest, que identifica la necesidad de aplicar una política penal común a nivel europeo encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de una legislación común y el fomento de la cooperación internacional para prevenir los actos delictivos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de estos. Todo esto mediante la tipificación de esos actos, la definición de regulaciones y normativas, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y así garantizando el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales y a la protección de datos [53].

Adicionalmente, existen directivas internacionales que indican a los estados miembros protocolos, tipificaciones y recomendaciones comunes, entre las cuales son las principales:

- Directiva 2002/58/CE, de 12 de julio [54].

- Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 marzo 2006 [55].

- Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011 [56].

- Directiva 2013/40/UE [57].

- Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 [58].

También existen algunas otras propuestas y reglamentos como el Reglamento de 2004 del Parlamento Europeo y del Consejo en virtud del cual se crea la Agencia Europea de Seguridad de las Redes y la Información [59].

2.4. Evidencia digital y admisibilidad en juicio

La evidencia digital se define como cualquier dato almacenado o transmitido mediante un ordenador que respalde o refute una teoría sobre cómo ocurrió un delito, o que aborde elementos críticos del delito [60] [61].

La admisibilidad es esta evidencia en procedimientos legales, se basa sin embargo en una serie de criterios, normas y regulaciones específicas, que si no seguimos, comprometerían la evidencia hasta el punto de considerarse inadmisible. Y de nada nos serviría todo el trabajo de investigación realizado si no podemos acreditar su validez ante un tribunal.

En cuanto a los requisitos que tiene que cumplir la investigación forense [62] [63], estos se pueden resumir en:

- Aceptabilidad: El uso de métodos y herramientas cuyo funcionamiento sea conocido.
- Integridad: Las pruebas deben mantener su estado, sin sufrir ninguna alteración. Para el tratamiento se emplean copias del medio, generalmente tres (de respaldo, para la investigación, y copia para parte contraria) que deben mantener los mismos hash.
- Credibilidad: El investigador debe acreditar el adecuado conocimiento de las herramientas, de forma que debe poder explicar la información que generan y los resultados obtenidos de ellas.
- Relación causa-efecto: Si bien no es trabajo del investigador dictaminar culpabilidad, deben poderse explicar los hechos en términos de causa y efecto o acción y consecuencia.
- Carácter repetible: Esto quiere decir que los mismos datos de entrada, deben producir los mismos datos de salida.
- Documentación: Sin excepción, debe documentarse cada paso de la investigación, con descripciones detalladas y exactas, para que no puedan impugnarse pruebas por ambigüedad o negligencia, con especial atención al mantenimiento de la cadena de custodia, donde es importante que el acceso a las pruebas esté regulado por detallados informes probatorios

Estos criterios generales, están regulados de manera específica por los estándares UNE/ISO, donde se definen las líneas de trabajo y criterios que debe seguir el perito forense en la gestión, análisis y preservación de evidencias digitales, asegurando de esta forma la fiabilidad de las investigaciones forenses y la viabilidad de la evidencia.

Estas normas son principalmente las siguientes:

- Norma UNE 71506 - Metodología para el análisis forense de evidencias digitales [64].
- Norma UNE 71505-1 - Sistema de Gestión de Evidencias Electrónicas. Parte 1: Vocabulario y principios generales [65].
- Norma UNE 71505-2 - Sistema de Gestión de Evidencias Electrónicas. Parte 2: Buenas prácticas en la gestión de evidencias electrónicas [66].
- Norma UNE 71505-3 - Sistema de Gestión de Evidencias Electrónicas. Parte 3: Formatos y mecanismos técnicos [67].
- UNE-EN ISO/IEC 27037:2016 - Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas [68].
- UNE-EN ISO/IEC 27042:2016 - Directrices para el análisis y la interpretación de las evidencias electrónicas [69].

Siguiendo estas normas, podremos garantizar la calidad de nuestro trabajo de investigación y un resultado favorable (refiriéndonos con esto a una imagen fiel a la realidad de lo ocurrido) en el caso.

2.5. Cadena de custodia y preservación de evidencia

Por otro lado, para que la evidencia obtenida sea admisible es indispensable garantizar que las evidencias digitales encontradas han sido almacenadas de forma adecuada y sin posibilidad de manipulación, es decir, que se respete la cadena de custodia [70].

Esta se refiere al protocolo meticuloso utilizado para documentar todo el manejo, cronología y procedencia de una prueba a lo largo del proceso judicial, garantizando que la misma no ha sido manipulada o alterada de ninguna forma ante un tribunal, para el cual debemos llevar un protocolo y seguimiento muy estricto.

La viabilidad procesal de la evidencia digital y su calificación como auténtica (no manipulada), íntegra (conservado su contenido original) y confiable (obtenida sin técnicas ilegítimas o fraudulentas) sigue un principio simple: si la prueba no ha sido alterada desde su recolección (que incluye la recuperación policial si la hubiera) hasta su estudio forense, la cadena de custodia habría sido conservada, mientras que, en caso contrario habría sido dañada irreversiblemente.

A nivel técnico, para mantener cadena de custodia y, por tanto, la admisibilidad de la prueba, es necesario realizar diferentes protocolos o técnicas según el caso, siendo la más común a nivel técnico el clonado o copia del medio que la representa, y la obtención de la denominada función hash o huella digital, que se define como un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado. Estas funciones hash son la única garantía explícita que permite certificar la inalterabilidad de la evidencia. Por otro lado, es necesario llevar un registro completo de todas las prácticas que se lleven a cabo sobre la evidencia, y debemos establecer directrices y pautas de control de acceso a la misma, para evitar posibles incidentes [71].

2.6. Responsabilidades legales, éticas, derechos y deberes de los peritos forenses

El perito forense, debe actuar con responsabilidad ética y legal en todos los aspectos de su profesión, asegurando la credibilidad y la calidad de su trabajo en el sistema judicial. Esto implica principalmente [72] [73]:

- Mantener independencia y libertad en sus opiniones y juicios profesionales actuando con objetividad, imparcialidad y veracidad, sin dejarse influenciar por presiones externas como poderes públicos, económicos, de las partes, o de otras índoles, pudiendo rechazar su participación en una investigación cuando no puedan cumplirse estos requisitos.
- Guardar secreto profesional y confidencialidad sobre toda la información a la que tenga acceso en el ejercicio de su labor, ya sea en cuanto a información recibida, evidencia o documentación, conforme a la Ley de Protección de Datos Personales.
- Recibir honorarios por su trabajo profesional, los cuales deben ser acordados de manera justa y conforme a las normativas vigentes.
- Mantenerse actualizado en su campo profesional, incorporando nuevos conocimientos y técnicas relevantes para mejorar su desempeño, pudiendo rechazar aquellos trabajos para los que no se encuentre capacitado.
- Actuar con dignidad, lealtad, integridad y respeto hacia todos los participantes en el proceso judicial, manteniendo una conducta profesional íntegra y honesta, teniendo la obligación de informar de cualquier hecho.
- Ser capaz de acercar los descubrimientos del caso a una audiencia no técnica, de forma que sea clara y comprensible para perfiles no especializados en la materia en la que se realice el peritaje.
- Abstenerse del empleo de formalidades, recursos innecesarios, y de toda gestión puramente dilatoria que entorpezca injustamente el normal desarrollo del procedimiento.
- No aceptar casos de familiares hasta el tercer grado de consanguinidad o afinidad, manteniendo el criterio de objetividad y evitando conflictos de interés con personas de relación estrecha.
- Notificar delitos graves, incluso si estos son cometidos por el cliente.

La credibilidad del perito y su defensa del caso, impacta directamente sobre los resultados obtenidos, ya que si por ejemplo, el investigador no es capaz de justificar las acciones realizadas o explicar plausiblemente la obtención de los datos resultantes, podría tirar por la borda toda la investigación, o en el peor de los casos, comprometerla irreversiblemente [74].

2.7. Jurisdicción y extradición en casos de delitos informáticos

En el caso de los ciberdelitos, en ocasiones no se cuenta con un lugar físico donde poder encuadrar los hechos o al responsable de los mismos. En casos donde la evidencia se encuentra o compone de elementos físicos, no es tan complicado, sin embargo, los delitos cometidos a través de internet suponen un gran reto en la determinación de la jurisdicción y los órganos que se encargarán de la investigación [75].

Se ha de determinar cual se considera el lugar en el que se comete el delito, para lo cual podemos servirnos de tres teorías: la teoría de la actividad (según la cual el delito se entiende cometido en el lugar desde el que se realiza la conducta), la teoría del resultado (por la que el delito se comete en el lugar donde se produce el resultado o impacto del mismo) y la teoría de la ubicuidad o teoría mixta (según la cual el delito se entiende cometido en ambos indiferentemente). Sin embargo, una vez iniciada una investigación por un presunto delito, a excepción de los casos de extradición, no se cederá a otro estado aunque éste lo reclame para enjuiciamiento o condena.

Teniendo en cuenta todo esto, se hace necesaria una gran cooperación internacional para poder resolver el no tan evidente lugar del delito y determinar a quién le compete. En este sentido, es evidente la necesidad de establecer normas claras al respecto, para siquiera empezar a hablar de los acuerdos de extradición en estos delitos de naturaleza transnacional y transfronteriza [76] [77] [78]. Principalmente porque faltan criterios concretos para determinar la competencia en los documentos legales de referencia en el ámbito comunitario: el Convenio de Budapest, la Decisión Marco 2009/948/JAI para la resolución de conflictos de jurisdicción, y el Convenio de Extradición entre Estados miembros. Además, fuera del ámbito comunitario existen problemas con la distribución jerárquica de la competencia, referidos al Acuerdo de Extradición entre UE y EEUU (2003) al que se adhieren también otros países no comunitarios.

Capítulo 3

Metodologías actuales en informática forense

3.1. Fases de un análisis forense

La investigación forense puede dividirse en diferentes etapas. La clasificación más común es la formada por las fases de identificación, recolección, adquisición, preservación, análisis, documentación y presentación de la evidencia, en ese orden (figura 3.1).

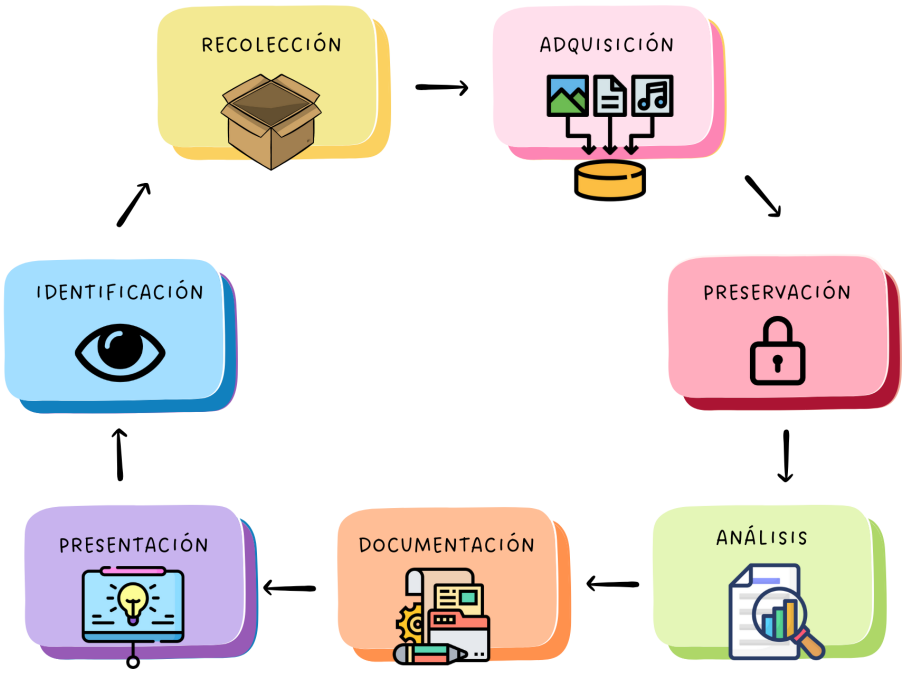


Figura 3.1: Fases del análisis forense [19]

Nuestros objetivos primordiales serán, recuperar la evidencia inalterada, llevar a cabo el análisis per sé, y exponer nuestra reconstrucción de los hechos [61].

3.1.1. Identificación y aseguramiento de la escena

Respecto a cómo debemos trabajar en la escena, donde muchas veces colaboraremos con otros forenses de otras ramas del conocimiento, existen una serie de buenas prácticas que se deben poner en marcha para evitar pérdidas de información y accidentes.

Previa autorización judicial, debe acordonarse y aislarse la escena, de forma que quede protegida de posibles alteraciones. Debemos identificar los objetos extraños o de interés para la investigación, y asegurarnos de no alterar los medios probatorios físicos o digitales en ningún sentido. Documentaremos mediante fotografías de la evidencia todo daño físico apreciable del hardware, marcas de tiempo en pantalla de equipos encendidos y otras características que puedan resultar relevantes. De ser necesario, solicitaremos apoyo de otros profesionales o unidades desplegadas. Una vez estabilizada la escena, comenzaremos con la fase de preservación de la evidencia [79].

3.1.2. Adquisición, recolección y preservación de la evidencia

Lo que debemos tener en cuenta en primer lugar, es recolectar y preservar la evidencia en la escena donde se ha producido el incidente (en estos casos, podríamos estar acompañados de fedatarios públicos, notario o testigos) hasta el final de la investigación.

En general nos va a interesar especialmente cualquier dispositivo de almacenamiento de datos, no suele incluir periféricos como ratón, teclados o monitores, y sí cualquier dispositivo informático o unidad de almacenamiento [63].

A grandes rasgos existen 2 métodos distintos de extracción de evidencias:

- Adquisición física: Este método implica la creación de una copia exacta del contenido del disco almacenado en el equipo, para así, preservar todas las evidencias potenciales, incluidos datos que podrían haber sido eliminados. Es ampliamente utilizado debido a su exhaustividad en la recolección de datos [80] [81].
- Adquisición lógica: Consiste en la copia del sistema de ficheros (directorios, ficheros, volúmenes cifrados, etc.) de un sistema operativo. Es un proceso más ágil que el utilizado en la adquisición física. Es muy útil en escenarios donde no contamos con mucho tiempo para realizar la adquisición o el objeto de encargo tiene que ver con documentos ofimáticos, archivos multimedia, etc.

Para la adquisición de discos duros, podemos usar jaulas diseñadas para disipar cargas electroestáticas y así asegurar que el disco duro permanezca en un entorno seguro. Para el caso de dispositivos móviles debemos prevenir que reciban o transmitan señales durante el análisis forense, se puede colocar en una jaula de Faraday. Estas jaulas bloquean todas las señales inalámbricas (de radiofrecuencia, comunicación con redes celulares, Wi-Fi, Bluetooth, etc). En caso de no disponer de esto último, podemos simplemente poner el teléfono en modo avión.

Por otro lado, dentro de nuestras responsabilidades respecto a la evidencia digital, debemos preservar el estado original de los dispositivos en la medida de lo posible dependiendo de las circunstancias, ¿pero qué implica esto? Implica la no alteración de su estado inicial, por ejemplo, si tenemos que analizar un equipo que se encuentra encendido, debemos dejarlo encendidos. Por el contrario, si encontramos un equipo apagado no debemos encenderlo. En base a este principio existen dos tipos de análisis. [61] [79].

El primer tipo es el dead analysis, análisis de un sistema “muerto”, postmortem, o en frío, que se realiza cuando el dispositivo en cuestión se encuentra apagado o no es un

dispositivo con funciones de encendido o apagado en sí mismo (memorias USB, discos duros externos, CDs, disquetes, etc). Este análisis trata de permitir que podamos analizar los datos contenidos en las evidencias sin la interferencia de procesos en ejecución que los modifiquen. Hay dos formas de realizarlo, crear un clon o imagen del dispositivo [82].

El segundo caso, sería el live analysis, análisis en “vivo” o en caliente, en el cual todos los servicios, procesos y herramientas que estuviesen en ejecución en el primer contacto con el dispositivo siguen funcionando. El sistema modificará continuamente los registros del dispositivo mientras este se esté ejecutando, ya que no habremos apagado el mismo. Es por esto que para usar este método, debemos trabajar con los valores de la máquina en instantes de tiempo concretos, haciéndose mucho más importante y sensible tanto la documentación de cada acción que se realice, cada herramienta que se use y cada proceso que se ejecute, como la cronología no solo del actuar de sujeto activo (si lo hubiera) que se investiga, sino la del propio investigador. Este tipo de análisis es el más arriesgado en cuanto a la contaminación (e incluso destrucción) de evidencia se refiere, ya que la alteración continua de los datos de la máquina puede inutilizar los hallazgos encontrados si no se opera con cautela, pero es muy útil en casos donde no podemos parar todo el sistema, como en el análisis de ataques cibernéticos a empresas e instituciones, que no pueden detener toda su estructura informática para la realización de la investigación, y aunque pudiesen, la cantidad de datos y dispositivos sobre todo en grandes arquitecturas lo haría demasiado complicado [63] [82].

