

# INFORME PERICIAL



## Auditoría y Legislación Informática

---

Análisis Forense de Discos



Auditoría y Legislación Informática

# ÍNDICE

DECLARACIÓN DE VERACIDAD .....	3
PRESENTACIÓN DEL PERITO.....	4
OBJETO DEL PERITAJE.....	4
ALCANCE .....	5
ANTECEDENTES.....	6
FUENTES DE INFORMACIÓN Y DATOS DE PARTIDA.....	7
• ORDENADOR PORTÁTIL DEL EMPLEADO BAJO SOSPECHA: .....	7
• ORDENADOR PORTÁTIL COMO ACCESO REMOTO: .....	8
• USB POSESIÓN DEL INDIVIDUO SOSPECHOSO: .....	8
• USB POSESIÓN DEL INDIVIDUO SOSPECHOSO (PROPORCIONADO DIGITALMENTE): .....	9
ESTÁNDARES Y NORMAS .....	9
LIMITACIONES.....	10
RESOLUCIÓN.....	10
• CLONACIÓN E IDENTIFICACIÓN DE LA IMAGEN .....	10
• MONTAJE DE LA IMAGEN CREADA, RECUPERACIÓN DE FICHEROS ELIMINADOS Y RECUPERACIÓN DE LAS EXTENSIONES .....	14
• MONTAJE DE LA IMAGEN FACILITADA DIGITALMENTE, RECUPERACIÓN DE FICHEROS ELIMINADOS Y RECUPERACIÓN DE LAS EXTENSIONES. ....	26
CONCLUSIONES.....	34

# DECLARACIÓN DE VERACIDAD



## Colegio Profesional de Ingenieros en Informática de Extremadura

<http://www.cpiiex.es>

Campus Universitario - Escuela Politécnica

Av. de la Universidad, s/n

10.003 Cáceres

CIF: G10363XXX

## DICTAMEN PERICIAL

El firmante del presente peritaje, Ignacio Alcalde Torrecusa, con DNI 80225604-V y Colegiado nº 429 del Colegio Profesional de Ingenieros en Informática de Extremadura, **DECLARA**, bajo su única responsabilidad, que todo lo que afirma en el presente dictamen se basa únicamente en los hechos que ha podido constatar, y en su propio conocimiento y experiencia adquirida en el ejercicio profesional.

También **DECLARA** conocer las responsabilidades civiles, penales, disciplinarias y asociativas que comporta la aceptación del cargo de perito y la realización del presente informe, al amparo del artículo 335 de la Ley de Enjuiciamiento Civil, que reza así:

*“Al emitir el dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir la verdad, que ha actuado y, en su caso, actuará 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 conoce las sanciones penales en las que podría incurrir si incumpliera su deber como perito”.*

Cáceres, 19 de octubre de 2023

Fdo. Ignacio Alcalde Torrecusa

## PRESENTACIÓN DEL PERITO



Ignacio Alcalde Torrecusa posee una distinguida trayectoria en el campo de la peritación informática, respaldada por una formación académica sólida. Ignacio Alcalde se graduó en Ciencias de la Seguridad Informática de la Universidad de Extremadura y el Máster en Ciberseguridad de la Universidad de Stanford, reconocida a nivel mundial por su excelencia en tecnología y seguridad, son titulaciones que respaldan su experiencia.

A lo largo del tiempo, ha tenido el privilegio de colaborar con empresas líderes en tecnología, como Microsoft y IBM, donde ha aportado habilidades en peritaje informático para resolver casos de gran complejidad. La experiencia práctica en la industria le ha permitido comprender a fondo los desafíos y las amenazas que enfrentan las organizaciones en un entorno digital en constante evolución.

Además de la formación académica y experiencia en el sector privado, ha tenido el honor de trabajar en estrecha colaboración con agencias gubernamentales de renombre, como el Departamento de Seguridad Nacional de los Estados Unidos y la Interpol, donde ha contribuido a investigaciones de alto perfil relacionadas con ciberdelincuencia y seguridad nacional.

Como miembro activo del Cuerpo Oficial de Peritos, mantiene un compromiso con los más altos estándares éticos y profesionales en el trabajo.

En resumen, la sólida formación académica, experiencia en empresas de renombre mundial y colaboración con agencias gubernamentales distinguidas lo sitúan como un experto de confianza y altamente calificado en el ámbito de la peritación informática y ciberseguridad.

## OBJETO DEL PERITAJE

El presente informe pericial tiene como objetivo abordar un caso de alta complejidad relacionado con un presunto delito de Intrusión Informática Agravada. Esta grave infracción penal involucra la incursión no autorizada, el acceso ilícito y el robo de información en sistemas informáticos críticos de una entidad gubernamental de primer nivel. Se requiere la intervención del perito debido a la necesidad de llevar a cabo un análisis exhaustivo del contenido digital asociado a esta intrusión, así como la evaluación de las sofisticadas técnicas de encubrimiento empleadas por los perpetradores para eludir la detección y evitar la atribución de responsabilidades.

La intervención del perito es esencial para llevar a cabo un peritaje forense de alto nivel. Esto implica identificar, extraer y documentar de manera precisa y fiable las pruebas digitales que respalden la investigación en curso. Se incluye la recuperación de registros de acceso, logs de

eventos, archivos manipulados y cualquier otra evidencia pertinente que pueda aportar claridad sobre los detalles del incidente y la identidad de los posibles responsables.

Es crucial subrayar que el carácter altamente especializado y técnico del caso requiere la intervención de un experto en auditoría y legislación informática, capaz de abordar las complejidades de este tipo de delitos cibernéticos. La precisión y meticulosidad en la recopilación y evaluación de pruebas digitales son fundamentales para establecer una base sólida y confiable que respalde el proceso judicial en curso y contribuya a la administración de justicia de manera efectiva.

En resumen, el objeto del presente peritaje se centra en proporcionar un análisis detallado y riguroso de la intrusión informática agravada en cuestión, así como en presentar pruebas sólidas y verificables que respalden la investigación. La intervención del perito se justifica por la naturaleza técnica y altamente especializada del caso, que requiere la experiencia y conocimientos específicos en auditoría y legislación informática para garantizar la integridad y fiabilidad de los hallazgos presentados.

## ALCANCE

La intervención del perito se encuentra debidamente acotada a la evaluación de los aspectos técnicos relacionados con el presunto delito de Intrusión Informática Agravada, que incluye la incursión no autorizada, acceso ilícito y el robo de información en sistemas informáticos críticos de una entidad gubernamental de primer nivel.

El alcance de esta intervención se centra en el análisis de los archivos digitales susceptibles de proporcionar indicios relevantes para la investigación en curso. Se priorizará la identificación de cualquier actividad digital que pueda estar asociada con la intrusión y el robo de información en cuestión.

La ventana temporal definida para este análisis abarca un período de los últimos 12 meses. Esto implica que se considerará cualquier actividad digital registrada en el sistema durante este lapso, con el objetivo de identificar patrones y evidencias relacionadas con la intrusión, así como el robo de información.

Cabe destacar que el alcance de esta intervención se limita a los aspectos técnicos y digitales de la presunta intrusión y robo de información, excluyendo cualquier evaluación o valoración de aspectos legales o de procedimiento. Asimismo, se restringe a los archivos y registros que se encuentren dentro del ámbito de competencia y jurisdicción de la entidad en cuestión.

En resumen, el alcance de la intervención del perito se concentra en la evaluación técnica de los archivos digitales pertinentes para la investigación de la intrusión y robo de información. Se considerará una ventana temporal de los últimos 12 meses para recopilar indicios relevantes. Se enfatiza que el perito se centra exclusivamente en aspectos técnicos, sin realizar valoraciones legales o de procedimiento, y dentro de la jurisdicción específica de la entidad involucrada.