Especialmente en este tipo de análisis, se debe justificar minuciosamente cada acción aplicada y el resultado que produce en la máquina, para que podamos diferenciar correctamente las acciones que constituyen evidencia, de las que han sido necesarias para extraerla.

El análisis de un sistema muerto suele comenzar por el análisis de los soportes de datos ya clonados, información no volátil almacenada en el disco, mientras que el análisis en vivo comienza por el análisis de la información volátil, como procesos en ejecución, conexiones de red, usuarios conectados, archivos abiertos, RAM, etc. Debemos recordar además que por lo general ante un ataque severo donde se sospeche que el atacante pueda tener aún acceso a los sistemas, debemos desconectar inmediatamente el dispositivo de la corriente eléctrica, desconectar el cable de red y deshabilitar la tarjeta Wifi para evitar un mal mayor como la destrucción de evidencias [83].

Particularmente INCIBE [84] nos recomienda aplicar una serie de principios y buenas prácticas (RFC 3227) [74] en la recolección de la evidencia. En cuanto a la preservación de la evidencia, pueden consultarse de organismos como el NIST (National Institute of Standards and Technology) [85].

3.1.3. Análisis y examen de la evidencia

Una vez intervenido todo el material y tomadas las medidas necesarias para asegurar la cadena de custodia comienza el trabajo propiamente dicho del informático forense.

Las herramientas de investigación se han vuelto cada vez más sencillas de usar en los últimos años, sin embargo, es necesario que realicemos una buena interpretación

de los datos que nos proporcionan para poder hacer un uso útil y eficiente de ellas. Para dar con la herramienta o herramientas adecuadas, primero debemos considerar las características del dispositivo que vamos a analizar, para poder enfocarnos en un tipo concreto de análisis. Generalmente, en la mayor parte de los casos podemos clasificar la evidencia según el tipo de dispositivo para que encuadre en una de las siguientes categorías de análisis forense [63] [82]:

- Soportes de datos.
- Sistemas Microsoft Windows.
- Sistemas Linux/Unix.
- Dispositivos móviles.
- Redes y sistemas distribuidos.
- Dispositivos IoT

Inicialmente, podemos definir una lista aproximada de los elementos de interés en el análisis forense, que con cada caso específico variarán en modo de extracción, herramientas utilizadas, metodología de trabajo, y ubicación de los archivos o elementos relevantes para el análisis. Esta lista es:

- Medio físico.
- Sistema de archivos y archivos del sistema operativo.
- Archivos existentes, temporales, cifrados, comprimidos, abiertos o borrados (imágenes y videos, documentos y archivos de texto, ejecutables).
- Metadatos.
- Registro de eventos (event logs).
- Registro del sistema operativo (hives).
- Memoria volátil (RAM).
- Tráfico, conexiones de red y puertos abiertos.
- Programas o procesos en ejecución o en escucha.
- Aplicaciones y software instalado.
- Actividad del usuario.
- Contraseñas y credenciales.
- Correo electrónico y comunicaciones.
- Navegación web e historial.
- Logs de seguridad.
- Dispositivos conectados y periféricos.
- Datos de geolocalización (GPS).
- Fecha y hora del sistema, último arranque.

Se pueden realizar exclusiones de archivos conocidos comunes en los sistemas operativos siempre y cuando comprobemos su hash, para lo cual tenemos importadas en muchas de las herramientas forenses listas de hash estandarizadas (que nos permitirán no perder tiempo en comprobaciones que no nos ofrecerán resultados) [63].

3.1.4. Documentación, presentación de resultados y testimonio experto

Es crucial comenzar a tomar notas detalladas de todas las actividades realizadas, documentando y fechando cada paso desde la detección hasta el final del análisis forense. Al concluir, se deben presentar dos informes:

El informe ejecutivo va dirigido a audiencias no técnicas. Debe ser claro, conciso y comprensible, destacando los hallazgos más importantes y las conclusiones. Su propósito es proporcionar una visión general del caso y de las evidencias encontradas sin entrar en detalles técnicos. Debe contener al menos [83]:

- Motivos de la intrusión.
- Desarrollo de la intrusión.
- Resultados del análisis.
- Recomendaciones.
- Cronología de la consecución de los hechos.

El informe técnico va destinado a audiencias expertas, como otros forenses digitales o expertos en informática. Debe contener una relación exhaustiva de todas las técnicas y herramientas utilizadas durante la investigación, los procedimientos seguidos, los hallazgos detallados y cualquier análisis realizado. Este informe es fundamental para que se cumpla el criterio de reproducibilidad del análisis que mencionamos anteriormente y para que otros expertos puedan entender y validar los métodos y resultados obtenidos. Debe contener al menos [83]:

- Antecedentes del incidente.
- Recolección de los datos.
- Descripción de la evidencia.
- Entorno del análisis.
- Descripción de las herramientas.
- Análisis de la evidencia.
- Información del sistema analizado.
- Metodología utilizada.
- Descripción de los hallazgos.
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones específicas.
- Referencias.

En estos informes y en nuestra experiencia nos basaremos para presentar los resultados de nuestra investigación y nuestro análisis del caso como expertos.

3.2. Técnicas antiforenses

Las técnicas antiforenses, como podemos intuir de su nombre, son aquellas técnicas o sistemas que dificulten o no permitan la realización del trabajo forense o el acceso a los datos e información necesaria para la misma. A nivel legal, también podemos definirlas como aquellas técnicas que buscan hacer cuestionable la fiabilidad de la evidencia, ya sea por provocar la no obtención de la prueba, o por contaminarla [86] [87].

En función de la intencionalidad con la que se realiza, tenemos dos tipos de técnicas: las provocadas por negligencia y las intencionales.

Dentro de las no intencionales tenemos la mala praxis, la contaminación por falta de conocimientos o por accidentes provocados por la inexperiencia del perito. Dentro de las intencionales tenemos aquellas que imposibilitan el acceso a la información, aquellas que consisten en una eliminación o destrucción de la misma y las que intentan alterar

las herramientas para que no recuperen la información o recuperen información errónea [88]. Algunas de estas técnicas se enumeran a continuación [89]:

- Ocultación de información o dispositivos para evitar que los procedimientos obtengan información legible y auditable mediante diversas técnicas (cifrado, ocultación de memoria, manipulación del sistema de archivos, esteganografía, cifrado de discos lógicos, virtuales o por hardware, cifrado de sistemas de archivos, cifrado de protocolos de comunicación uso de empaquetadores de programas, ocultación en espacios inaccesibles a las herramientas, etc.).
- Limpieza o destrucción de datos o dispositivos, que puede ser muy elaborada o muy sencilla. Podemos simplemente realizar un borrado de metadatos, discos e historiales con técnicas de sanitización lógica, analógica, digital o criptográfica (clearing, wiping, purging o degaussing) o incluso destruir el dispositivo o su contenido físicamente desmagnetizando los discos, dañándolos, etc.
- Ataques contra las herramientas forenses o que modifican o evitan el funcionamiento normal del sistema de tal manera que no se registra la información (syscall proxying, compiladores/ensambladores en memoria, inyección de código en memoria, manipulación del kernel, uso de live distros o máquinas virtuales, etc.)

3.3. Cadena de custodia en informática forense

Antes hablamos de los aspectos legales e importancia de la cadena de custodia. Ahora, analizaremos en qué consiste a nivel práctico. Como ya dijimos, la cadena de custodia contribuye a garantizar la integridad y autenticidad de la evidencia digital. Como elemento de la investigación, está compuesta por una serie de registros documentales de control de la evidencia. Estos registros que nos permiten llevar el seguimiento de la misma son [70]:

- Los que componen los datos específicos de la evidencia en el momento inicial, como el identificador del caso o identificadores físicos que pueda tener (marca, modelo, número de serie, MAC. . .), la descripción detallada de la misma y los objetos que la componen, lugar, fecha y hora donde se encontró la evidencia, estado de la misma, características adicionales, lugar y condiciones de almacenamiento, etc.
- Los registros de control [90] , donde se establecen el acceso o posesión de las mismas en todo momento, el uso que se les ha dado, si han sido intervenidas y con qué herramientas, cambios en las mismas, etc, todo documentado con fecha y hora exactas. Existen documentos o formularios estándar para estos procedimientos. Estos no pueden prescindir de información como la fecha y hora de cada transferencia, el emisor y el receptor de la misma y el motivo por el cual se solicita su acceso a la misma, pero sí pueden ampliarla ya sea en el mismo documento o mediante otros adicionales.

Esta información debe ir siempre con la evidencia, y hacerse constar en el llamado formulario de adquisición de evidencias, que se compone de todos los elementos anteriormente mencionados, y nos servirá en los tribunales para demostrar que la cadena de custodia de la evidencia ha sido correctamente gestionada y no se ha roto.

Capítulo 4

Estudio y análisis forense de un caso práctico

4.1. Introducción

Este caso práctico se centra en el análisis forense de un equipo que ha sufrido un ciberataque por ransomware.

¿Qué es el ransomware? Se trata de un ciberataque ampliamente utilizado por los actores maliciosos, cuyo objetivo es conseguir información (datos personales, confidenciales, bancarios, etc.) tanto de empresas como de usuarios víctima.

¿Cómo lo llevan a cabo? Una vez que han conseguido acceso al equipo víctima y como consecuencia a la información almacenada en el disco, proceden a cifrar los archivos de la víctima y posteriormente solicitan un rescate utilizando técnicas de extorsión (amenazan con publicar la información sensible de sus víctimas en caso de que no se realice el pago que demandan).

En este caso la tarea que nos ocupa como analistas informáticos profesionales es identificar el tipo de ransomware que ha afectado al equipo y averiguar lo ocurrido en el sistema para poder generar una cronología del cómo, quién y cuándo se ha producido el ciberataque. La investigación que se va a realizar está basada en la simulación de un escenario real en el que se ve comprometido el equipo de un empleado de una corporación.

Acerca del incidente sufrido en el ordenador del empleado, la empresa nos facilita la siguiente información:

- Nos indican que el incidente se ha producido entre el 24 y el 26 de abril de 2023.
- El empleado cuyo equipo ha sufrido el ciberataque, iba a ser despedido en unos días acusado de mala praxis en el desarrollo de sus tareas.
- Se tienen sospechas de que además del incidente sufrido en el equipo, el empleado haya podido obtener información confidencial almacenada en el mismo.
- El departamento de TI de dicha empresa, mantiene que el sistema se encontraba debidamente actualizado en el momento de los hechos y no tienen una idea previa de lo que ha podido ocasionar la infección por parte del ciberataque.

4.2. Metodología e investigación forense

La metodología empleada en esta investigación se basa en el análisis exhaustivo de los artefactos del sistema para identificar, comprender y documentar la secuencia de eventos ocurridos en el dispositivo y la naturaleza de la infección por ransomware, mediante una serie de herramientas de distinta índole.

4.2.1. Identificación, aseguramiento, adquisición y preservación de evidencias

Siguiendo las normativas y regulaciones necesarias que hemos mencionado anteriormente, se ha creado una imagen forense del equipo infectado de la víctima con la que trabajaremos durante todo el proceso de análisis.

Sin embargo, dado que se nos ha proporcionado la imagen en formato comprimido para nuestra investigación, las fases de identificación, recolección y preservación ya se habían llevado a cabo, en su lugar, para ilustrar el proceso, realizaremos una demostración del procedimiento de adquisición de imágenes forenses mediante la herramienta dd. Para llevar a cabo la demostración práctica, se utilizará una unidad de almacenamiento extraíble (memoria USB).

La herramienta dd (figura 4.1), haciendo uso de la consola de Windows, nos permite realizar la adquisición física de un dispositivo extraíble como una memoria USB, tarjeta SD, tarjeta PCMCIA, etc. Para identificar el dispositivo conectado al equipo, debemos conocer la etiqueta asignada del volumen del que queramos crear la imagen (figura 4.2).

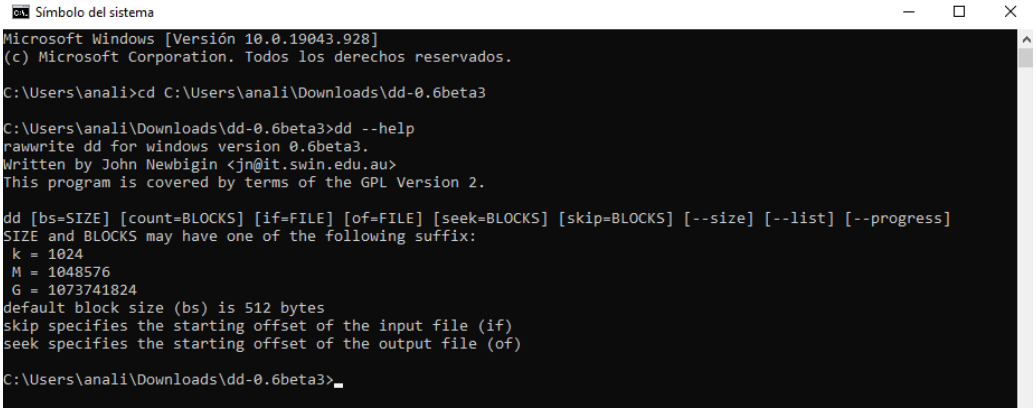


Figura 4.1: Funcionamiento de dd.

Figura 4.2: Identificación de unidad.

Nos permitirá seleccionar (figura 4.3) la entrada mediante if (input file) donde debemos indicarle el punto de montaje del dispositivo extraíble conectado y la salida of (output file) para indicar donde queremos dejar el fichero resultante de la adquisición (la ruta que nosotros seleccionemos).

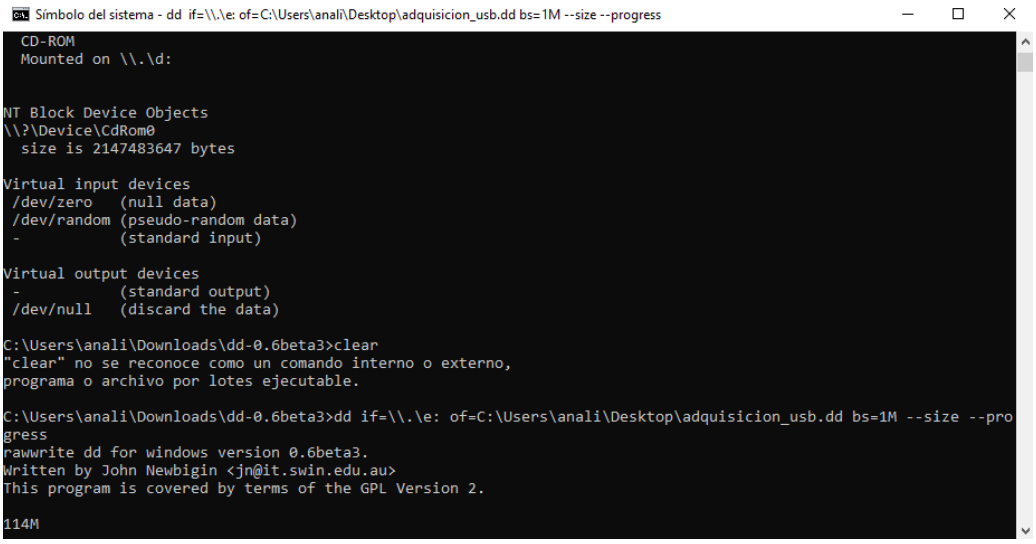


Figura 4.3: Ejecución de dd.

En este caso, se han seleccionado alguno de los parámetros más importantes de la herramienta como `--bs` (para indicar el tamaño de la tasa de transferencia del fichero, en nuestro caso 1MB), `--size` que nos permite visualizar por pantalla el tamaño de el fichero resultante en tiempo real y `--progress` que nos va a permitir visualizar el progreso (figura 4.4) de los bytes transmitidos.

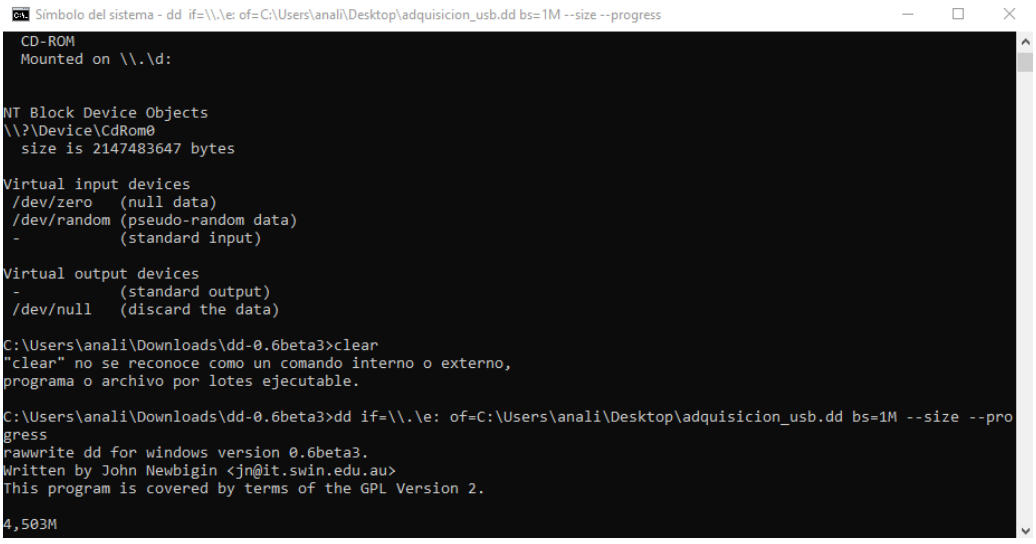


Figura 4.4: Progreso de la adquisición con dd.

La herramienta dd no aplica tasa de compresión a la imagen, se traduce en que nuestro fichero imagen resultante tendrá el mismo tamaño que el dispositivo USB original (figura 4.5) en este caso, su tamaño es de 32 GB.

Figura 4.5: Resultado final de la adquisición con dd.

En cuanto a la adquisición de la memoria de un dispositivo móvil (figura 4.6), MOBILedit Forensic Pro es una herramienta comercial para la extracción de información almacenada en la memoria, también es adecuada para adquirir información almacenada en relojes inteligentes y datos en la nube. Utiliza tanto la adquisición de datos física como lógica, y permite análisis de aplicaciones, recuperación de datos eliminados, generación de informes, procesamiento concurrente y una interfaz fácil de usar.

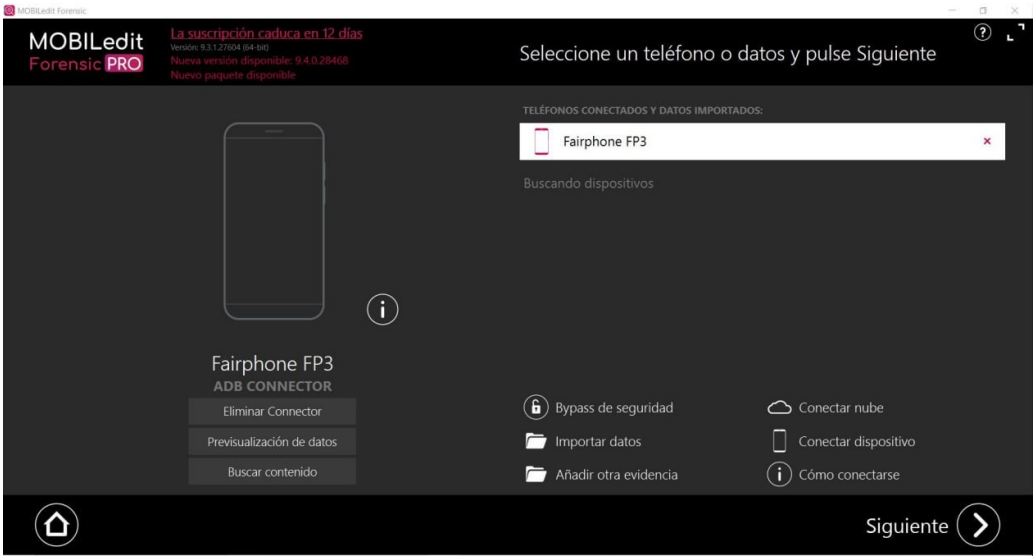


Figura 4.6: Detección y selección del dispositivo móvil con MOBILedit.

Vamos a realizar un proceso de extracción lógica de los datos almacenados en un dispositivo móvil (figura 4.7). Inicialmente, debemos conectar mediante cable USB tipo C el dispositivo a nuestra estación forense donde está instalada la herramienta comercial. Además, debemos tener instalada en nuestra estación forense la herramienta ADB para poder comunicarnos con el dispositivo (modelo cliente- servidor) y acceder al mismo. En el dispositivo móvil, debe estar habilitado el modo desarrollador y tener activa la depuración mediante USB. El procedimiento que llevamos a cabo para realizar la extracción, se muestra a través de las ilustraciones incluidas en esta sección.

Las opciones de extracción que ofrece MOBILedit incluyen la extracción de contenido completo, análisis de aplicaciones, datos eliminados, información y características del dispositivo, etc. (figura 4.8).

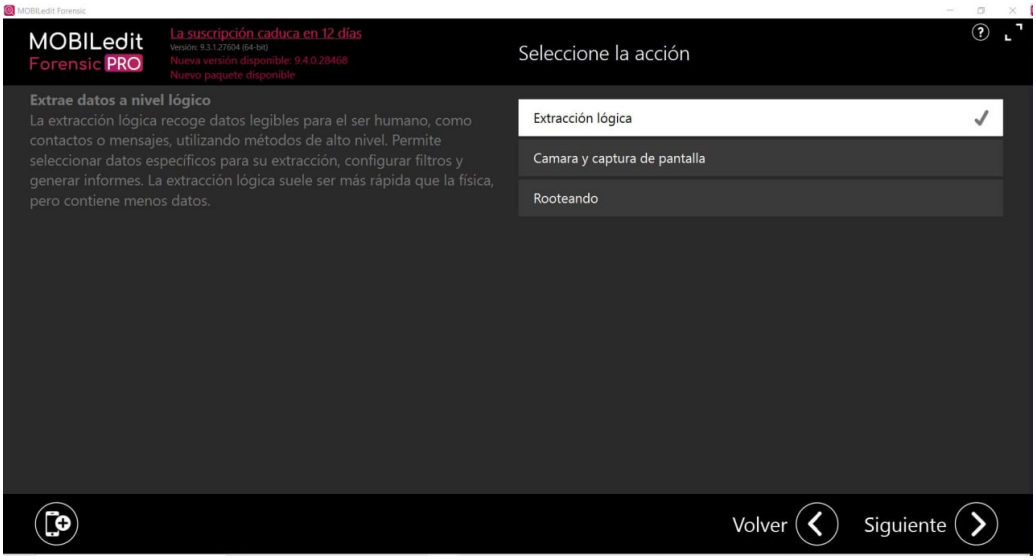


Figura 4.7: Selección del tipo de acción a realizar por MOBILedit.

Figura 4.8: Selección del tipo de extracción a realizar por MOBILedit.

Seleccionaremos el contenido y la ubicación donde realizaremos el volcado de la extracción, así como el formato de salida, y la herramienta comenzará el proceso de análisis (figura 4.9).

Cuando la herramienta finalice (figura 4.10), en función del tipo de salida que hayamos indicado, obtendremos directamente la extracción de los datos en formato de copia o informe forense (HTML, PDF o Excel), facilitando mucho el trabajo de peritaje.

Sin embargo, pese a que este tipo de suites nos permiten llevar a cabo un trabajo de análisis de una manera sencilla, no debemos olvidar que es crucial entender sus acciones y funcionamiento interno. Conocer cómo funciona el proceso de extracción de datos, la forma en que se tratan y almacenan, y las limitaciones inherentes a cada herramienta es fundamental para garantizar la admisibilidad de la evidencia recolectada.

Figura 4.9: Comienzo de la extracción a realizar por MOBILedit.

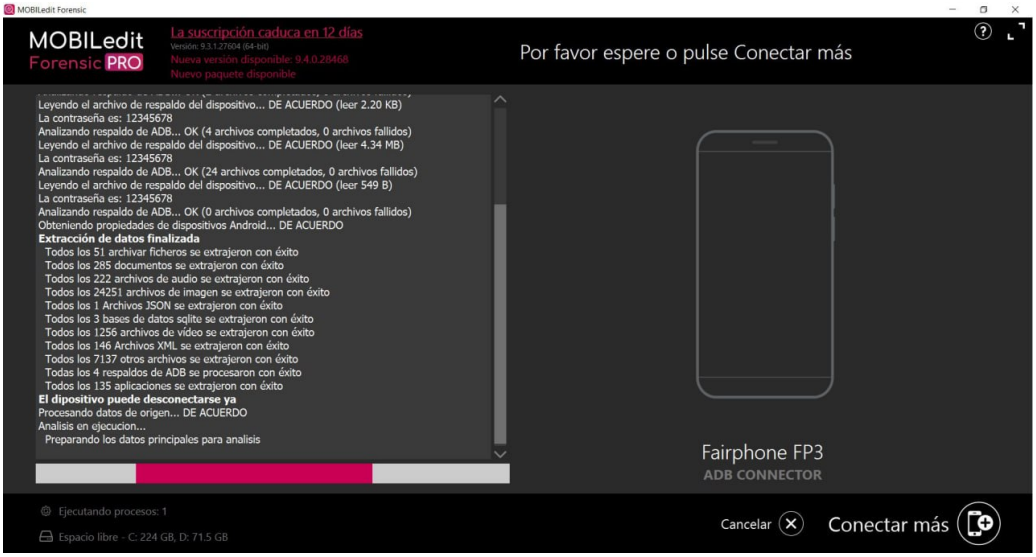


Figura 4.10: Finalización de la extracción a realizar por MOBILedit.

4.2.2. Análisis y examen de la evidencia digital

¿Qué es un ransomware? Un ransomware es un tipo de malware cuyo modus operandi consiste en bloquear o ”secuestrar” el acceso a los archivos o dispositivos para luego exigir un rescate por ellos.

¿Cómo analizamos un ransomware? Lo primero que debemos hacer es utilizar la herramienta forense FTK Imager y añadir la imagen forense en formato EnCase que nos han facilitado del disco infectado.

Una vez añadida la imagen, visualizamos las diferentes particiones con las que cuenta el disco, nuestro principal objetivo en este punto de la investigación es navegar por los diferentes directorios para acceder a la carpeta del perfil de usuario, (nombre de usuario ficticio usado en este análisis: Juanito) y analizar su actividad.

Normalmente cuando un equipo sufre un ataque por ransomware se suele hallar la

nota de rescate en el escritorio del perfil del usuario puesto que los actores maliciosos tienen como objetivo que el usuario víctima pueda visualizar la nota de rescate de manera inmediata. El escritorio del usuario suele ser un objetivo accesible.

En nuestro caso, hemos hallado la nota de rescate en el escritorio del usuario Juanito cuya ruta es `C:\Users\Juanito\Desktop` (figura 4.11), observamos que existen una serie de archivos interesantes: unos ficheros cifrados con extensión .deria, y ficheros .html. Debemos comprobar si esta nota de rescate corresponde o no a algún ransomware relacionado con la extensión .deria.

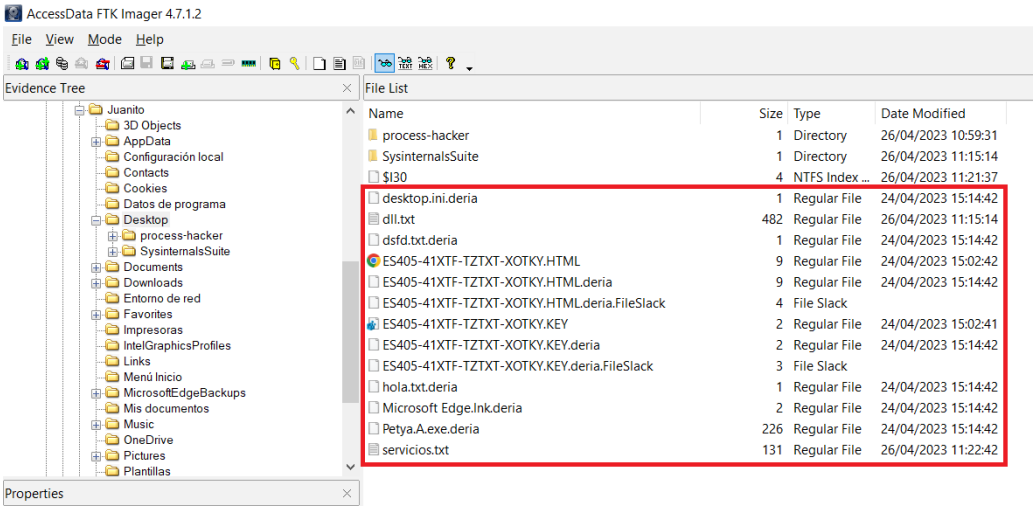


Figura 4.11: Elementos del escritorio del usuario principal.

La nota de rescate (figura 4.12) se encuentra en un fichero HTML denominado `ES405-41XTF-TZTXT-XOTKY.html`. Aparece en ruso, lo que nos hace sospechar que los actores maliciosos tengan algo que ver con esta localización.

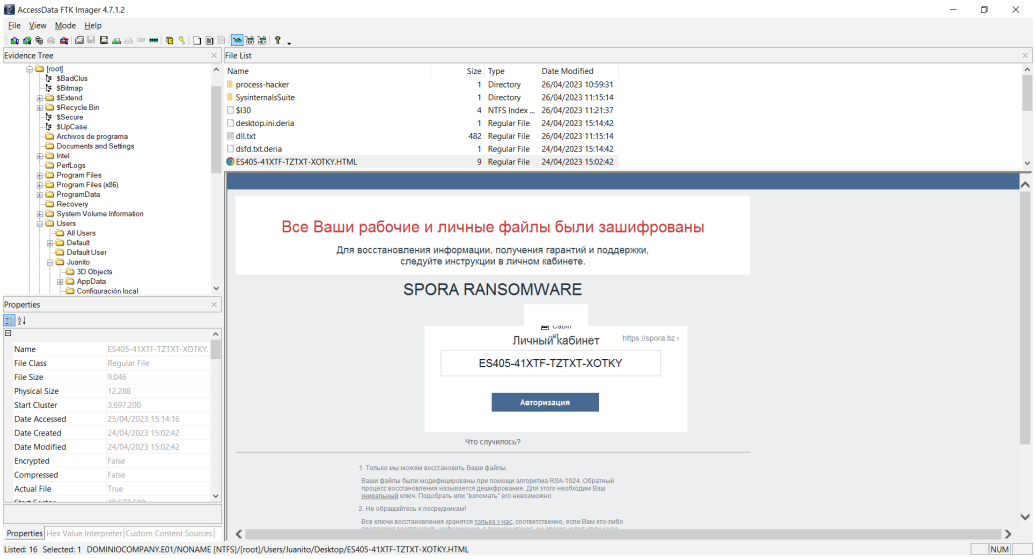


Figura 4.12: Nota de rescate.

Nuestro siguiente paso será determinar a qué familia pertenece este ransomware, para ello, exportamos la nota de rescate `ES405-41XTF-TZTXT-XOTKY.html`.

¿Cómo identificamos qué ransomware nos ha infectado?

Para obtener más información sobre este tipo de ransomware podemos visitar las webs: `www.nomoreransom.org`, `www.virustotal.com` o `id-ransomware.malwarehunterteam.com`, donde nos indican que debemos seleccionar el fichero correspondiente a la nota de rescate o una muestra del archivo cifrado por el ransomware. En base a buenas prácticas se debe facilitar a la plataforma la nota de rescate para no dejar rastro de nuestra actividad puesto que el ataque puede seguir activo y es preferible llevar a cabo esta metolodología para no dar pistas a los actores maliciosos de que estamos investigando.

Para hallar información más precisa sobre esta familia de malware,hemos añadido la nota de rescate en el siguiente sitio web: `https://id-ransomware.malwarehunterteam.com/index.php?lang=es_ES` (figura 4.13)

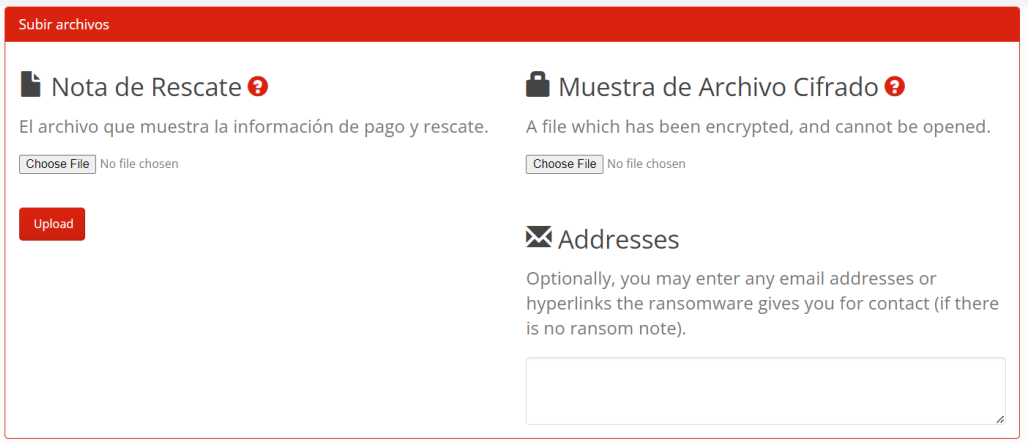


Figura 4.13: Opciones e interfaz de ID-Ransomware.

Una vez finalizado el análisis de la misma, nos arroja la siguiente información (figura 4.14):

Se trata del ransomware Spora y nos indica que, actualmente, no existe un decrypter que nos permita descifrar los ficheros de Juanito y una url donde podemos obtener más información: https://www.emsisoft.com/en/blog/25772/from-darknet-with-love-meet-spora-ransomware.