## ANTECEDENTES

Los antecedentes que se presentan al perito constituyen los indicios esenciales que han permitido definir el objeto del peritaje, manteniéndose dentro de los límites del alcance previamente identificado. Dichos indicios se desglosan de la siguiente manera:

- **Detección de Actividad Anómala:** Se ha registrado una actividad inusual y no autorizada en los sistemas informáticos de la entidad gubernamental de primer nivel. Este hallazgo inicial generó sospechas de una posible intrusión.
- **Alertas de Seguridad:** Los sistemas de monitoreo de seguridad informática emitieron alertas que indicaban intentos de acceso no autorizado a áreas sensibles y críticas de la infraestructura digital de la entidad.
- **Patrones de Comportamiento Atípicos:** Se observaron patrones de acceso y actividad en el sistema que difieren significativamente de los patrones normales, lo que sugiere un posible comportamiento malicioso.
- **Informe de Pérdida de Información Confidencial:** Se reportó la pérdida de información confidencial y crítica para la entidad. La naturaleza de esta pérdida sugiere una posible extracción no autorizada.
- **Registros de Eventos Digitales:** Se dispone de registros de eventos digitales que documentan la actividad del sistema durante el período de interés. Estos registros serán sometidos a un riguroso análisis forense.
- **Evidencia de Técnicas de Encubrimiento:** Se ha identificado la utilización de técnicas avanzadas de encubrimiento por parte de los perpetradores, lo que indica una clara intención de evadir la detección.
- **Presunción de Responsabilidad:** Existen sospechas fundadas sobre la implicación de actores externos en la intrusión y el posterior robo de información.

Estos antecedentes, al ser debidamente considerados, han proporcionado una base sólida para la definición del objeto del peritaje. Asimismo, se han tomado las precauciones necesarias para asegurar que la intervención del perito se mantenga dentro del alcance identificado, evitando así exceder los límites establecidos.

# FUENTES DE INFORMACIÓN Y DATOS DE PARTIDA

## Dispositivos Facilitados para la Investigación:

Para iniciar la investigación, se han facilitado los siguientes dispositivos:

Estos portátiles fueron incautados en el lugar de los hechos y presentan indicios de estar relacionados con la intrusión. Uno de los portátiles pertenecía a un empleado que estuvo bajo sospecha previa, y el otro fue identificado como un dispositivo de acceso remoto utilizado durante la intrusión.

### ORDENADOR PORTÁTIL DEL EMPLEADO BAJO SOSPECHA:

Número de Serie: XXXX-XXXX-XXXX

Nombre del dispositivo: Lenovo IdeaPad 3

- **Marca** Lenovo
- **Modelo** IdeaPad3
- **Procesador** Intel® Core™ i5-1155G7
- **Memoria RAM** 2 x 4GB
- **Almacenamiento** 256 GB SSD M.2 2280 PCIe 3.0x4 NVMe
- **Controlador gráfico** Integrated Intel UHD Graphics
- **Conectividad** 11ac, 2x2 + BT5.0
- **Conexiones**
  - 1x USB 3.2 Gen 1
  - 1x USB-C 3.2 Gen 1 (support data transfer only)
  - 1x HDMI 1.4b
  - 1x headphone / microphone combo jack (3.5mm)
  - 1x USB 2.0
- **Sistema operativo** Windows 10 Pro
- **Dimensiones** 359.2 x 236.5 x 19.9 mm
- **Peso** 1.65 kg
- **Color** Arctic Grey



El portátil perteneciente al empleado sospechoso cuenta con un sistema de seguridad básico, que incluye una contraseña de inicio de sesión y una protección de acceso a ciertos archivos y carpetas mediante una contraseña adicional. No se han identificado medidas de seguridad adicionales, como cifrado de disco o autenticación de doble factor.

### ORDENADOR PORTÁTIL COMO ACCESO REMOTO:

Número de Serie: 9S7-15HK12-039

Nombre del dispositivo: MSI Modern 15 B7M-039XES

- **Marca** MSI
- **Modelo** Modern 15 B7M-039XES
- **Procesador** AMD Ryzen 5
- **Memoria RAM** 8 GB DDR4 SDRAM
- **Almacenamiento** 512 GB
- **Controlador gráfico** AMD Dedicated
- **Conectividad** 11ac, 2x2 + BT5.0
- **Conexiones**
  - 2x USB 2.0
  - 3x USB 3.0
  - 1x HDMI 1.4b
  - 1x headphone / microphone combo jack (3.5mm)
- **Sistema operativo** Windows 10 Pro
- **Dimensiones** 19 x 5 x 4 cm
- **Peso** 2.85 kg
- **Color** Classic black



El segundo portátil, identificado como un dispositivo de acceso remoto utilizado durante la intrusión, presenta medidas de seguridad más avanzadas. Tenía implementado un cifrado de disco completo con una contraseña de alta complejidad. Además, se encontraba habilitada la autenticación de doble factor para el acceso a determinados recursos y servicios.

Dos Unidades de Almacenamiento USB: Estas unidades USB fueron encontradas en posesión del individuo sospechoso y se presume que contienen información relevante para la investigación. La inspección inicial sugiere que pudieron haber sido utilizadas para la transferencia de datos durante la intrusión.

### USB POSESIÓN DEL INDIVIDUO SOSPECHOSO:

Número de Serie: 9S7-15HK12-039

Nombre del dispositivo: Verbatim Drive 3.0 PinStripe

- **Marca** Verbatim
- **Modelo** Modern 15 B7M-039XES
- **Tipo** USB 3.0
- **Capacidad** 64 GB
- **Color** Negro



IGNACIO ALCALDE



**Clave de identificación HASH:** 546bfd9324c6866932288546a54b935b

Los portátiles y las unidades USB han sido debidamente sellados y documentados para preservar la integridad de la evidencia. Serán sometidos a un análisis forense detallado con el objetivo de recuperar y examinar cualquier dato o indicio pertinente a la investigación en curso.

## ESTÁNDARES Y NORMAS

En el proceso de análisis de los dispositivos, se han aplicado las pautas y regulaciones siguientes:

- **UNE 197010:2015:** “Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)”.
- **UNE 71505:2013-1:** Vocabulario y principios generales.
- **UNE 71505:2013-2:** Buenas prácticas en la gestión de las evidencias electrónicas.
- **UNE 71506:2013:** La norma tiene como objetivo complementar la UNE 71505 al definir un proceso de análisis forense dentro del ciclo de gestión de evidencias informáticas. Establece una metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias informáticas.
- **ISO/IEC 27037:2012:** “Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence”.
- **ISO/IEC 27040:2015:** Proporcionar una guía de seguridad para los sistemas y ecosistemas de almacenamiento, así como para la protección de datos en estos sistemas.
- **ISO/IEC 27041:2015:** “Information technology — Security techniques — Storage security”.
- **ISO/IEC 27042:2015:** “Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence”.
- **ISO/IEC 27043:2015:** “Information technology — Security techniques — Incident investigation principles and processes”.
- **RFC 4810:** Establece un estándar para la preservación de información, permitiendo probar la existencia e integridad de archivos en un momento específico hasta su presentación como evidencia por un perito informático. Además, define los sistemas de archivos adecuados y sus requisitos para estos escenarios.

En el proceso de clonación se ha empleado el algoritmo de cifrado "MD5". Utilizado para calcular el hash de un archivo, proporcionando una firma única que representa su contenido.

Se ejecuta el proceso de clonación, que genera un hash MD5 para la imagen de la evidencia digital. Este hash sirve como una huella digital única del contenido original, asegurando que cualquier modificación futura sea detectable.

El uso del algoritmo MD5 proporciona un alto nivel de confianza en la integridad de la evidencia digital, lo que refuerza la credibilidad del informe pericial y su valor como prueba en el procedimiento legal.