Se obtiene un mayor detalle sobre el tipo de muestra de ransomware al que nos enfrentamos:

"Spora es un ransomware sofisticado escrito en C que se destaca por su profesionalidad en la implementación y presentación. No renombra los archivos cifrados, sino que deja una nota de rescate en HTML y un archivo .KEY, ambos en ruso. Spora se propaga principalmente a través de correos electrónicos falsos de facturas de 1C, un software contable popular en Rusia. Utiliza una combinación de cifrado RSA y AES, lo que hace imposible recuperar los archivos sin la clave privada del autor del malware. Además, ofrece diferentes paquetes de rescate y permite comunicación directa con los atacantes."

Figura 4.14: Identificación con ID-Ransomware.

¿De qué tipo de ransomware se trata?

En nuestro análisis, comprobamos que Juanito es usuario administrador del sistema, y que el resto de usuarios han sido creados por el sistema por defecto, por lo que es probable que la amenaza se encuentre en los directorios de este usuario.

Continuamos con nuestra investigación, nuestro siguiente objetivo es hallar la localización del fichero binario `.exe` causante de la infección. Lo hallamos en la ruta causante de la infección. Lo hallamos en la ruta C:\Users\Juanito\AppData\Roaming, que almacena un directorio llamado “Zumi” (figura 4.15) y que dentro contiene un ejecutable o binario denominado “paed.exe” 4.16). Ambos fueron creados el 24 de abril de 2023, coincidiendo con las fechas en las que nos comentan que se produjo el incidente.

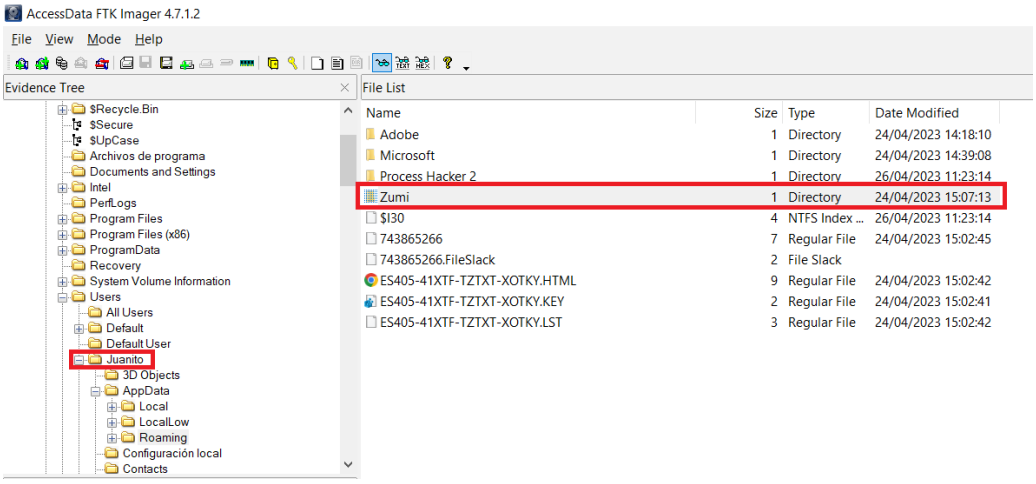


Figura 4.15: Ubicación de la carpeta ’Zumi’.

Exportamos el fichero “paed.exe”. Para evitar que el antivirus elimine el archivo binario, desactivamos la protección en tiempo real de Windows Defender en nuestra estación de trabajo forense, posteriormente, para analizar el ejecutable, usaremos una máquina virtual como precaución para eliminar el posible riesgo de cifrado de nuestro ordenador

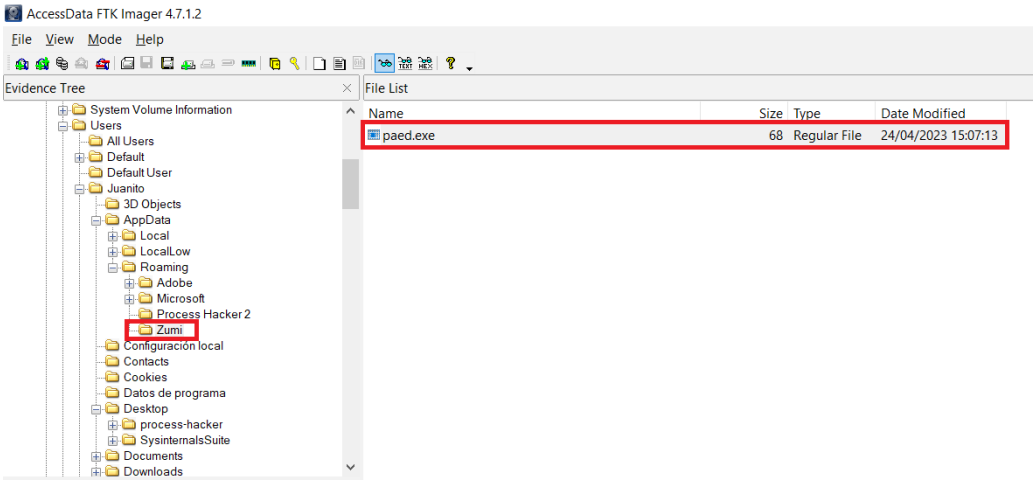


Figura 4.16: Ubicación del archivo paed.exe.

de trabajo en caso de que este fichero se ejecute por un descuido. En primer lugar, debemos comprobar la información en formato hexadecimal de las cabeceras del fichero, para ello, haremos uso de la herramienta de edición hexadecimal HxD.

En nuestro análisis, observamos que este ejecutable muestra un código ASCII denominado “MZ”, y contiene como cabecera 4D 5A 90 00 (figura 4.17), por lo que podemos distinguir que se trata de un ransomware autoejecutable, esto nos indica que no necesita comunicarse con un servidor de comando y control o un agente externo que envíe señales para infectar a la máquina.

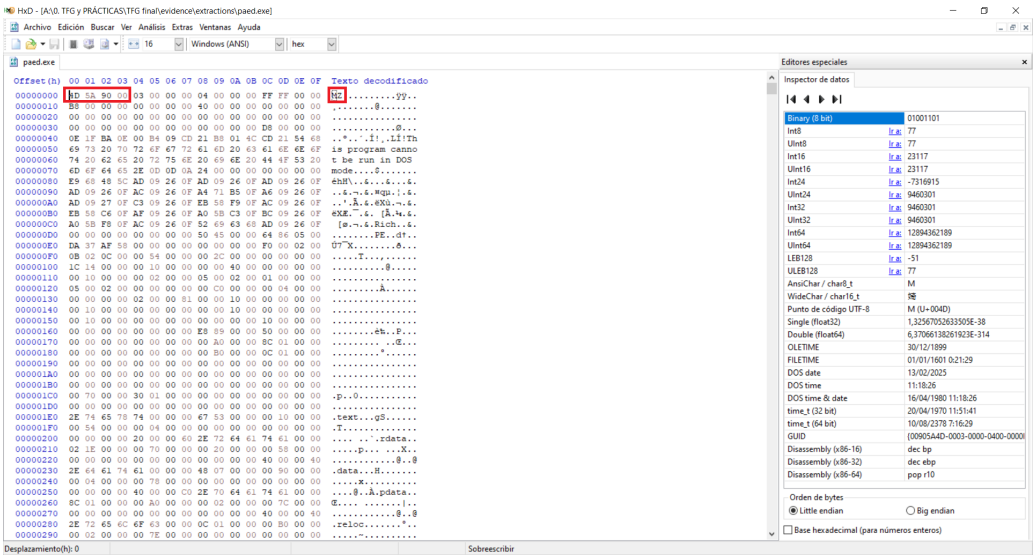


Figura 4.17: Cabeceras del ejecutable paed.exe.

El siguiente paso es averiguar cómo ha llegado ese malware al equipo víctima y en qué momento se autoejecutó por si sólo, podría tratarse de una infección provocada por la visita a un sitio web determinado o debido a una descarga por parte del usuario.

Muchos ransomware cifran los archivos del usuario impidiendo el acceso. Estos ransomware suelen modificar la extensión de los archivos cifrados, agregando una nueva extensión que no estaba presente antes del ataque. Este cambio es un indicador de que los archivos pueden haber sido comprometidos, por lo tanto, es importante revisar las

extensiones de los archivos para detectar cualquier información sospechosa o desconocida que indique que los archivos han sido cifrados por un ransomware.

Si revisamos la información obtenida sobre este ransomware, llama la atención que este tipo de malware no agrega extensión a los ficheros, pero, por el contrario, hemos visualizado los ficheros almacenados en el escritorio del usuario y cuentan con una extension denominada “.deria”.

En mayor detalle, existe un archivo llamado `dsfd.txt.deria` (figura 4.18), se trata de fichero de texto cifrado, analizando las propiedades del fichero, fue cifrado a fecha 24 de abril a las 15:14h.

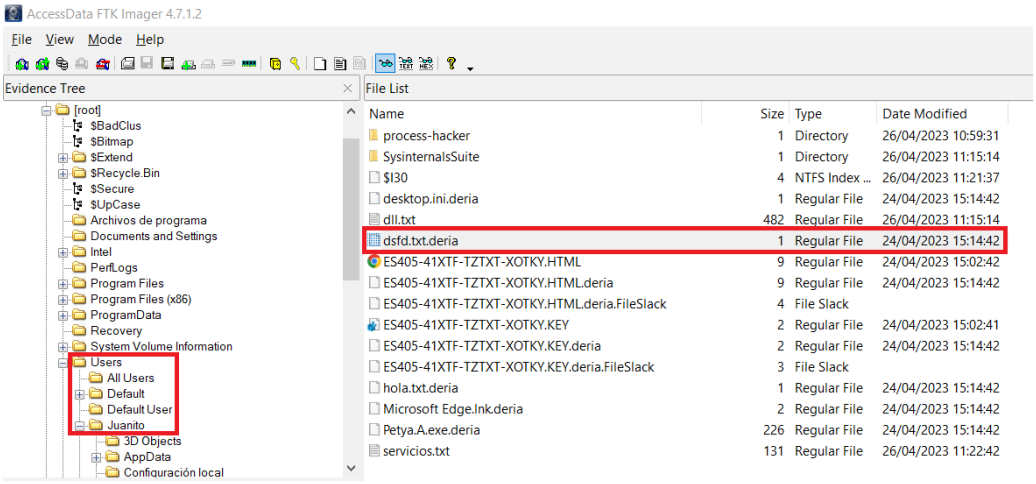


Figura 4.18: Archivo cifrado con extensión .deria.

En cambio, el binario previamente analizado, paed.exe. además de no agregar extensión a los ficheros que cifra, fue creado en el equipo el 24 de abril a las 15:07h. Por ello, debemos investigar qué ocurrió en el equipo el día 24 de abril en el período comprendido entre las 15:07h y las 15:14h.

Podemos realizar una primera hipótesis, que afirma que el equipo ha sido infectado por dos muestras de ransomware de diferente familia, donde el binario paed.exe pudo ser el ransomware causante de la primera infección, ya que su fecha de ejecución es anterior a la fecha del cifrado de los archivos con la extensión .deria.

Para obtener evidencias basadas en nuestras sospechas, debemos acceder a la información almacenada en un artefacto de sistema denominado $MFT (Master File Table), una tabla maestra de ficheros que funciona como una base de datos utilizada por el sistema de ficheros de Windows (NFTS) que registra información sobre cada archivo y directorio almacenado en el disco. Estos registros contienen atributos importantes que le dicen al sistema operativo cómo manejar cada archivo o directorio. Por ejemplo, incluyen detalles como el tipo de archivo, su tamaño, su fecha de creación, de su última modificación, etc.

Debemos consultar la fecha de creación original de los ficheros y su fecha de modificación una vez que se ejecutó el binario paed.exe.

Para acceder a su contenido, debemos exportar el artefacto forense $MFT que se encuentra en la raíz del sistema C:\que almacena dicha información.

Dicho artefacto, una vez exportado mediante FTK Imager, debemos analizarlo, para ello, usaremos la herramienta forense MFTECmd.exe (que cuenta con versión gráfica, pero ésta, consume más recursos del sistema, por ejemplo, mayor cantidad de RAM).

Para realizar el volcado de la información mediante esta herramienta, utilizaremos el siguiente comando haciendo uso de nuestra consola de Windows:

```
MFTECmd.exe -f "C:\Input\$MFT" --csv "C:\Output\MFT.csv"
```

Donde el parámetro -f hace referencia a la ruta donde está almacenado el fichero $MFT extraído, mediante `-- csv` se indica en que formato queremos obtener la información y, por último, el directorio de salida donde se almacenará el resultado dicho formato.

Una vez obtenido el fichero de salida (figura 4.19), debemos acceder a su contenido y centrar nuestra investigación en las columnas que contienen los siguientes parámetros: Parent Path, que nos indica la ruta del sistema donde se encuentran los ficheros, y File-Name, que nos indica el nombre de los ficheros.

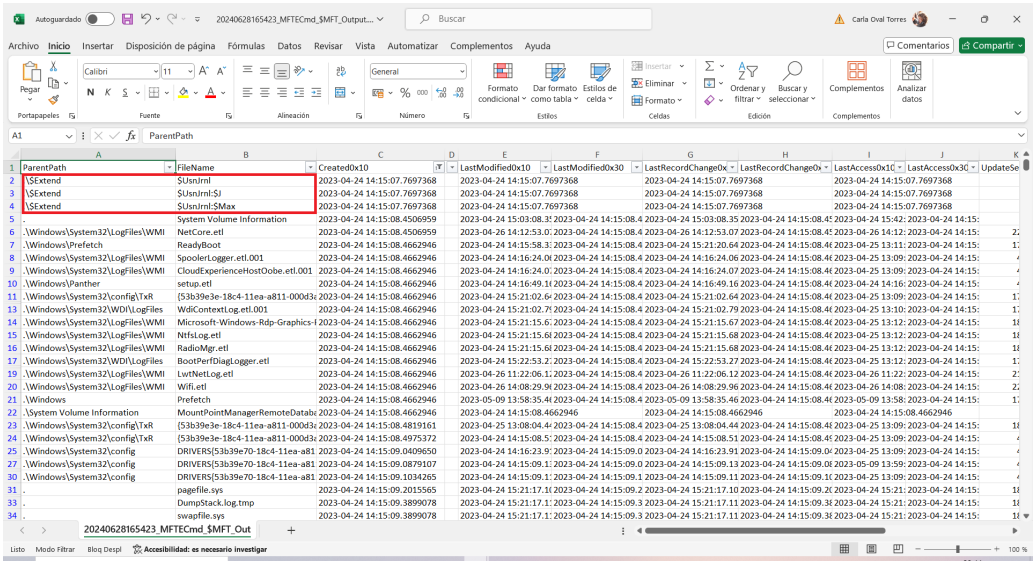


Figura 4.19: Fichero CSV resultante de MFTECmd.exe.

Con respecto a las fechas de modificación y creación de los ficheros, contamos con dos identificadores: el primer tipo es 0x10, que hace referencia al `$FILE_NAME`, y el segundo tipo es el 0x30 que hace referencia a `$STANDARD_INFO`, cuyas marcas de tiempo pueden estar sujetas a modificaciones (de hecho, existe un ataque que es el *timestomp*, que consiste en su manipulación).

Estas marcas de tiempo pueden ser recogidas mediante el acrónimo MAC(b) [91] que reflejan los metadatos (información que caracteriza un dato) de marcas de tiempo, que indican cuándo un archivo fue modificado, accedido, cambiado y creado. Esta información se almacena en los dos atributos que mencionamos anteriormente: `$STANDARD_INFO` y

$FILE_NAME. Conocer su significado en cuanto a marcas de tiempo es imprescindible para los analistas forenses puesto que facilita rastrear actividades de archivos y detectar anomalías, ya que las diferencias en cuanto a marcas de tiempo entre ellos, puede implicar que los ficheros o directorios han podido ser manipulados.

Nos vamos a la ruta C:\$Extend (figura 4.19) , donde encontraremos el archivo $UsnJrnl, que tiene tamaño cero, pero si hacemos click sobre él, nos aparecerán en su interior tres archivos. De estos, exportaremos $J. Además, exportaremos también $LogFile de C:\.

Estos artefactos nos serán de utilidad en nuestro análisis, ya que su propósito es el siguiente:

- $UsnJrnl:$J: Es un artefacto perteneciente a una característica utilizada para registrar cambios detallados en archivos y directorios, útil para el análisis forense y seguimiento de actividades en el sistema. Mantiene un historial detallado de todas las modificaciones, adiciones y eliminaciones de archivos en el sistema.
- $LogFile: Contiene un registro de transacciones del sistema de archivos NTFS, crucial para la recuperación y reconstrucción de datos en análisis forenses y para la integridad del sistema de archivos.