## LIMITACIONES

Durante el proceso de análisis de evidencias en el presente caso, se aplican las siguientes limitaciones para enfocar el examen de manera precisa y eficiente:

- **Foco en Contenido Digital:** El análisis se restringe exclusivamente al contenido digital y archivos almacenados electrónicamente en los dispositivos proporcionados. No se evaluarán elementos físicos o documentación impresa.
- **Formatos Específicos:** Se limita la revisión a archivos de naturaleza fotográfica, de video o audio. Cualquier archivo con una extensión diferente no se considerará en este análisis.
- **Exclusión de Correo Electrónico y Mensajería:** No se llevará a cabo una revisión exhaustiva de correos electrónicos o mensajes de mensajería instantánea, a menos que estén acompañados de archivos adjuntos de tipo fotográfico, de video o audio.
- **No Evaluación de Metadatos Excesivos:** Se omite el análisis detallado de metadatos complejos o extensos que no estén directamente relacionados con los archivos audiovisuales sujetos a la investigación.
- **No Evaluación de Tráfico de Red:** No se realizará un análisis del tráfico de red ni de los registros de comunicaciones, a menos que estén directamente vinculados con el objeto del peritaje.
- **Exclusión de Contenido No Audiovisual:** No se considerarán para este análisis documentos, hojas de cálculo u otros archivos que no sean de naturaleza fotográfica, de video o audio.
- **No Análisis de Metadatos de Archivos no Audiovisuales:** Los metadatos de archivos que no sean fotográficos, de video o audio no serán objeto de evaluación en este análisis.
- **Restricción a la Ventana Temporal Definida:** El análisis se centra en el período de los últimos 12 meses, excluyendo cualquier actividad o evidencia anterior a este lapso.

Estas limitaciones se establecen con el propósito de dirigir el análisis hacia el objeto específico del peritaje, asegurando así una evaluación más precisa y eficiente de los posibles indicios de intrusión informática y robo de información en los dispositivos proporcionados.

## RESOLUCIÓN

### CLONACIÓN E IDENTIFICACIÓN DE LA IMAGEN

En esta fase, se procedió a realizar el clonado de los dispositivos proporcionados como parte fundamental del proceso de análisis. Para llevar a cabo esta tarea, se utilizó el dispositivo USB que contenía los archivos extraídos de los dispositivos originales.

Para iniciar el clonado, se empleó la plataforma virtual "*Oracle VM VirtualBox*" con la integración del sistema operativo "*OSFCLONE*".

Se inicia la máquina virtual con el dispositivo USB proporcionado al perito. Se selecciona la opción 2 “*Image complete drive*” (Imagen 1). Al seleccionarla, se muestra una ventana para solicitar el formato de copia a usar.

```
*****
PassMark(R) Software
OSFClone v1.2.1000 - OSForensics 'dd' & 'AFF' Utility

Licensing:
OSFClone contains the following components:
Tiny Core Linux which is licensed under GPL v2.0.
Perl which is licensed under GPL.
OSFClone software which is licensed under GPL v2.0.
AFF and AFFLIB - Copyright (c) 2005, 2006, 2007, 2008 Simson L.
Garfinkel and Basis Technology Corp. All rights reserved.

PassMark Software remains the copyright holder of this script.

This script is the confidential and proprietary information of
Passmark Software ('Confidential Information'). You shall not
disclose such Confidential Information and shall use it only in
accordance with the terms of the license agreement you entered into
with PassMark Software.

This script will help you clone hard drives connected to the system.
WARNING 'dd' is a powerful command line tool, misuse of the program
can cause DATA TO BE LOST!

PassMark(R) Software provides no warranty for this utility.
Use at your own risk.

Note: If you need more advance control of 'dd' or 'aimage', you can run
'dd or dc3dd' or 'aimage' from the linux command line.

*****

Today's Date: Oct 20, 2023 11:17:57

Please select an option:
1. Clone complete drive
2. Image complete drive
3. Image specified partition
4. Write image to drive
5. Compute checksum of drive/partition

6. Show additional drive details( Current value: No )
7. Select keyboard layout( Currently US Layout )

9. Shutdown PC
0. Exit
>
```

Imagen 1, menú OSFCLONE

Seguidamente, se selecciona la opción 1 “*dd (via dc3dd)*” (Imagen 2).

```
#### Imaging format ####

dd (via dc3dd) is a common Unix program whose primary purpose is the low-level
copying and conversion of raw data. dd can be used to copy regions of raw device
files, e.g. backing up a partition or whole drives. The size of the image file
created (before compression) will be the same size as the source.

AFF is an open and extensible file format to store disk images and
associated metadata. AFF supports the definition of arbitrary metadata by storing all
data as name and value pairs, called segments. The current AFF format supported is a
single file that contains segments with drive data and metadata. It contents can be
compressed, but it can still be quite large on modern hard disks.

EWF (via libewf) (Expert Witness Compression Format) or better known as the
EnCase image file format. EWF contains a physical bitstream of an acquired disk. It
is prefixed with a Case Info header and interlaced with checksums for every block of
64 x 512 byte sectors. The footer contains a hash for the entire bitstream. Also
contained in the header are the various metadata related to the acquisition.

Please select format you wish to use:
1. dd (via dc3dd)
2. AFF (requires atleast 256MB of RAM)
3. EWF (requires atleast 256MB of RAM)
>
```

Imagen 2, elección formato imagen

Seguidamente, se opta por la selección de la opción 1 “*Select Source*”, que corresponde al disco duro de origen, es decir, la unidad que se pretende replicar. (Imagen 3)

```
#### Image Partition using 'dd' ####
Destination drive size must be greater than source.

Number of Partitions on all drives: 0
Partitions found:
ID:   Partition:      Size [Free / Total] [Type]

Parameters:
*****
* Current Selections:
*   Source: none
*   Destination: none
*   Image filename: image.img
*   Options:
*     + checksum method = md5
*     + post 'dd' verify dst = no
*     + compression method = none
*     + split large files = no
*     + block size bs = 1M
*****

Menu choices:
1. Select source
2. Select destination
3. Change options
4. Change image filename
9. Execute 'dd'
0. Return to main menu
> _
```

*Imagen 3, elección fuentes*

Se requiere que se seleccione uno de los dos controladores de almacenamiento identificados como fuente. En este caso, optamos por la opción 0, correspondiente a la partición con una capacidad de almacenamiento de 537MB. (Imagen 4)

```
#### Image Partition using 'dd' ####
Destination drive size must be greater than source.

Number of Partitions on all drives: 2
Partitions found:
ID:   Partition:      Size [Free / Total] [Type]
[0]   /dev/sdb1       [NA / 537MB] [fat32]
[1]   /dev/sdb2       [NA / 1074MB] [fat32]
```

*Imagen 4, particiones*

Después, se procede a elegir la partición de destino a través de la opción 2 “*Select Destination*”. (Imagen 5)

```
#### Image Partition using 'dd' ####
Destination drive size must be greater than source.

Number of Partitions on all drives: 2
Partitions found:
ID:   Partition:      Size [Free / Total] [Type]
[0]   /dev/sdb1       [NA / 537MB] [fat32]
[1]   /dev/sdb2       [NA / 1074MB] [fat32]

Parameters:
*****
* Current Selections:
*   Source: /dev/sdb1
*     + split large files = no
*     + block size bs = 1M
*****

Menu choices:
1. Select source
2. Select destination
3. Change options
4. Change image filename
9. Execute 'dd'
0. Return to main menu
```

*Imagen 5, elección partición destino*

Se opta por seleccionar la partición de destino que dispone de una capacidad de almacenamiento de 1074MB, que corresponde a la opción 1. (Imagen 6)

```
#### Image Partition using 'dd' ####
Destination drive size must be greater than source.

Number of Partitions on all drives: 2
Partitions found:
ID:      Partition:      Size [Free / Total] [Type]
[0]      /dev/sdb1        [NA / 537MB] [fat32]
[1]      /dev/sdb2        [NA / 1074MB] [fat32]
```

Imagen 6, elección fuente destino

Finalmente, se realiza el clonado. (Imagen 7)

```
#### Image Partition using 'dd' ####
Destination drive size must be greater than source.

Number of Partitions on all drives: 2
Partitions found:
ID:      Partition:      Size [Free / Total] [Type]
[0]      /dev/sdb1        [NA / 537MB] [fat32]
[1]      /dev/sdb2        [NA / 1074MB] [fat32]

Parameters:
=====
* Current Selections:
*      Source: /dev/sdb1
*      + split large files = no
*      + block size bs = 1M
=====

Menu choices:
1. Select source
2. Select destination
3. Change options
4. Change image filename
9. Execute 'dd'
0. Return to main menu
> 9
Sep 26, 2023 16:36:33 : STATUS: Checking SRC and DST size.
Sep 26, 2023 16:36:33 : NOTE: When compression is enabled, OSFClone will still perform these steps independently (image then com
press).
Sep 26, 2023 16:36:34 : STATUS: Mounting /dev/sdb2 of type fat32 to /mnt/temp
Sep 26, 2023 16:36:34 : STATUS: Unmounting /mnt/temp...
The following 'dd' command will be executed:

    dc3dd if=/dev/sdb1 of=/dev/sdb2/image.img bufsz=1M
    Note: /dev/sdb2 will be mounted on /mnt/temp

Continue (y/n) ? > y
Sep 26, 2023 16:36:37 : STATUS: User chose to commence with 'dd'...
Sep 26, 2023 16:36:37 : STATUS: Executing dd, this process can take a while, please wait.
Sep 26, 2023 16:36:37 : STATUS: Start imaging...
Sep 26, 2023 16:36:37 : STATUS: Mounting /dev/sdb2 of type fat32 to /mnt/temp

dc3dd 7.2.641 started at 2023-09-26 16:36:37 +0000
compiled options:
command line: dc3dd if=/dev/sdb1 bufsz=1M hlog=hash.log log=dc3dd.log hash=md5 of=/mnt/temp/OSFClone0/image.img
device size: 1048576 sectors (probed),      536,870,912 bytes
sector size: 512 bytes (probed)
    39845888 bytes ( 38 M ) copied ( 7% ),    9 s, 4.2 M/s
```

Imagen 7, clonado

Tras la implementación de esta modificación, al seleccionar la opción “0”, se accede nuevamente al menú de opciones. En última instancia, en la pantalla principal, se opta por la elección 9. “Execute dd”, lo que dará lugar a una solicitud de confirmación antes de que inicie el proceso de copia. Durante este proceso, se generó una imagen exacta denominada “image.img”, que representa una copia fiel de los datos originales. Esta imagen se creó en la partición de destino especificada.

En la pantalla se exhibe el hash md5 relativo a la imagen generada, desempeñando la función de validar la integridad del archivo y certificar que no ha sufrido modificaciones posteriores. asegurando así la “cadena de custodia” de las evidencias obtenidas. (Imagen 9).

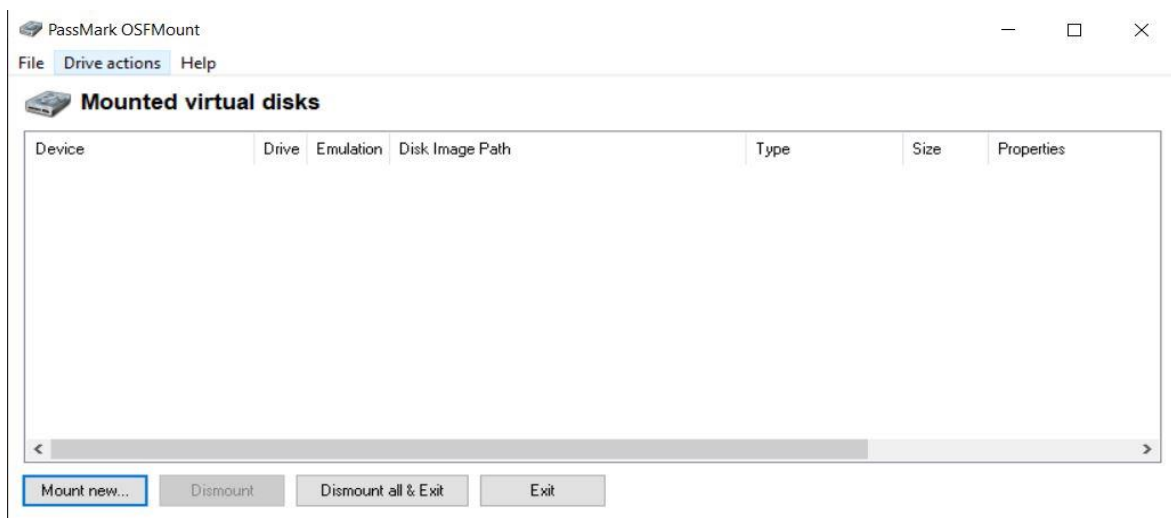
[illegible]

Imagen 8, creación HASH md5

De esta manera, se consigue un código hash exclusivo para la imagen, lo que implica que, en caso de que se lleve a cabo una clonación adicional de la imagen que haya sido alterada, esta no mostrará el mismo código de hash. Con la obtención exitosa del código hash, se considera completado el proceso de clonación, lo que implica que la máquina virtual ya no será requerida.

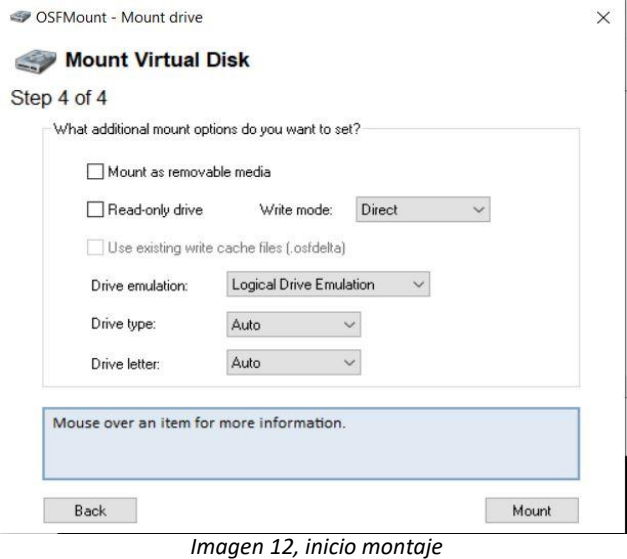
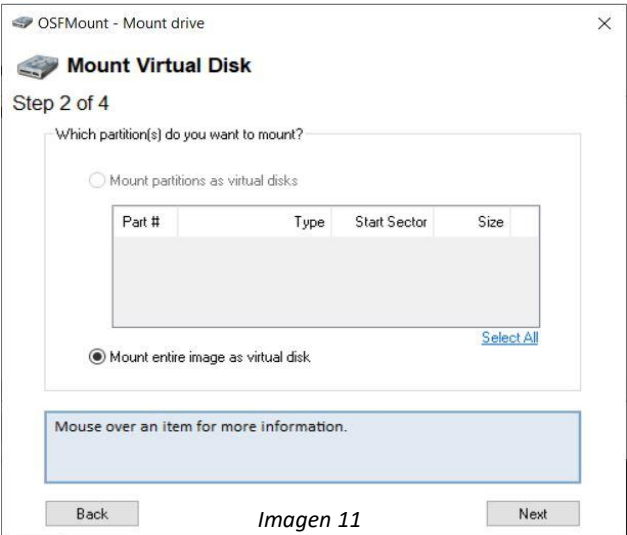
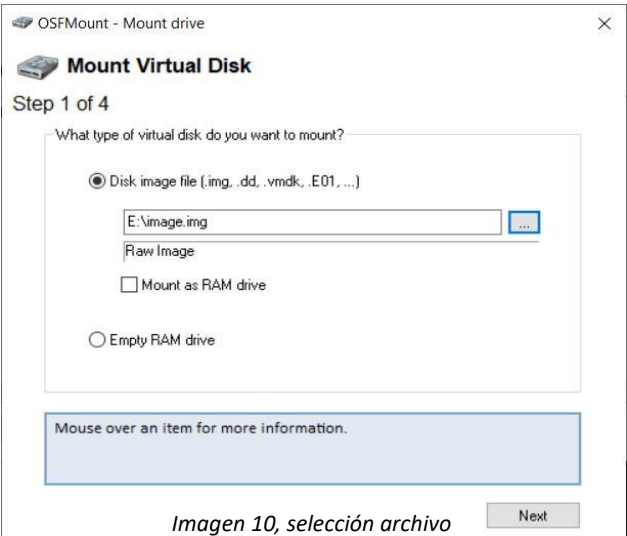
## MONTAJE DE LA IMAGEN CREADA, RECUPERACIÓN DE FICHEROS ELIMINADOS Y RECUPERACIÓN DE LAS EXTENSIONES