Vamos a proceder al análisis de estos archivos utilizando NTFS Log Tracker. Esta es una herramienta utilizada para analizar y rastrear los registros (logs) del sistema de archivos NTFS (New Technology File System). Esta herramienta permite examinar eventos detallados relacionados con el acceso, modificación, eliminación de archivos y directorios dentro de un sistema NTFS (sistema de archivos estándar para las versiones modernas de Windows).

Una vez ejecutamos la herramienta (figura 4.20), seleccionamos los artefactos que estamos interesados en analizar y hacemos clic en la opción "Parse"para iniciar el análisis. Es fundamental que especifiquemos el formato en cuanto a marcas de tiempo en el que queremos visualizar el resultado, tomaremos como referencia UTC+00:00, dado que es el estándar empleado por la mayoría de las herramientas de análisis.

Una vez ha terminado, utilizaremos el filtro para realizar búsquedas con resultados coincidentes con el nombre del binario paed.exe (figura 4.21).
En la pestaña del programa ”$UsnJrnl:$J”, podemos observar que la fecha de creación del archivo paed.exe coincide con la fecha reflejada por la herramienta FTK Imager 15:07:13h (figura 4.22).

En la pestaña $LogFile, vemos sin embargo que la marca de tiempo de ejecución en el Prefetch es de las 15:07:13 h, (luego se realiza una copia, y en descargas hay otro binario de Spora pero ninguno ha sido el que ha infectado la máquina).

En el excel filtrado y ordenado que tenemos de la herramienta MFTECmd, si filtramos por el FileName paed.exe, nos saldrán una serie de líneas con los archivos paed.exe, PAED.EXE-15DB0E8A.pf, paed.PNG.lnk y paed.exe.dmp.lnk (figura 4.22) donde podemos observar que la fecha y hora, coincide con la del archivo de infección y la del Prefetch.

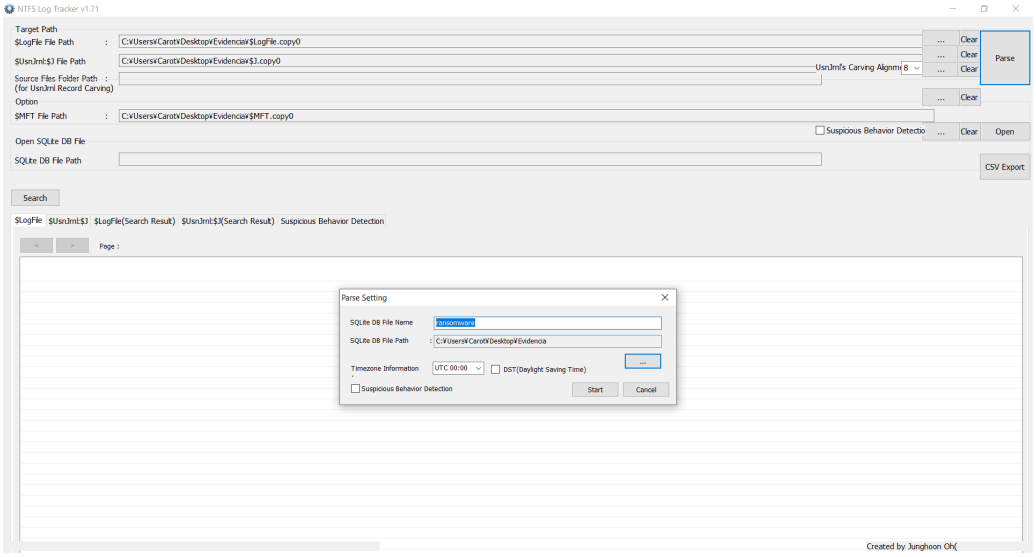


Figura 4.20: Análisis de artefactos con NTFS Log Tracker.

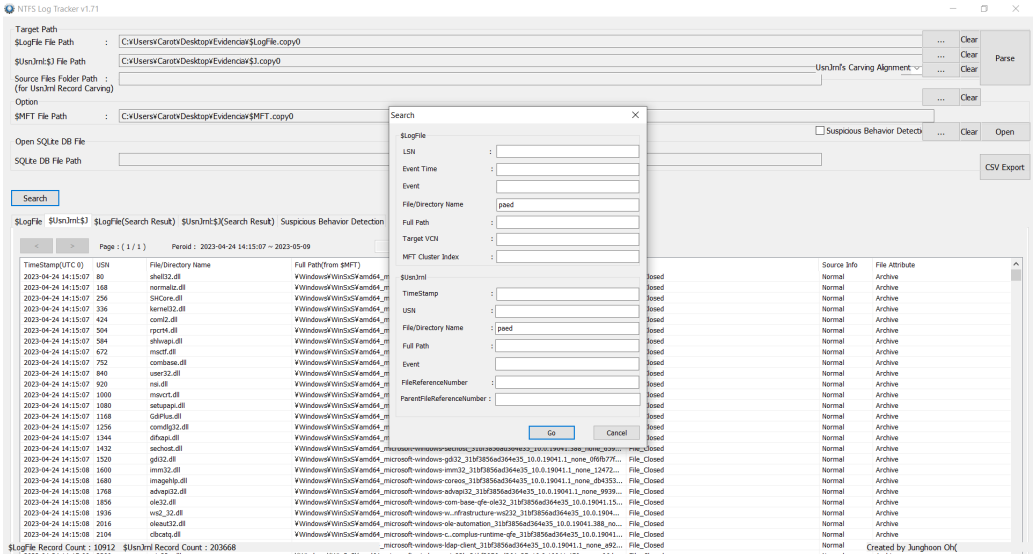


Figura 4.21: Filtrado de artefactos con NTFS Log Tracker.

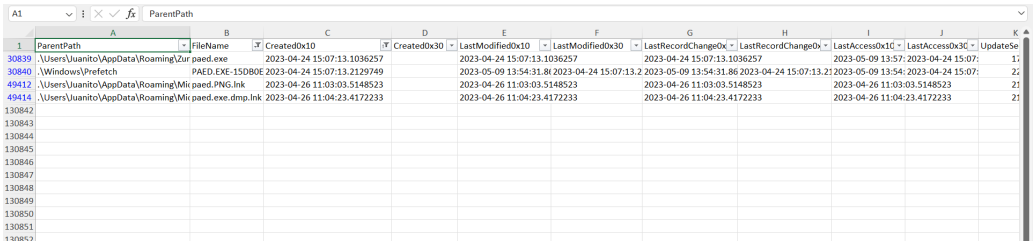


Figura 4.22: Ficheros relacionados con paed.exe.

Este otro artefacto del sistema denominado Prefetch, almacena información con respecto a la fecha y hora de ejecución de una aplicación, un fichero o un software. En este caso, la ejecución del ransomware paed.exe se produjo unos segundos después de su fecha de creación, además de otros intentos de infección posteriores a la infección del equipo mediante el ransomware derialock.exe en fechas comprendidas entre el 26 de abril y el 9 de mayo (figura 4.23).

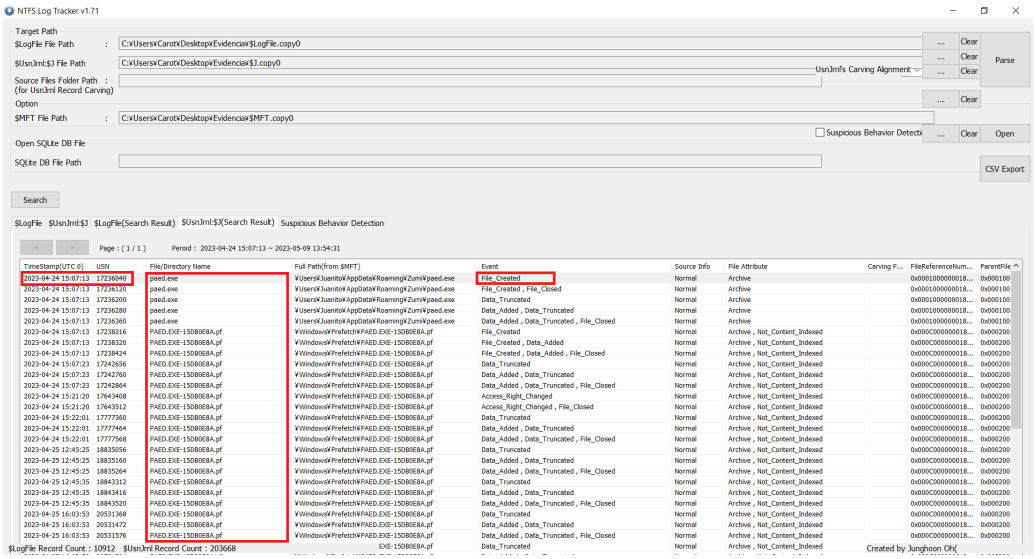


Figura 4.23: Filtrado de artefactos con NTFS Log Tracker.

Para el ransomware Spora, al tratarse de un artefacto malware autoejecutable, las marcas de tiempo entre su fecha de creación y ejecución, coinciden.

¿Cuánto tiempo ha tardado el Ransomware en infectar el sistema?

Si eliminamos los filtros y consultamos las propiedades de un fichero que haya sido infectado, se puede observar la progresión de la infección. Por un lado, Spora,a través de su binario paed.exe cifra el fichero hola.txt a las 15:07:13h, provocando que el usuario no pueda abrir el fichero y posteriormente, se produce un segundo cifrado del mismo fichero que añade la extensión al fichero hola.txt.deria a las 15:14:32h (figura 4.24).

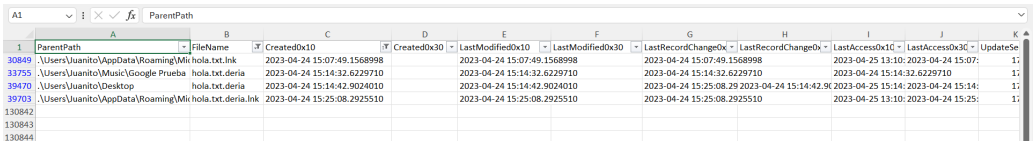


Figura 4.24: Progresión de la infección y el cifrado de ficheros.

¿Hay más de una infección activa en el equipo?

En este punto, nos interesa hallar todas las evidencias del sistema que confirmen la fecha y hora de la infección causada por Spora y qué ocurrió en momentos previos a su ejecución. Para ello, usaremos WinPrefetchView para analizar el contenido de la carpeta Prefetch que se encuentra en la ruta C:\Windows\Prefetch (figura 4.25).

Analizamos los artefactos que se han podido ejecutar antes que el ransomware Spora (PAED.EXE), pero no hallamos nada sospechoso. Por ello, nos centramos en analizar las ejecuciones de aplicaciones y procesos que se han producido después de la primera infección.

Se obtienen evidencias de la ejecución del ransomware DERIALOCK.EXE, se ejecutó ese mismo día a las 15:22h, lo que nos confirma, la causa de la segunda infección y del

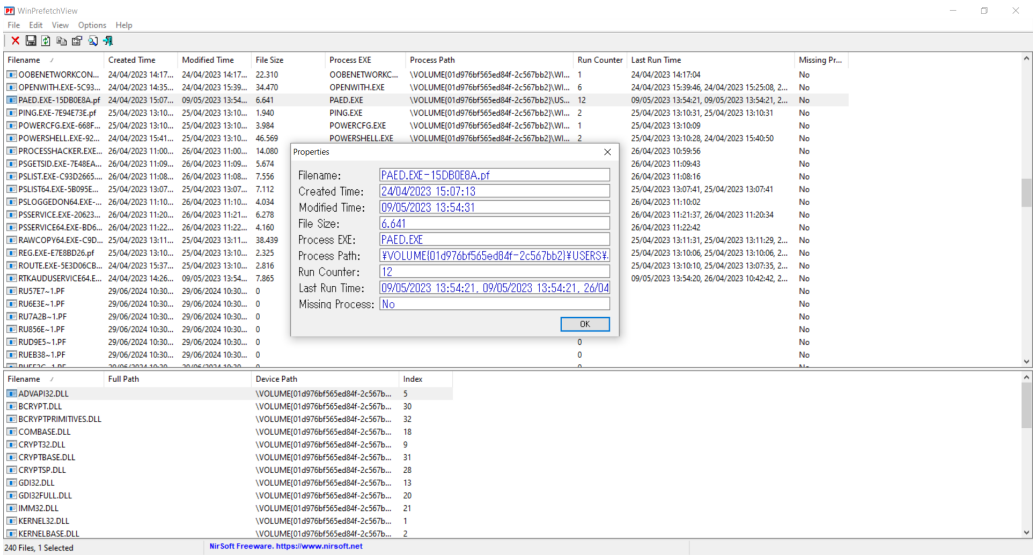


Figura 4.25: Fichero PAED.EXE en WinPrefech.

cifrado de extensión .deria. Si investigamos sobre este archivo encontramos que:

"El ransomware DeriaLock se instala en un sistema mediante archivos descargados por otros malware, en este caso Spora, o al visitar sitios maliciosos. Este ransomware cifra el sistema del usuario, donde los archivos aparecerán con extensión .deria."

¿Qué herramientas se han utilizado para realizar la adquisición?

El análisis de los archivos Prefetch indica que durante la adquisición posterior al incidente se emplearon herramientas forenses como Wintriage, FTK Imager y CyLR.

¿Se han extraído datos del usuario?

Una forma de evidenciar si se han llevado información almacenada del usuario en el equipo a través de alguna aplicación es analizar el artefacto SRUM (System Resource Utilization Monitor), que se trata de un sistema de monitorización de uso de aplicaciones de Windows, compuesto de tablas donde existe información de rutas, drivers del sistema, aplicaciones ejecutada en el equipo, bytes enviados y recibidos mediante aplicaciones, etc. Para ello extraemos el archivo SRUDB.dat que se localiza en la ruta C:\Windows\System32\srum. Para obtener la información almacenada en este artefacto, ejecutamos la herramienta SrumCmd desde la consola de comandos de Windows:

```
SrumECmd.exe -f C:\Input\SRUDB.dat --csv "C:\Output\SRUDB.csv"
```

La herramienta obtiene como salida una serie de archivos en formato CSV que contienen los registros del SRUM (figura 4.26).

En el archivo AppResourceUseInfo obtenemos un par de registros de rutas del sistema donde se han almacenado los ficheros malware que coinciden con las dos infecciones por ransomware.

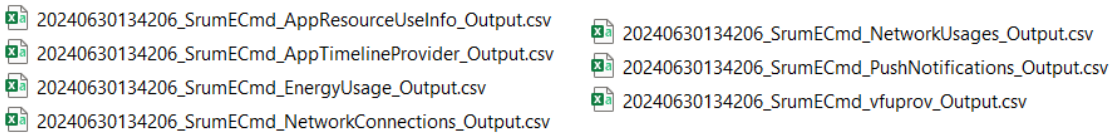
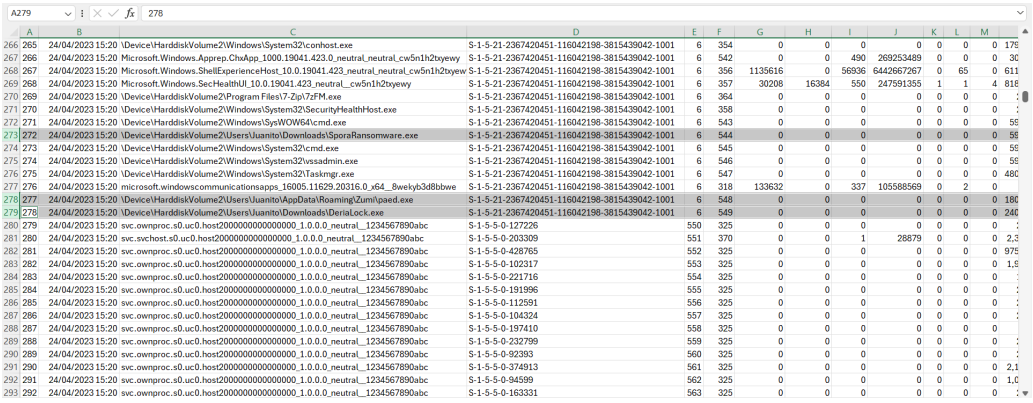


Figura 4.26: Archivos generados por SrumECmd.exe.

No debemos fiarnos de la marca de tiempo que registra este resultado, no es fiable, para ello, hemos analizado previamente los registros correspondientes a estos binarios almacenados en la $MFT. Lo interesante de esta tabla (figura 4.27) reside en que existe un artefacto llamado SporaRansomware.exe que se descargó en la carpeta de descargas del usuario, pero no existen evidencias de su ejecución. También obtenemos información acerca de la muestra de ransomware DerialLock que también se descargó en la carpeta de descargas del usuario y del binario paed.exe cuya localización ya habíamos obtenido, además, de evidencias de sus ejecuciones en el sistema.