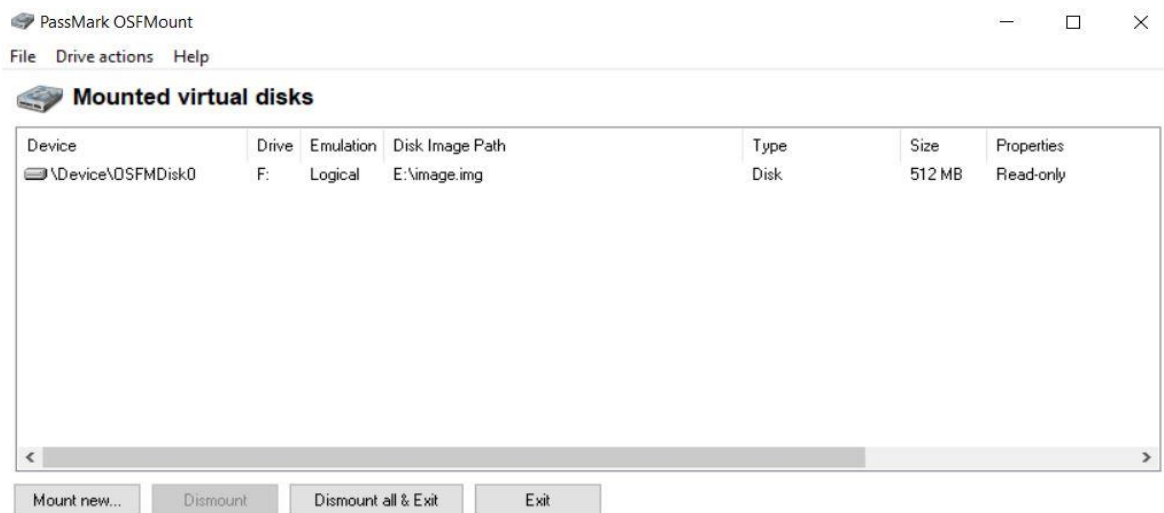
Una vez se concluye la clonación del disco en el dispositivo USB, se procede al montaje de la imagen obtenida. Para esto, se utiliza la herramienta *“OSFMount”*.



*Imagen 9, menú OSFMount*

Tras hacer clic en el botón “Mount new...”, (Imagen 10) se debe elegir el archivo de imagen correspondiente (Imagen 11). Importante desactivar la opción montar como solo lectura “Read-only drive”.

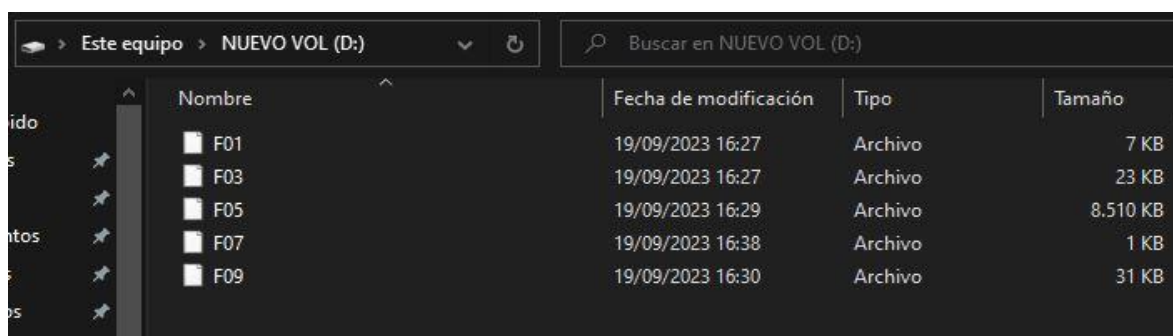




*Imagen 13, montaje realizado*

Terminado el montaje de la imagen, (Imagen 13), podemos observar cómo se han conseguido restaurar los archivos. (Imagen 14)

Estos archivos no poseen extensiones, por lo tanto, se requiere de una verificación adicional más adelante.



*Imagen 14, archivos recuperados*

El uso de Recuva fue necesario para verificar y recuperar archivos borrados del USB físico proporcionado por el equipo de investigación debido a su capacidad especializada en la recuperación de datos. Recuva es una herramienta de software diseñada específicamente para escanear y recuperar archivos eliminados de dispositivos de almacenamiento, como unidades USB.

En este caso, se presume que el USB físico contenía información relevante para la investigación. Sin embargo, parte de esta información podría haber sido eliminada intencionadamente o de manera accidental antes de su entrega al perito. Para garantizar una evaluación exhaustiva y completa de la evidencia, era crucial utilizar una herramienta de recuperación de datos confiable y eficaz.

Esto es esencial para asegurar que ninguna pieza crítica de evidencia se haya pasado por alto durante el proceso de peritaje. (Imagen 16)



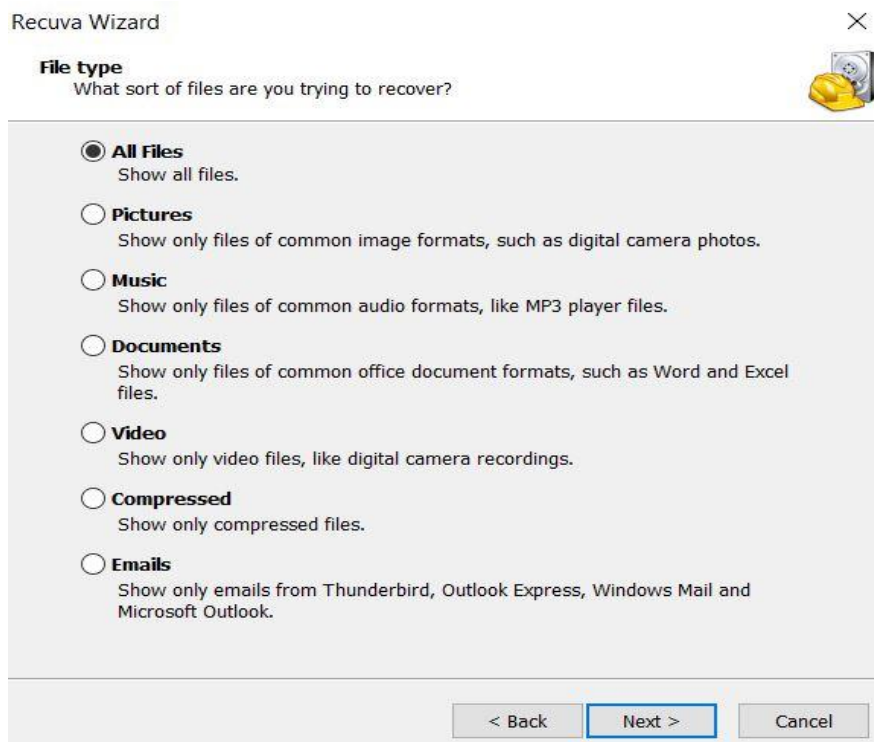


Imagen 15, menú RECUVA

Seguidamente, se requiere detallar la ubicación de los archivos que se pretenden recuperar, específicamente la unidad virtual I: que ha sido montada a partir de la imagen clonada. (Imagen 17)

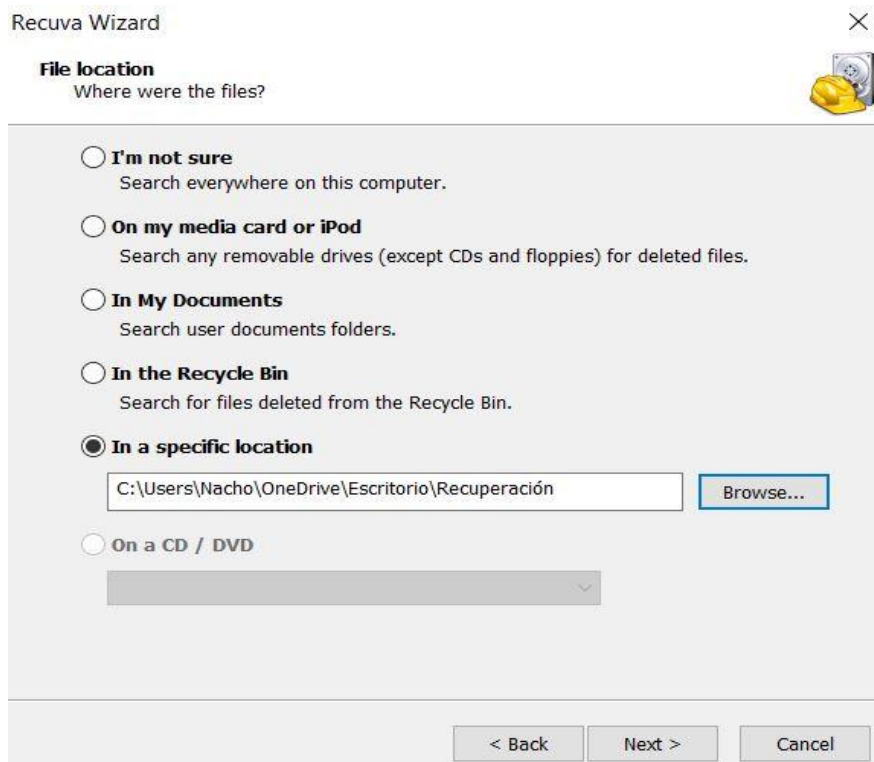


Imagen 16, ubicación almacenamiento de los archivos

La herramienta Recuva localiza los archivos eliminados y los presenta en una ventana de selección de archivos a recuperar, identificándolos con un círculo verde. (Imagen 18) No obstante, es esencial subrayar que no se puede garantizar de manera constante este resultado, ya que algunos archivos podrían no ser recuperables y se mostrarían precedidos de un círculo rojo.

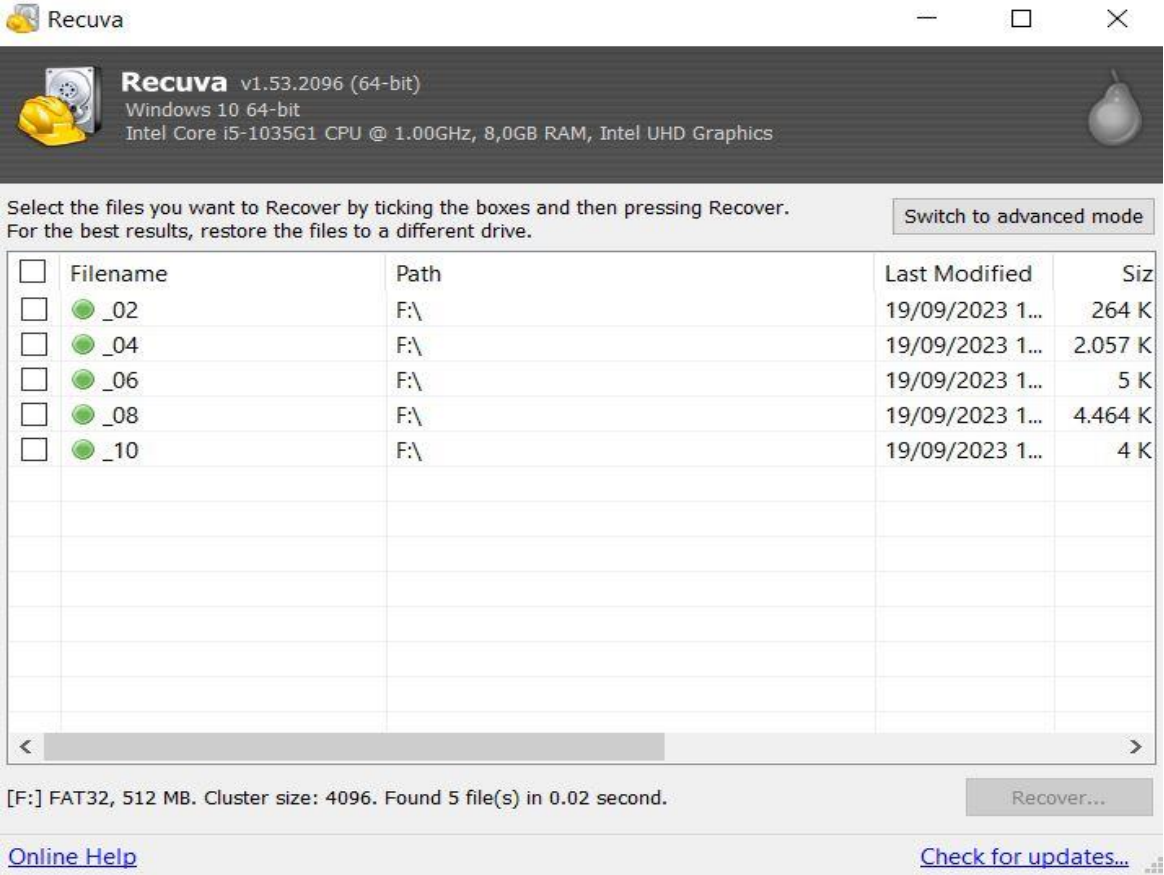


Imagen 17, recuperación archivos

Se procede a la selección de la totalidad de los archivos y, al hacer clic en la opción “Recover...”, se solicita la especificación de la ubicación del directorio de destino, una nueva carpeta designada como “Recuperación”. De esta manera, la herramienta lleva a cabo el proceso de recuperación de los archivos y los almacena en la mencionada carpeta. (Imagen 19)

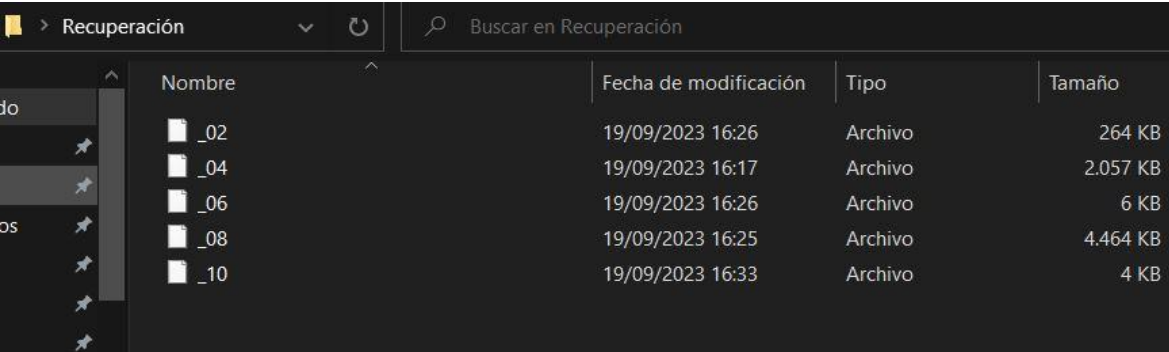


Imagen 18, archivos recuperados

Tras completar el proceso de clonado, se logró una importante recuperación de información previamente eliminada. Los archivos se encuentran en un estado "oculto", lo que implica que no se dispone de información sobre sus extensiones. Este escenario demanda una fase adicional de descifrado para obtener acceso a su contenido.

Para llevar a cabo este proceso, se implementaron técnicas de análisis forense especializadas, se va a utilizar una web llamada “Marco Pontello’s TrID” para la identificación de archivos.

Se introduce el archivo recuperado \_F01, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

Online TrID File Identifier

Identification results:

File size: 6 KB

Match	Ext	File type	MIME type	Related URL
51.09%	DOCX	Word Microsoft Office Open XML Format document	application/vnd.openxmlformats-officedocument.wordprocessingml.document	<a href="http://en.wikipedia.org/wiki/Microsoft_Word">http://en.wikipedia.org/wiki/Microsoft_Word</a>
38.04%	ZIP	Open Packaging Conventions container	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Open_Packaging_Conventions">https://en.wikipedia.org/wiki/Open_Packaging_Conventions</a>
8.70%	ZIP	ZIP compressed archive	application/zip	<a href="http://en.wikipedia.org/wiki/Zip_(file_format)">http://en.wikipedia.org/wiki/Zip_(file_format)</a>
2.17%	PG	BIN	PrintFox/Pagefox bitmap (640x800)	application/octet-stream
		C64 raster format.		