	A	B	C	D	E	F	G	H	I	J	K	L	M	
266	265	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\System32\conhost.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	354	0	0	0	0	0	0	0	175
267	266	24/04/2023 15:20	Microsoft.Windows.Apprep.ChxApp_1000.19041.423.0_neutral_neutral_cw5n1h2txyewy	S-1-5-21-2367420451-1160421198-3815439042-1001	6	542	0	0	490	269253489	0	0	0	30
268	267	24/04/2023 15:20	Microsoft.Windows.ShellExperienceHost_10.0.19041.423_neutral_neutral_cw5n1h2txyew	S-1-5-21-2367420451-1160421198-3815439042-1001	6	356	1135616	0	56936	6442667267	0	65	0	611
269	268	24/04/2023 15:20	Microsoft.Windows.SecHealthUI_10.0.19041.423_neutral__cw5n1h2txyewy	S-1-5-21-2367420451-1160421198-3815439042-1001	6	357	30208	16384	550	247591355	1	1	4	818
270	269	24/04/2023 15:20	\Device\HarddiskVolume2\Program Files\7-Zip\7zFM.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	364	0	0	0	0	0	0	0	
271	270	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\System32\SecurityHealthHost.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	358	0	0	0	0	0	0	0	
272	271	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\SysWOW64\cmd.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	543	0	0	0	0	0	0	0	56
273	272	24/04/2023 15:20	\Device\HarddiskVolume2\Users\Juanito\Downloads\SporaRansomware.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	544	0	0	0	0	0	0	0	56
274	273	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\System32\cmd.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	545	0	0	0	0	0	0	0	56
275	274	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\System32\vssadmin.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	546	0	0	0	0	0	0	0	59
276	275	24/04/2023 15:20	\Device\HarddiskVolume2\Windows\System32\Taskmgr.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	547	0	0	0	0	0	0	0	480
277	276	24/04/2023 15:20	microsoft.windowscommunicationsapps_16005.11629.20316.0_x64__8wekyb3d8bbwe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	318	133632	0	337	105588569	0	2	0	
278	277	24/04/2023 15:20	\Device\HarddiskVolume2\Users\Juanito\AppData\Roaming\Zumi\paed.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	548	0	0	0	0	0	0	0	180
279	278	24/04/2023 15:20	\Device\HarddiskVolume2\Users\Juanito\Downloads\DeriaLock.exe	S-1-5-21-2367420451-1160421198-3815439042-1001	6	549	0	0	0	0	0	0	0	240
280	279	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-127226	550	325	0	0	0	0	0	0	0	
281	280	24/04/2023 15:20	svc.svchost.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-203309	551	370	0	0	1	28879	0	0	0	2,3
282	281	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-428765	552	325	0	0	0	0	0	0	0	975
283	282	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-102317	553	325	0	0	0	0	0	0	0	1,9
284	283	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-221716	554	325	0	0	0	0	0	0	0	
285	284	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-191996	555	325	0	0	0	0	0	0	0	
286	285	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-112591	556	325	0	0	0	0	0	0	0	
287	286	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-104324	557	325	0	0	0	0	0	0	0	
288	287	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-197410	558	325	0	0	0	0	0	0	0	
289	288	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-232799	559	325	0	0	0	0	0	0	0	
290	289	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-92393	560	325	0	0	0	0	0	0	0	
291	290	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-374913	561	325	0	0	0	0	0	0	0	2,1
292	291	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-94599	562	325	0	0	0	0	0	0	0	1,0
293	292	24/04/2023 15:20	svc.ownproc.s0.uc0.host2000000000000000_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-163331	563	325	0	0	0	0	0	0	0	

Figura 4.27: Artefactos SporaRansomware.exe y DeriaLock.exe

Es interesante realizar el cotejo de las horas reflejadas almacenadas en UsnJrnl con las obtenidas en el Prefetch, la $MFT y el $LogFile. Nos indica que la fecha y hora de la descarga de SporaRansomware.exe fue el 24 de abril a las 14:52:51h, una vez almacenado en la carpeta de descargas del usuario, se intentó ejecutar a las 15:02:28h sin éxito. Posteriormente, a las 15:07:13h se ejecutó el ransomware Spora original (paed.exe) desde la ruta donde estaba almacenada la carpeta Zumi. Este sí infectó el equipo, y posteriormente, se produjo la segunda infección causada por la ejecución de DeriaLock.

En las horas previas al incidente, se hallan evidencias del uso de OneDrive (14:19:28h) y 7-Zip (14:27:23h), puesto que visualizamos la ruta de instalación de estas aplicaciones en el sistema y su posterior ejecución. Esta información es de gran ayuda para reconstruir parte de la actividad desarrollada por el usuario en el sistema (figuras 4.28 y 4.29).

Esto puede indicar que el usuario pudo haber estado manipulando, subiendo, descargando o sincronizando archivos, y que alguna de estas acciónes podría ser la responsable de la presencia del malware.

Continuando con el análisis del SRUM, el archivo NetworkConnections almacena información sobre las interfaces de red a las que estuvo conectado el equipo, en particular, nos interesa la información relativa a el InterfaceType, Timestap, ConnectStartTime.

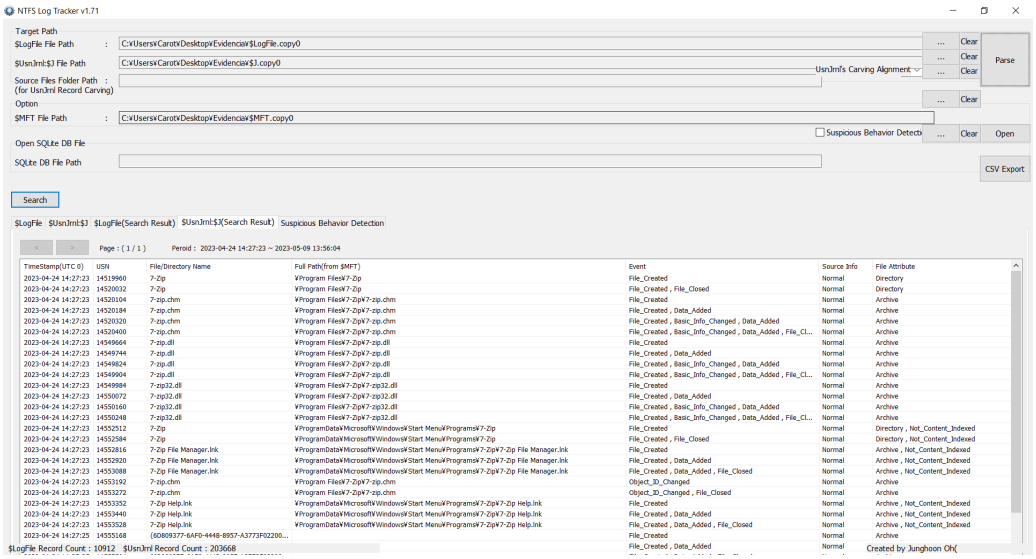


Figura 4.28: Registro de la ruta de instalación de 7-Zip en NTFS Log Tracker

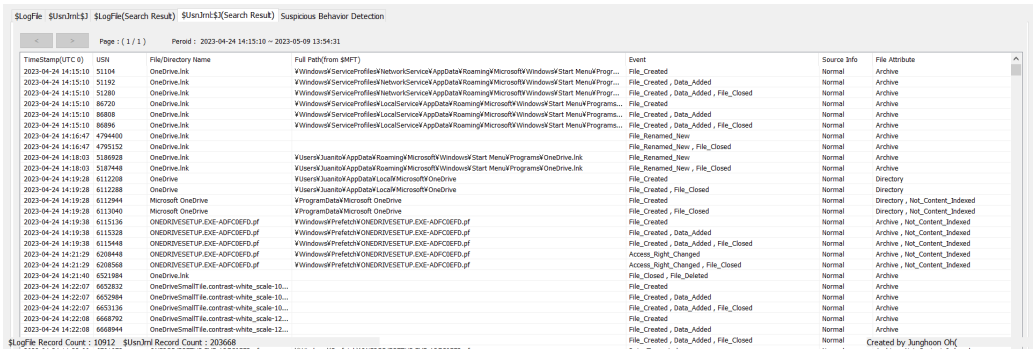
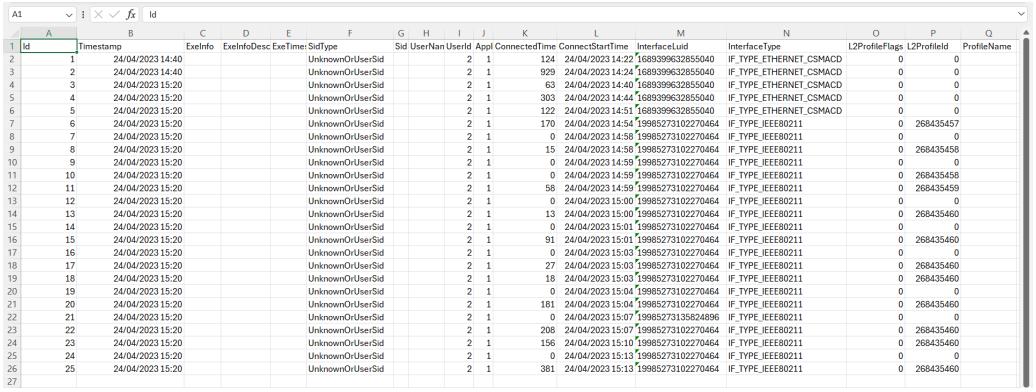


Figura 4.29: Registro de la ruta de instalación de OneDrive en NTFS Log Tracker

La información hallada (figura 4.30), refleja que el equipo se encontraba conectado previamente a la red local por cable (IF_TYPE_ETHERNET_CSMACD) y posteriormente, durante el proceso de doble infección por Spora y DeriaLock, estuvo conectado a través de Wifi (IF_TYPE_IEE80211).



Id	Timestamp	ExeInfo	ExeInfoDesc	ExeTimes	SidType	Sid	UserNan	UserId	Appl	ConnectedTime	ConnectStartTime	InterfaceLuid	InterfaceType	L2ProfileFlags	L2ProfileId	ProfileName
1	24/04/2023 14:40				UnknownOrUserSid			2	1	124	24/04/2023 14:22	1689399632855040	IF_TYPE_ETHERNET_CSMACD	0	0	
2	24/04/2023 14:40				UnknownOrUserSid			2	1	929	24/04/2023 14:24	1689399632855040	IF_TYPE_ETHERNET_CSMACD	0	0	
3	24/04/2023 15:20				UnknownOrUserSid			2	1	63	24/04/2023 14:40	1689399632855040	IF_TYPE_ETHERNET_CSMACD	0	0	
4	24/04/2023 15:20				UnknownOrUserSid			2	1	303	24/04/2023 14:44	1689399632855040	IF_TYPE_ETHERNET_CSMACD	0	0	
5	24/04/2023 15:20				UnknownOrUserSid			2	1	122	24/04/2023 14:51	1689399632855040	IF_TYPE_ETHERNET_CSMACD	0	0	
6	24/04/2023 15:20				UnknownOrUserSid			2	1	170	24/04/2023 14:54	1998527310227046	IF_TYPE_IEE80211	0	268435457	
7	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 14:58	1998527310227046	IF_TYPE_IEE80211	0	0	
8	24/04/2023 15:20				UnknownOrUserSid			2	1	15	24/04/2023 14:58	1998527310227046	IF_TYPE_IEE80211	0	268435458	
9	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 14:59	1998527310227046	IF_TYPE_IEE80211	0	0	
10	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 14:59	1998527310227046	IF_TYPE_IEE80211	0	268435458	
11	24/04/2023 15:20				UnknownOrUserSid			2	1	58	24/04/2023 14:59	1998527310227046	IF_TYPE_IEE80211	0	268435459	
12	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:00	1998527310227046	IF_TYPE_IEE80211	0	0	
13	24/04/2023 15:20				UnknownOrUserSid			2	1	13	24/04/2023 15:00	1998527310227046	IF_TYPE_IEE80211	0	268435460	
14	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:01	1998527310227046	IF_TYPE_IEE80211	0	0	
15	24/04/2023 15:20				UnknownOrUserSid			2	1	91	24/04/2023 15:01	1998527310227046	IF_TYPE_IEE80211	0	268435460	
16	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:03	1998527310227046	IF_TYPE_IEE80211	0	0	
17	24/04/2023 15:20				UnknownOrUserSid			2	1	27	24/04/2023 15:03	1998527310227046	IF_TYPE_IEE80211	0	268435460	
18	24/04/2023 15:20				UnknownOrUserSid			2	1	18	24/04/2023 15:03	1998527310227046	IF_TYPE_IEE80211	0	268435460	
19	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:04	1998527310227046	IF_TYPE_IEE80211	0	0	
20	24/04/2023 15:20				UnknownOrUserSid			2	1	181	24/04/2023 15:04	1998527310227046	IF_TYPE_IEE80211	0	268435460	
21	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:07	1998527313582489	IF_TYPE_IEE80211	0	0	
22	24/04/2023 15:20				UnknownOrUserSid			2	1	208	24/04/2023 15:07	1998527310227046	IF_TYPE_IEE80211	0	268435460	
23	24/04/2023 15:20				UnknownOrUserSid			2	1	156	24/04/2023 15:10	1998527310227046	IF_TYPE_IEE80211	0	268435460	
24	24/04/2023 15:20				UnknownOrUserSid			2	1	0	24/04/2023 15:13	1998527310227046	IF_TYPE_IEE80211	0	0	
25	24/04/2023 15:20				UnknownOrUserSid			2	1	381	24/04/2023 15:13	1998527310227046	IF_TYPE_IEE80211	0	268435460	

Figura 4.30: Registros de red del archivo NetworkConnections

Específicamente, se utilizó una tarjeta (antena) WiFi externa conectada por USB al equipo, ya que este no contaba con una tarjeta WiFi interna.

Es posible que el equipo intentara conectarse a la red WiFi corporativa. Sin embargo, es probable que dicha red estuviera configurada con restricciones para impedir el acceso a sitios web conocidos por distribuir malware, como repositorios de software malicioso.

Otra posibilidad es que el usuario del equipo haya utilizado su dispositivo móvil para compartir su conexión a Internet. Esta técnica, conocida como tethering, permite a los dispositivos conectarse a Internet a través de la red móvil del teléfono. El tethering puede ser utilizado para eludir las restricciones de la red corporativa, proporcionando acceso a Internet sin las limitaciones impuestas por los administradores de la red.

¿Cuál sería el origen de infección?

Teniendo en cuenta la existencia de esta conexión con antena, que nos abre la posibilidad de que los archivos maliciosos fueran descargados mediante la red inalámbrica, es necesario extraer y analizar las bases de datos de los navegadores instalados (History.dat para Chrome y Places.sqlite para Firefox).

En primer lugar, debemos corroborar la descarga de archivos maliciosos, para lo que vamos a ejecutar la herramienta DB Browser for SQLite, para poder correlacionar la información entre ambas herramientas y confirmar si el usuario ha descargado los archivos maliciosos.

Emplearemos la herramienta BrowsingHistoryView, donde seleccionaremos el fichero History.dat, para analizar el historial de navegación del usuario. En los resultados obtenidos, observamos que se ha accedido a páginas de malware y que se han realizado búsquedas específicas sobre el mismo. Esto nos hace sospechar de las intenciones del usuario (figura 4.31).

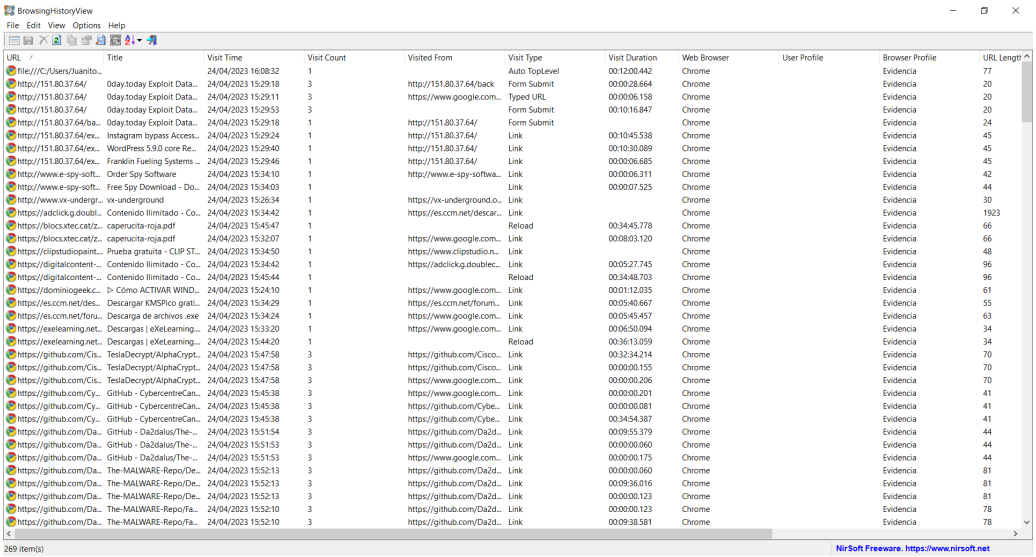


Figura 4.31: Análisis del historial de Chrome con BrowserHistoryView

Durante la investigación con DB Browser for SQLite, se identificaron entradas correspondientes a descargas de varios ransomware (figura 4.32), pero no encontramos coincidencias con el binario que provocó la infección, paed.exe. Es probable que alguno

de los archivos descargados con anterioridad a la infección lo contuviera. Visualizamos el archivo SporaRansomware.exe, y comprobamos en el Prefetch. Observamos que este archivo se descargó y es anterior. Es probable que el usuario descargase este ejecutable y que el binario paed.exe se encontrase oculto en su interior (esto suele ser habitual debido a que los actores maliciosos utilizan técnicas de esteganografía).