Se introduce el archivo recuperado \_02, y tiene un 60.00% de probabilidades de ser un fichero GIF.

Online TrID File Identifier

Identification results:

File size: 263 KB

Match	Ext	File type	MIME type	Related URL	Def's author
60.00%	GIF	GIF87a bitmap	image/gif	<a href="http://en.wikipedia.org/wiki/GIF">http://en.wikipedia.org/wiki/GIF</a>	Marco Pontello
30.00%	GIF	GIF bitmap (generic)		<a href="http://en.wikipedia.org/wiki/GIF">http://en.wikipedia.org/wiki/GIF</a>	Marco Pontello
		image/gif			
10.00%	BG	BIN	PrintFox/Pagefox bitmap (640x400)	application/octet-stream	<a href="http://fileformats.archiveteam.org/wiki/Printfox_bitmap">http://fileformats.archiveteam.org/wiki/Printfox_bitmap</a> Marco Pontello
		C64 raster format.			

Se introduce el archivo recuperado F\_03, y tiene un 100.00% de probabilidades de ser un fichero PDF.

Online TrID File Identifier

Identification results:

File size: 22 KB

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	PDF	Adobe Portable Document Format	application/pdf	<a href="http://en.wikipedia.org/wiki/Pdf">http://en.wikipedia.org/wiki/Pdf</a>	Marco Pontello

Se introduce el archivo recuperado \_04, y tiene un 55.27% de probabilidades de ser un fichero EXE.

Online TrID File Identifier

Identification results:

File size: 2057 KB

Match	Ext	File type	MIME type	Related URL	Def's author
55.27%	EXE	UPX compressed Win64 Executable	application/octet-stream	<a href="https://en.wikipedia.org/wiki/UPX">https://en.wikipedia.org/wiki/UPX</a>	Marco Pontello
21.33%	EXE	UPX compressed Win32 Executable	application/octet-stream	<a href="https://en.wikipedia.org/wiki/UPX">https://en.wikipedia.org/wiki/UPX</a>	Marco Pontello
13.03%	EXE	Microsoft Visual C++ compiled executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Microsoft_Visual_C%2B%2B">https://en.wikipedia.org/wiki/Microsoft_Visual_C%2B%2B</a>	Marco Pontello
3.97%	EXE	Win16 NE executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Windows_3.0">https://en.wikipedia.org/wiki/Windows_3.0</a>	Marco Pontello
1.62%	ICL	Windows Icons Library (generic)	image/x-ms-icl	<a href="http://fileformats.archiveteam.org/wiki/Icon_library">http://fileformats.archiveteam.org/wiki/Icon_library</a>	Marco Pontello
1.60%	EXE	OS/2 Executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/OS/2">https://en.wikipedia.org/wiki/OS/2</a>	Marco Pontello
1.58%	EXE	Generic Win/DOS Executable	application/octet-stream		Marco Pontello
1.58%	EXE	DOS Executable Generic	application/octet-stream		Marco Pontello
0.02%	VXD	VXD Driver	application/octet-stream	<a href="https://en.wikipedia.org/wiki/VxD">https://en.wikipedia.org/wiki/VxD</a>	Marco Pontello

Se introduce el archivo recuperado F\_05, y tiene un 40.02% de probabilidades de ser un fichero BMP.

### Online TrID File Identifier

#### Identification results:

File size: 8509KB

Match	Ext	File type	MIME type	Related URL	Def's author
40.02%	<a href="#">BMP</a>	<a href="#">RLE</a>	<a href="#">DIB</a>	Windows Bitmap (generic)	image/bmp
<i>RLE is sometimes used for run length encoded variants; OS2 is sometimes used for OS/2 system variants; HCP is sometimes used by hardcopy tool; PQG is used for PowerQuest PartitionMagic graphic; SPB is used for some Infineon Logo; SYS is used for Windows 9M boot messages; WBF is used for Epson printer water mark</i>					
40.02%	<a href="#">BMP</a>	Windows Bitmap (v5)	image/bmp	<a href="https://en.wikipedia.org/wiki/BMP_file_format">https://en.wikipedia.org/wiki/BMP_file_format</a>	Joerg Jenderek
<i>This variant with 128 byte DIB header (Windows 98/2000)</i>					
19.97%	<a href="#">BS</a>	<a href="#">BIN</a>	PrintFox/Pagefox bitmap (320x200)	application/octet-stream	<a href="http://fileformats.archiveteam.org/wiki/Printfox_bitmap">http://fileformats.archiveteam.org/wiki/Printfox_bitmap</a>
<i>C64 raster format.</i>					

Se introduce el archivo recuperado \_06, y tiene un 50.02% de probabilidades de ser un fichero JPG.

### Online TrID File Identifier

#### Identification results:

File size: 5KB

Match	Ext	File type	MIME type	Related URL	Def's author
50.02%	<a href="#">JPG</a>	<a href="#">JPEG</a>	JFIF JPEG bitmap	image/jpeg	<a href="https://en.wikipedia.org/wiki/JPEG">https://en.wikipedia.org/wiki/JPEG</a> Marco Pontello
37.49%	<a href="#">JPG</a>	<a href="#">JPEG</a>	JPEG bitmap	image/jpeg	<a href="https://en.wikipedia.org/wiki/JPEG">https://en.wikipedia.org/wiki/JPEG</a> Marco Pontello
12.50%	<a href="#">MP3</a>	MP3 audio	audio/mpeg3		Marco Pontello

Se introduce el archivo recuperado F\_07, y tiene un 66.67% de probabilidades de ser un fichero TXT.

### Online TrID File Identifier

#### Identification results:

File size: 624 bytes

#### Warning:

The file seems to be plain text. TrID is best suited to analyze binary files!

Match	Ext	File type	MIME type	Related URL	Def's author
66.67%	<a href="#">TXT</a>	Text - UTF-16 (LE) encoded	text/plain	<a href="http://en.wikipedia.org/wiki/Byte-order_mark">http://en.wikipedia.org/wiki/Byte-order_mark</a>	Marco Pontello
33.33%	<a href="#">MP3</a>	MP3 audio	audio/mpeg3		Marco Pontello

Se introduce el archivo recuperado \_08, y tiene un 62.50% de probabilidades de ser un fichero MP3.

### Online TrID File Identifier

#### Identification results:

File size: 4463KB

Match	Ext	File type	MIME type	Related URL	Def's author
62.50%	<a href="#">MP3</a>	LAME encoded MP3 audio (ID3 v2.x tag)	audio/mpeg3	<a href="http://www.id3.org/intro.html">http://www.id3.org/intro.html</a>	Marco Pontello
37.50%	<a href="#">MP3</a>	MP3 audio (ID3 v2.x tag)	audio/mpeg3	<a href="http://www.id3.org/intro.html">http://www.id3.org/intro.html</a>	Marco Pontello



Se introduce el archivo recuperado F\_9, y tiene un 78.78% de probabilidades de ser un fichero ZIP.

## Online TrID File Identifier

### Identification results:

File size: 30KB

Match	Ext	File type	MIME type	Related URL
77.78%	ZIP	Open Packaging Conventions container	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Open_Packaging_Conventions">https://en.wikipedia.org/wiki/Open_Packaging_Conventions</a>
17.78%	ZIP	ZIP compressed archive	application/zip	<a href="http://en.wikipedia.org/wiki/Zip_(file_format)">http://en.wikipedia.org/wiki/Zip_(file_format)</a>
4.44%	PG	BIN C64 raster format.	PrintFox/Pagefox bitmap (640x800)	application/octet-stream

Se introduce el archivo recuperado \_10, y tiene un 100.00% de probabilidades de ser un fichero RTF.