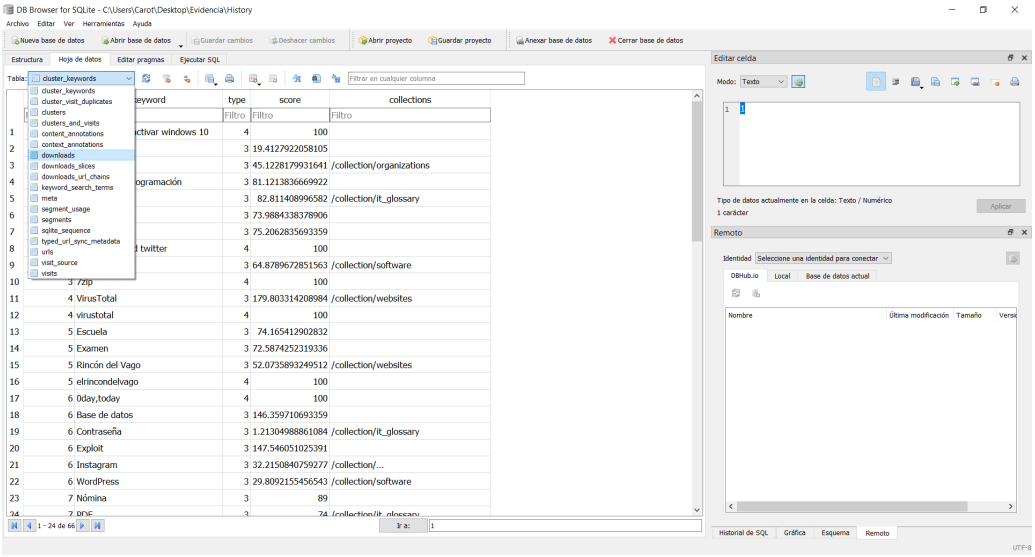


Figura 4.32: Análisis de descargas con DB Browser for SQLite

Pese a que hemos confirmado el origen de los archivos maliciosos, vamos a proceder con un análisis más profundo que corrobore esta información. Haremos uso de artefactos clave del sistema para eliminar la posibilidad de que se haya introducido la amenaza mediante un dispositivo externo. Para ello, necesitamos extraer los siguientes artefactos que posteriormente analizaremos con la herramienta USB Detective (figura 4.33): SYSTEM, SOFTWARE y NTUSER.DAT.

En los resultados del análisis, hemos observado que se ha realizado la conexión de dos dispositivos USB, Kingston y Sandisk (figura 4.34). Dicha información parece relevante. Por lo tanto, realizaremos un análisis de las shellbags (una característica del sistema operativo Windows que registra y almacena información sobre el historial de acceso a carpetas y archivos) con ShellBagsExplorer. Sin embargo, pese a que la hora y fecha de conexión de estos USB es relativamente cercana a la hora y fecha de la infección, las shellbacks no evidencian actividad ilícita haciendo uso de estos dispositivos.

Por lo tanto, podemos concluir que las dos muestras de ransomware fueron descargadas por el usuario Juanito a través del navegador Chrome, mediante la conexión a Internet a través de una antena WiFi.

Para comprobar que el usuario Juanito es culpable de las actividades ilícitas realizadas a través de su equipo corporativo, utilizaremos la herramienta FullEventLogView para comprobar que tipo de inicio de sesión se produjo el día del incidente por parte del usuario. Observamos un registro que nos indica un inicio de sesión de tipo dos que corresponde a una sesión local, esto implica que el inicio de sesión se produjo estando físicamente frente a la máquina, haciendo uso de teclado y ratón (figura 4.35).

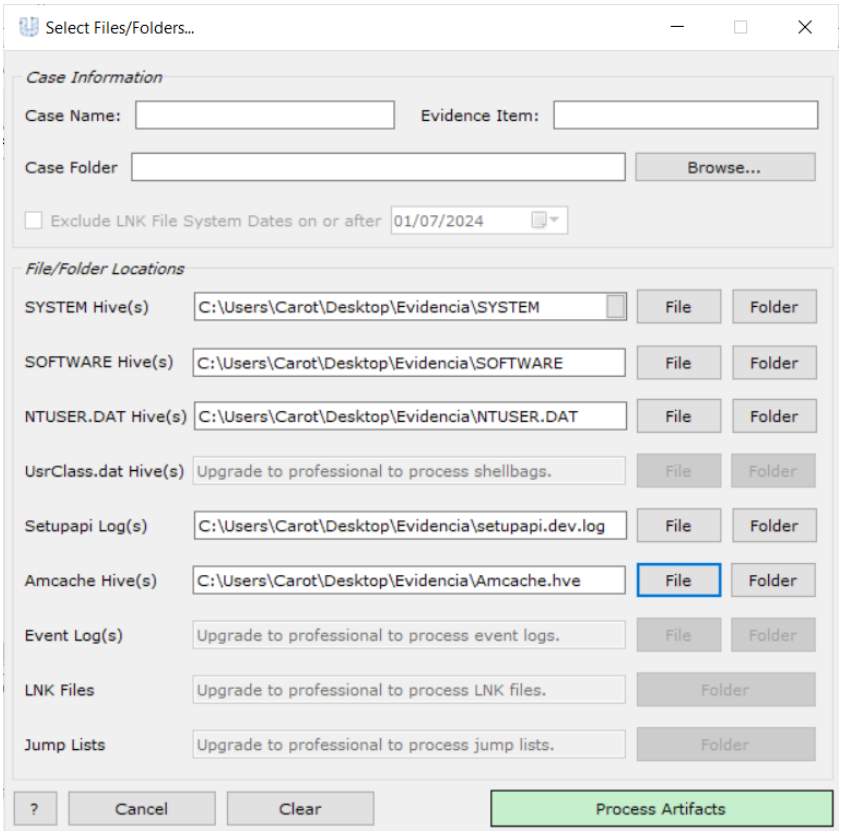


Figura 4.33: Adición artefactos con USB Detective

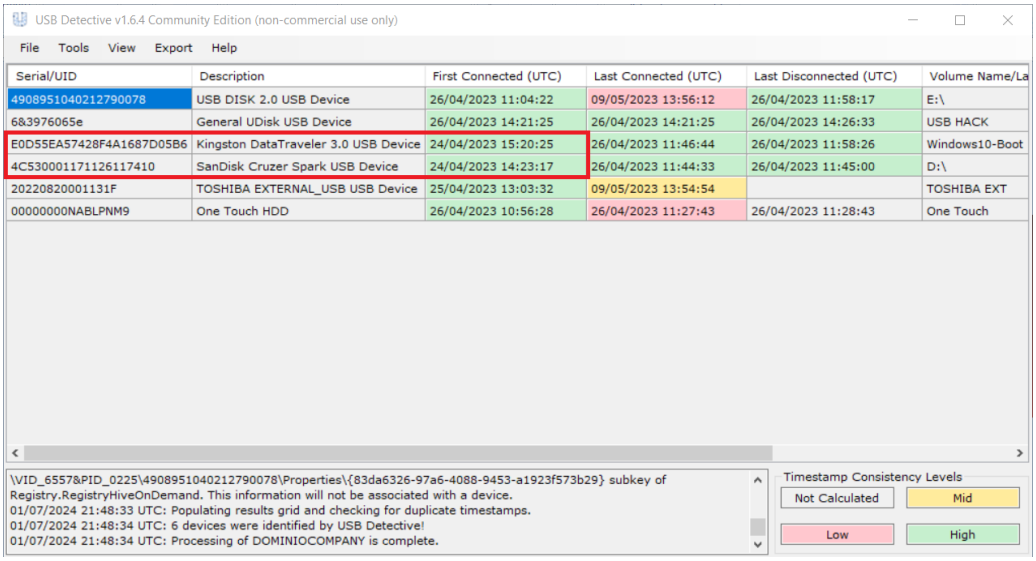


Figura 4.34: Análisis de dispositivos USB con USB Detective

Si el inicio de sesión registrado hubiera hubiera tenido un identificador tipo diez, indicaría una conexión remota en el equipo. Sin embargo, no encontramos ninguna evidencia de que esto se haya producido.

Mediante las evidencias obtenidas, podemos afirmar que el usuario Juanito, es el responsable de la descarga y posterior ejecución de las infecciones causadas por ransomware en el equipo corporativo.

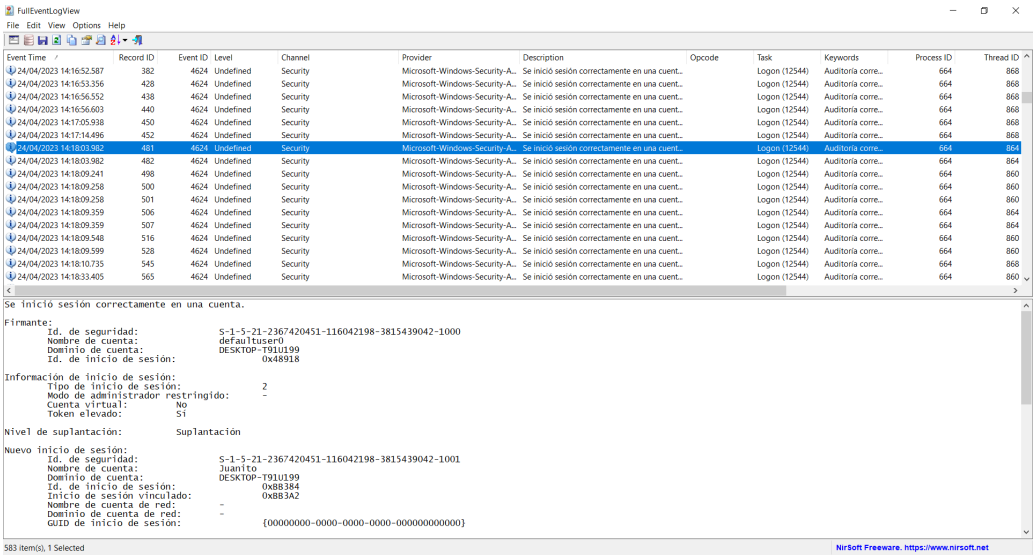


Figura 4.35: Análisis de inicio de sesión con FullEventLogView

4.3. Presentación de resultados y testimonio experto

Tras este análisis práctico, hemos comprendido el escenario del ataque y la forma en que se llevó a cabo la infección. A continuación expondremos los puntos claves de la misma, como la conclusión final del caso.

4.3.1. Escenario del ataque e infección

El análisis nos confirma en cuanto al proceso de infección de la máquina, que:

Para no ser descubierto, el usuario Juanito, utilizó una antena Wi-Fi. La antena posiblemente se conectó a un teléfono móvil configurado como enrutador para compartir su conexión a Internet debido al sistema capado de la empresa que no permite visitar páginas peligrosas como aquellas que contienen malware.

Una vez establecida la conexión, se accedió a repositorios de malware como VX Underground (https://www.vx-underground.org/), desde donde se descargó una muestra del binario para posteriormente, ejecutarlo y llevar a cabo el proceso de infección, dejando el equipo en el estado en el que fue encontrado.

Por tanto, podemos concluir que Juanito es el usuario responsable de la infección, pero no hay evidencia de que se haya llevado información confidencial de la empresa.

Capítulo 5

Resumen, conclusiones y líneas futuras

El desarrollo de esta investigación nos ha proporcionado una visión completa de los desafíos y necesidades en el campo de la informática forense. Hemos observado cómo los expertos deben enfrentar una multitud de casos complejos, manejando no solo cuestiones técnicas, sino también dilemas éticos, morales y legales. Esta experiencia ha resaltado la ausencia de una guía detallada de protocolos, obligando a los expertos a depender de recursos dispersos o genéricos y a compensar las deficiencias con su propia experiencia y juicio profesional.

La necesidad de una legislación y metodologías más específicas ha sido evidente. Sin embargo, la relativa novedad de esta disciplina en comparación con otras, junto con su amplitud y el rápido avance tecnológico, hace difícil abarcar todos los posibles escenarios prácticos y legales, así como mantener el ritmo con los cambios impuestos por la curva de desarrollo exponencial de la tecnología. Por lo tanto, la colaboración entre expertos informáticos, legisladores y agencias es esencial para desarrollar continuamente marcos legales adaptables y precisos que respondan a esta evolución.

Además, el estudio estadístico realizado ha revelado un aumento exponencial en los cibercrímenes, afectando particularmente a los grupos vulnerables. Estos grupos, incluidos individuos con conocimientos tecnológicos limitados, son más susceptibles a estafas y otros cibercrímenes. Este hallazgo subraya la importancia de implementar métodos de formación y prevención que aborden específicamente las necesidades de estos grupos, mejorando su capacidad para protegerse en el entorno digital. Además, un área clave de investigación que podríamos seguir en relación con las conclusiones de este proyecto es la incidencia de cibercrímenes como las estafas y el papel de la ingeniería social.

Finalmente, el análisis de casos prácticos nos ha proporcionado una visión directa de las tareas y desafíos que enfrenta un experto forense durante el análisis. Este ejercicio ha confirmado lo que ya sabíamos teóricamente sobre los desafíos en la adquisición, preservación y análisis de evidencias, así como las estrategias que utilizan los perpetradores para evitar la detección. En el futuro, sería interesante realizar más análisis demostrativos de otros tipos de malware.

En conclusión, el papel del experto en informática forense es multifacético, desafiante y cada vez más necesario, ya que la tecnología continúa evolucionando constantemente, presentando nuevos desafíos cada día.

Summary, conclusions and future lines

The development of this research has given us a comprehensive view of the challenges and needs in the field of computer forensics. We have been able to observe how experts must tackle a multitude of complex cases, managing not only technical issues but also ethical, moral, and legal dilemmas. This experience has highlighted the absence of a single detailed guide to protocols, forcing experts to rely on scattered or generic resources and to compensate for deficiencies with their own experience and professional judgment.

The need for more specific legislation and methodologies has been evident. However, the relative novelty of this discipline compared to others, coupled with its breadth and the rapid technological advancement, makes it difficult to encompass all possible practical and legal scenarios, as well as to keep pace with the changes imposed by technology's exponential development curve. Hence, collaboration among computer experts, legislators, and agencies is essential to continuously develop adaptable and precise legal frameworks that respond to this evolution.

Furthermore, the statistical study conducted has revealed an exponential increase in cybercrimes, particularly affecting vulnerable groups. These groups, including individuals with limited technological knowledge, are more susceptible to scams and other cybercrimes. This finding underscores the importance of implementing training and prevention methods that specifically address the needs of these groups, enhancing their ability to protect themselves in the digital environment. Additionally, one key area of investigation we could pursue related to the conclusions of this project is the incidence of cybercrimes such as scams and the role of social engineering.

Finally, the practical case analysis has provided us with a direct insight into the tasks and challenges faced by a forensic expert during analysis. This exercise has confirmed what we already knew theoretically about the challenges in acquiring, preserving, and analyzing evidence, as well as the strategies perpetrators use to avoid detection. In the future, it would be interesting to conduct more demonstrative case analyses of other types of malware.

In conclusion, the role of the computer forensic expert is multifaceted, challenging, and increasingly necessary, as technology continues to evolve constantly, presenting new challenges every day.

Capítulo 6

Presupuesto

Finalmente, se proporcionará una estimación del costo total del proyecto de análisis del caso práctico, considerando los medios utilizados y los honorarios correspondientes.

La fórmula que usaremos para calcular la amortización de los recursos es la siguiente:

$$\text{Coste (€)} = \text{Coste equipo} \cdot \frac{\text{Meses de uso}}{\text{Periodo de amortización (en meses)}} \cdot \text{Porcentaje de uso} \cdot \text{Unidades} \tag{6.1}$$

En el cual consideraremos el periodo de amortización de los recursos será en el caso del hardware de 5 años, mientras que en el caso de los recursos de software será de un año. Al estar en Canarias, debemos aplicar el siete por ciento de IGIC a los productos sin IVA para obtener el coste final.

Tabla 6.1: Presupuesto de honorarios

HONORARIOS	**Coste €/hora**	**Horas**	**Total**
Realización del análisis	50,00 €	168	8400,00
Traza, cronograma, redacción	25,00 €	100	2500,00
		SUBTOTAL	10900,00 €

Tabla 6.2: Presupuesto de hardware

HARDWARE	**Coste equipo**	**Meses de uso**	**Porcentaje de uso**	**Coste**
MSI Apache GE62	1650,00 €	6	1	165,00 €
Memoria USB 32GB	25,00 €	6	1	2,50 €
			SUBTOTAL	167,50 €

Tabla 6.3: Presupuesto de software

SOFTWARE	Coste	Meses de uso	Porcentaje de uso	Coste
Windows 10 Home	148,99 €	6	1	74,50 €
Windows 10 Pro	212,98 €	6	1	106,49 €
MOBILedit Pro	4500,00 €	1	0,2	75 €
USB Detective	466,14 €	4	0,4	62,15 €
FTK Imager	0,00 €	4	1	0,00 €
MFTECmd.exe	0,00 €	4	1	0,00 €
NTFS Log Tracker	0,00 €	4	1	0,00 €
WinPrefetchView	0,00 €	4	1	0,00 €
HxD	0,00 €	4	1	0,00 €
SrumECmd	0,00 €	4	1	0,00 €
Event Log Explorer	0,00 €	4	1	0,00 €
RegRipper	0,00 €	4	1	0,00 €
BrowsingHistoryView	0,00 €	4	1	0,00 €
DB Browser for SQLite	0,00 €	4	1	0,00 €
ShellBackView	0,00 €	4	1	0,00 €
dd	0,00 €	1	1	0,00 €
			SUBTOTAL	318,14 €

Tabla 6.4: Presupuesto subtotal del proyecto

HARDWARE	SOFTWARE	HONORARIOS	SUBTOTAL
167,50 €	318,14 €	10900,00	11385,64 €

Tabla 6.5: Presupuesto total

SUBTOTAL	11385,64 €
% IGIC	7,00 %
IGIC	796,99 €
TOTAL	12182,63 €

Bibliografía

[1] Tapia, J. (2023). Origen de la Informática forense. 10.13140/RG.2.2.18012.97927. Recuperado de https://doi.org/10.13140/RG.2.2.18012.97927

[2] IBM. (s.f.). Computer forensics. Recuperado de https://www.ibm.com/es-es/topics/computer-forensics.

[3] Tapia, J. (2022). Análisis de casos forenses digitales. ResearchGate. https://www.researchgate.net/publication/366570092_Analisis_de_casos_forenses_digitales

[4] Roussev, V. (2016). Digital Forensic Science: Issues, Methods, and Challenges. Elsevier.

[5] Informática Forense. (s.f.). La evolución de la informática forense desde sus inicios. Recuperado de https://www.informaticaforense.com.co/la-evolucion-de-la-informatica-forense-desde-sus-inicios/

[6] Ciberseguridad. (2023). Organismos y entidades en España. Ciberseguridad. https://ciberseguridad.com/normativa/espana/organismos

[7] Agencia Española de Protección de Datos. (s.f.). Agencia Española de Protección de Datos (AEPD). AEPD. https://www.aepd.es

[8] Policía Nacional. (s.f.). Brigada Central de Investigación Tecnológica (B.C.I.T.). Policía Nacional. https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

[9] Guardia Civil. (s.f.). Grupo de Delitos Telemáticos (GDT). Guardia Civil. https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gdt/index.html

[10] Centro Criptológico Nacional (CCN-CERT). (s.f.). CCN-CERT. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/

[11] Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). INCIBE. INCIBE. https://www.incibe.es/

[12] Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). 10 Aniversario INCIBE. INCIBE. https://www.incibe.es/incibe/informacion-corporativa/10-aniversario-incibe

[13] Centro Criptológico Nacional (CCN-CERT). (s.f.). CCN-CERT. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/

[14] Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). (s.f.). CNPIC. Ministerio del Interior https://cnpic.interior.gob.es/es/inicio/

[15] Juanes Fernández, D. (2020). Instituciones españolas referentes en ciberseguridad. Sec2Crime. https://www.sec2crime.com/2020/12/06/instituciones-espanolas-referentes-en-ciberseguridad/

[16] Jiménez Chouza, M. (2013). La amenaza cibernética: Un nuevo factor de riesgo para la seguridad internacional. IEEE. https://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA40-2013_AmenazaCibernetica_MJC.pdf

[17] Ministerio del Interior. (s.f.). Informe sobre la cibercriminalidad en España. Ministerio del Interior. https://www.interior.gob.es/opencms/es/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas/informe-sobre-la-cibercriminalidad-en-espana/

[18] Ministerio del Interior. (2013). Avance de datos de cibercriminalidad 2013. Ministerio del Interior. https://www.interior.gob.es/opencms/pdf/avance-datos-ciberciminalidad-2013_2037732.pdf

[19] Observatorio Español de Delitos Informáticos (OEDI). (s.f.). Estadísticas. OEDI. https://oedi.es/estadisticas/

[20] Ministerio del Interior. (s.f.). Búsqueda de ciberdelitos. Ministerio del Interior. https://www.interior.gob.es/opencms/es/search/index.html?lq=&reloaded=&q=ciberdelitos&sort=score+desc&fechaInicio=&fechaFin=

[21] Instituto Nacional de Estadística (INE). (s.f.). Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. INE. https://www.ine.es/dyngs/INEbase/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=resultados&idp=1254735976608

[22] Alonso, C. (2014). El asesino en serie BTK fue descubierto por los metadatos. Un informático en el lado del mal. https://www.elladodelmal.com/2014/06/el-asesino-en-serie-btk-fue-descubierto.html

[23] de la Torre, A. (2016). ¿Es Dennis Rader el asesino del Zodíaco?. Investigación Criminal. https://investigacioncriminal.es/es-dennis-rader-el-asesino-del-zodiaco/

[24] Pastor, A. J. (2023). El 'caso Déborah' se fía a los expertos informáticos de Diana Quer y Marta del Castillo. Atlántico. https://www.atlantico.net/articulo/vigo/caso-deborah-fia-expertos-informaticos-diana-quer-marta-castillo/20230316235901973848.html

[25] La Nación. (2024). La desaparición de Madeleine McCann: descubrieron dos cuentas de correo electrónico que comprometen al principal acusado. La Nación. https://www.lanacion.com.ar/

[26] Indalics. (s.f.). Caso Diana Quer: entrevista Tele 5. https://indalics.com/noticias/caso-diana-quer-entrevista-tele-5

[27] El Ideal Gallego. (2017). Experto señala el caso Diana Quer como ejemplo del trabajo silencioso que hace la Guardia Civil. El Ideal Gallego. https://www.elidealgallego.com/

[28] Macian, A. (2020). ANÁLISIS CRIMINOLÓGICO-JURÍDICO DEL CASO DIANA QUER. https://www.uv.es/gicf/5C1_Macian_GICF_37.pdf

[29] Diario de Sevilla. (2023, junio 25). Ingenieros informáticos denunciaron a Marta por intrusismo. Diario de Sevilla. Recuperado de https://www.diariodesevilla.es/juzgado_de_guardia/actualidad/ingenieros-informaticos-denuncio-Marta-intrusismo_0_1866713832.html

[30] Diario de Sevilla. (2023, mayo 12). Entrega del informe pericial del teléfono de Carcaño. Diario de Sevilla. Recuperado de https://www.diariodesevilla.es/juzgado_de_guardia/actualidad/entrega-informe-pericial-telefono-Carcano_0_1854416853.html

[31] Chen, L., Drannbauer, E., Ademoroti, A., Williams, D., Sebastian, G. (2023). How Plausible is North Korea's Involvement in the Sony Pictures Hack? A Comprehensive Analysis. Retrieved from https://www.researchgate.net

[32] Satheesh Kumar, M., Ben-Othman, J., Srinivasagan, K.G. (2018). .ªn Investigation on Wannacry Ransomware and its Detection,"2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, pp. 1-6, doi: 10.1109/ISCC.2018.8538354.

[33] Chen, Q., Bridges, R.A. (2017). .ªutomated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware,"2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, pp. 454-460, doi: 10.1109/ICMLA.0-119. keywords: Malware;Feature extraction;Encryption;Robustness;Tools;Data mining,

[34] INCIBE. (n.d.). *¿Has recibido un email de Correos? Guarda precaución, puede ser un phishing*. Retrieved from https://www.incibe.es/ciudadania/avisos/has-recibido-un-email-de-correos-guarda-precaucion-puede-ser-un-phishing

[35] Universidad Pontificia Comillas. (n.d.). Retrieved from https://repositorio.comillas.edu/rest/bitstreams/6234/retrieve

[36] Harvard Law School Forum on Corporate Governance. (2021, April 5). *Twenty years later: The lasting lessons of Enron*. Retrieved from https://corpgov.law.harvard.edu/2021/04/05/twenty-years-later-the-lasting-lessons-of-enron/

[37] Integrity Forensic. (n.d.). *Enron's fall from grace: How forensic accounting exposed fraud*. Retrieved from https://integrityforensic.com/enrons-fall-from-grace-how-forensic-accounting-exposed-fraud/

[38] Almudena Badiola Enseñat. (n.d.). Universidad Pontificia Comillas. Retrieved from https://repositorio.comillas.edu/rest/bitstreams/440626/retrieve

[39] Maras, M. H. (2014). Inside Darknet: the takedown of Silk Road: Marie-Helen Maras reports on the unexplored underworld of cyberspace. Criminal Justice Matters, 98(1), 22–23. https://doi.org/10.1080/09627251.2014.984541

[40] Camacho-Losa, L. (1987). Delito Informático. Madrid: Gráficas Cóndor.

[41] L. Hernández Díaz, "El delito informático". Eguzkilore. Cuaderno del Instituto Vasco de Criminología. nº 23. pp. 227- 243. 2009. Recuperado de https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

[42] Acurio Del Pino, S. (s.f.). Delitos informáticos: generalidades. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[43] Sánchez, J. (2007). Delitos informáticos. Recuperado de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

[44] Jefatura del Estado. (1978). Constitución Española. Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[45] BOE. (2000, 7 de enero). Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

[46] Ministerio de la Gobernación. (1882, 14 de septiembre). Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (Capítulo VII: Del informe pericial, Artículos 456-485). BOE-A-1882-6036. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20231220

[47] Jefatura del Estado. (2002). Ley Orgánica 10/2002, de 23 de diciembre, de Calidad de la Educación. Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

[48] Jefatura del Estado. (2007). Ley Orgánica 6/2007, de 24 de mayo, de reforma de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

[49] Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[50] Laboratorio Electrónica Forense. (2021). Legislación que afecta al perito judicial en España. Recuperado de https://laboratorioelectronicaforense.com/2021/04/05/legislacion-que-afecta-al-perito-judicial-espana/

[51] Jefatura del Estado. (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

[52] Agencia Estatal Boletín Oficial del Estado. (2021). Código de Derecho de la Ciberseguridad. Recuperado de https://www.boe.es/biblioteca_juridica/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho_de_la_Ciberseguridad.pdf

[53] Jefatura del Estado. (2010). Ley 22/2010, de 20 de julio, del Código de Consumo de Cataluña. Boletín Oficial del Estado. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[54] Unión Europea. (2002). Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371

[55] Unión Europea. (2006). Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2006-80647

[56] Unión Europea. (2011). Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/doue/2011/335/L00001-00014.pdf

[57] Unión Europea. (2013). Reglamento (UE) Nº 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648

[58] Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/doue/2016/194/L00001-00030.pdf

[59] Unión Europea. (2004). Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, sobre el derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros. Diario Oficial de la Unión Europea. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2004-80487

[60] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press.

[61] Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.

[62] Geschonneck, A. (2014). Computer-Forensik (iX Edition). Heidelberg, Germany: dpunkt.

[63] Lázaro Domínguez, F. (2014). Introducción a la informática forense. Paracuellos de Jarama, Madrid, RA-MA Editorial. Recuperado de https://elibro-net.accedys2.bbtk.ull.es/es/ereader/bull/106250?page=38

[64] AENOR. (2013). Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias digitales (Norma UNE 71506). Madrid, España: AENOR.

[65] AENOR. (2013). Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas. Parte 1: Vocabulario y principios generales (Norma UNE 71505-1). Madrid, España: AENOR.

[66] AENOR. (2013). Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas. Parte 2: Buenas prácticas en la gestión de evidencias electrónicas (Norma UNE 71505-2). Madrid, España: AENOR.

[67] AENOR. (2013). Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas. Parte 3: Formatos y mecanismos técnicos (Norma UNE 71505-3). Madrid, España: AENOR.

[68] AENOR. (2016). UNE-EN ISO/IEC 27037:2016. Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas (ISO/IEC 27037:2012). Madrid, España: AENOR.

[69] AENOR. (2016). UNE-EN ISO/IEC 27042:2016. Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de las evidencias electrónicas (ISO/IEC 27042:2015). Madrid, España: AENOR.

[70] González Reyes, J. M. (2021). La prueba pericial digital y la cadena de custodia. Anales de la Facultad de Derecho, 38, 43-79. https://doi.org/10.25145/j.anfade.2021.38.03

[71] Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda. (s. f.). ¿Qué es una huella digital? Recuperado el 23 de junio de 2024, de https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9IeUoAH/content/1025-que-es-una-huellla-digital-#:~:text=Una%20huella%20digital%20es%20un,datos%20singular%20de%20longitud%20fija

[72] Universidad Nacional Autónoma de Nicaragua León, Facultad de Derecho, Modalidad sabatina. (Noviembre, 2012). Deontología criminalística en el ejercicio de la investigación penal. Br. Lester Manuel Solís A, Br. Jorge Luis Rojas Castellón, Br. Álvaro Rojas Navarrete, y Lic. Juan Pablo Medina Rojas (Tutor). Recuperado de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/202/1/224267.pdf

[73] Asociación de Peritos Judiciales de España, APJUDE. (2020). Código deontológico. Recuperado de https://apjude.com/wp-content/uploads/2020/03/codigo-deontologico.pdf

[74] Martínez, A. (2014, 18 de junio). RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento. INCIBE-CERT. Recuperado de https://www.incibe.es/incibe-cert/blog/rfc3227

[75] Arocha Vinagre, S. B. (2017). Ciberdelincuencia: Problemas en la determinación de la jurisdicción y competencia de los tribunales del orden penal [Cybercrime: Problems in the determination of the jurisdiction and criminal jurisdiction of the criminal courts]. (Trabajo de fin de grado, Universidad de La Laguna, Facultad de Derecho).

[76] Unión Europea. (2002). Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre los Estados miembros. Recuperado de https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32002F0584

[77] Jefatura del Estado. (1982). Ley Orgánica 10/1982, de 10 de agosto, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1982-13611

[78] Unión Europea. (1996). Convenio relativo a la extradición entre los Estados miembros de la Unión Europea. Recuperado de https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-extradition-between-member-states.html

[79] Pardo, J. F. & Vitola, J. L. (2023). Aplicación de las fases del análisis forense digital simulando una escena del crimen denominada "El hacker Asesino". Recuperado de http://hdl.handle.net/11371/5950

[80] INCIBE-CERT. (n.d.). Herramientas para realizar análisis forenses a dispositivos móviles. Instituto Nacional de Ciberseguridad. Recuperado de https://www.incibe.es/incibe-cert/blog/herramientas-para-realizar-analisis-forenses-dispositivos-moviles

[81] Nilles, G., Silva, G., and Semprini, G. (2024). Adquisición de dispositivos móviles Android con imagen en vivo. En Simposio Argentino de Informática y Derecho. ISSN: 2451-7526.

[82] Soto, M. G. (2021). Análisis forense informático. RA-MA.

[83] López Delgado, M. Análisis Forense Digital. 2nd ed., revised and adapted for publication in CriptoRed. Ciudad de México, México: Editorial Forense, 2007. Print. (First edition: June 2006).

[84] Instituto Nacional de Ciberseguridad de España (INCIBE). RFC 3227 Guidelines for Evidence Collection and Archiving."2021. Web. Recuperado de https://www.incibe.es/incibe-cert/blog/rfc3227.

[85] Guttman B, White DR, Walraven T (2022) Digital Evidence Preservation: Considerations for Evidence Handlers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8387. https://doi.org/10.6028/NIST.IR.8387

[86] Oltra Gutiérrez, J. V. (2021). Bloqueos (intencionales o no) en el camino de un perito informático [Vídeo]. Polimedia. https://polimedia.upv.es/visor/?id=14f91da0-af10-11eb-b7fc-e95eca16729b

[87] Muñoz Muñoz, A. (2016). Privacidad y ocultación de información digital. Madrid: RA-MA Editorial.

[88] Johansen, G. (2022). Digital Forensics and Incident Response (3rd ed.). Birmingham, England: Packt Publishing.

[89] Vasquez, M. D. (2016). Técnicas Anti-Forenses Informáticas. Trabajo Final Integrador, Universidad Nacional de Córdoba.

[90] Oval Torres, C. (2024). Documentos de custodia de evidencia. Recuperado de https://drive.google.com/file/d/1KQG7nHIZDOaJzLaLdBOWCx-a2_6_gJzI/view?usp=drive_link

[91] Fortuna, A. (2017, octubre 6). MACB times in Windows forensic analysis. Andrea Fortuna's Blog. https://andreafortuna.org/2017/10/06/macb-times-in-windows-forensic-analysis/