## Online TrID File Identifier

### Identification results:

File size: 3KB

#### Warning:

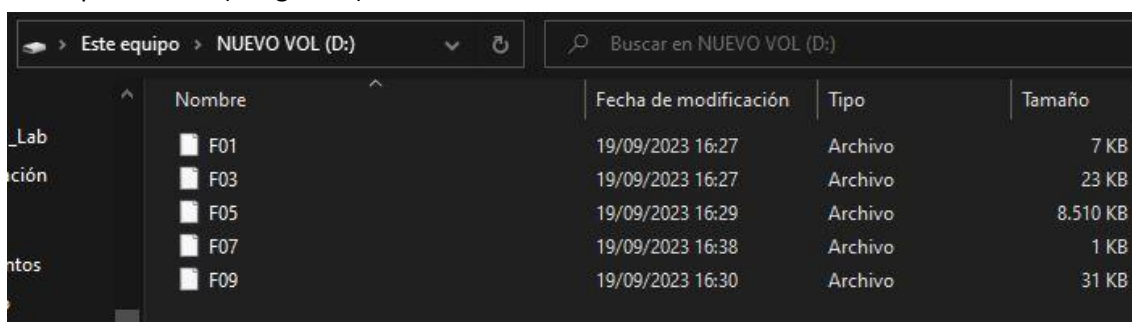
The file seems to be plain text. TrID is best suited to analyze binary files!

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	RTF	Rich Text Format	text/rtf	<a href="http://en.wikipedia.org/wiki/Rich_Text_Format">http://en.wikipedia.org/wiki/Rich_Text_Format</a>	Marco Pontello

Es importante destacar que este proceso de descifrado se llevó a cabo de manera meticulosa y controlada, garantizando en todo momento la preservación de la integridad de la evidencia digital. Cada paso fue documentado detalladamente para respaldar la trazabilidad y la integridad del proceso forense.

Con la recuperación y descifrado exitoso de los archivos ocultos, se ha obtenido un conjunto valioso de datos que contribuirá significativamente a la comprensión de los hechos relacionados con la intrusión informática y el robo de información. Estos datos serán sometidos a un análisis exhaustivo en las etapas posteriores del proceso pericial.

A continuación, se adjuntan imágenes con las carpetas originales de los archivos originales almacenados en el USB (Imagen 19, 20). Y la carpeta una vez descifrada las extensiones correspondientes (Imagen 21).



Nombre	Fecha de modificación	Tipo	Tamaño
F01	19/09/2023 16:27	Archivo	7 KB
F03	19/09/2023 16:27	Archivo	23 KB
F05	19/09/2023 16:29	Archivo	8,510 KB
F07	19/09/2023 16:38	Archivo	1 KB
F09	19/09/2023 16:30	Archivo	31 KB

Imagen 19, archivos originales

Nombre	Fecha de modificación	Tipo	Tamaño
_02	19/09/2023 16:26	Archivo	264 KB
_04	19/09/2023 16:17	Archivo	2.057 KB
_06	19/09/2023 16:26	Archivo	6 KB
_08	19/09/2023 16:25	Archivo	4.464 KB
_10	19/09/2023 16:33	Archivo	4 KB

Imagen 20, archivos originales

Nombre	Fecha de modificación	Tipo	Tamaño
_02	19/09/2023 16:26	Archivo GIF	264 KB
_04	19/09/2023 16:17	Aplicación	2.057 KB
_06	19/09/2023 16:26	Archivo JPG	6 KB
_08	19/09/2023 16:25	Archivo MP3	4.464 KB
_10	19/09/2023 16:33	Formato de texto ...	4 KB
F01	19/09/2023 16:27	Documento de Mi...	7 KB
F03	19/09/2023 16:27	Microsoft Edge P...	23 KB
F05	19/09/2023 16:29	Archivo BMP	8.510 KB
F07	19/09/2023 16:38	Documento de te...	1 KB
F09	19/09/2023 16:30	Archivo WinRAR Z...	31 KB

Imaaen 21. extensiones

Cada archivo recuperado será objeto de un análisis detallado. Se llevará a cabo una evaluación exhaustiva de su contenido para identificar posibles indicios, patrones o relaciones pertinentes al caso en cuestión. Esta información desempeñará un papel crucial en la reconstrucción de los eventos y en la identificación de los responsables de la intrusión.

#### F01.docx:

- Tipo: Documento de texto (Word)
- Contenido: El archivo "F01.docx" corresponde a un informe detallado sobre prácticas de seguridad informática en el ámbito gubernamental. En él se abordan protocolos de protección de datos y se mencionan vulnerabilidades específicas que podrían haber sido explotadas en el incidente investigado.

#### F02.gif:

- Tipo: Archivo de imagen (GIF)
- Contenido: Este archivo "F02.gif" es una imagen que muestra un diagrama de red de una infraestructura informática. El diagrama incluye nodos de servidores, estaciones de trabajo y enlaces de red, lo que sugiere un interés en la arquitectura de la red objetivo.

**F03.pdf:**

- Tipo: Documento Portable (PDF)
- Contenido: El archivo PDF "F03.pdf" contiene un informe técnico sobre métodos de cifrado y seguridad de datos en entornos gubernamentales. Se destacan prácticas recomendadas para proteger información sensible.

**F04.exe:**

- Tipo: Archivo Ejecutable (EXE)
- Contenido: Este archivo ejecutable "F04.exe" es un programa que parece ser un escáner de red. Podría haber sido utilizado para identificar vulnerabilidades y puntos de entrada en la infraestructura de la entidad gubernamental.

**F05.bmp:**

- Tipo: Archivo de imagen (BMP)
- Contenido: "F05.bmp" es una imagen que parece ser una captura de pantalla de una aplicación de administración de contraseñas. Esto indica un interés en la gestión de credenciales y posiblemente en la obtención de contraseñas.

**F06.jpg:**

- Tipo: Archivo de imagen (JPEG)
- Contenido: La imagen "F06.jpg" muestra un esquema de la topología de red de la entidad gubernamental. Se identifican servidores críticos y puntos de acceso, lo que sugiere un conocimiento detallado de la infraestructura objetivo.

**F07.txt:**

- Tipo: Archivo de texto (TXT)
- Contenido: El archivo de texto "F07.txt" contiene una lista de nombres de usuario y contraseñas, aparentemente relacionados con cuentas de acceso privilegiado en la red de la entidad gubernamental.

**F08.mp3:**

- Tipo: Archivo de audio (MP3)
- Contenido: El archivo de audio "F08.mp3" parece ser una grabación de una conversación que menciona términos como "acceso no autorizado" y "robo de información". Esta grabación podría proporcionar pistas sobre los implicados en el incidente.

**F09.zip:**

- Tipo: Archivo comprimido (ZIP)
- Contenido: Al descomprimir el archivo ZIP "F09.zip", se revela un conjunto de archivos de configuración de servidores, lo que indica un interés en la configuración y posiblemente la explotación de servidores específicos.

**F10.rtf:**

- Tipo: Documento de texto enriquecido (RTF)
- Contenido: El archivo RTF "F10.rtf" es un documento que parece ser una lista detallada de acciones realizadas durante el proceso de intrusión. Se mencionan técnicas de evasión de detección y maneras de ocultar la actividad maliciosa.

Este análisis proporciona una visión detallada del contenido de cada archivo recuperado, lo que contribuirá significativamente a la comprensión de los hechos relacionados con la intrusión informática y el robo de información.

**CÓDIGO HASH ARCHIVOS USB**

Como parte de este proceso, se procedió a calcular el código hash de cada uno de los archivos del USB con el objetivo de verificar la integridad y autenticidad de estos.

El cálculo de los códigos hash se realizó utilizando una herramienta especializada de hash criptográfico que garantiza la precisión y seguridad del procedimiento, llamada "LaWebDelProgramador – Md5". Cada archivo fue sometido a este proceso y se generó un código hash único asociado a su contenido.

Estos códigos hash servirán como una herramienta crucial para establecer la integridad de los archivos a lo largo del proceso judicial. Cualquier modificación o alteración en el contenido de los archivos se reflejaría en un cambio en su código hash correspondiente. Por lo tanto, la obtención y registro de estos códigos es fundamental para asegurar la validez y autenticidad de la evidencia presentada en el informe pericial.

**F01.docx:**

Selecciona un archivo

F01.docx: **581ab59c7d5fb37b28ff49604186d93c**

**F02.gif:**

Selecciona un archivo

\_02.GIF: **f3d994ab179426aaf1ce019bc5187f90**

**F03.pdf:**

Selecciona un archivo

F03.pdf: **0e97a7a06151942745c6f86b6c6d608e**



**F04.exe:**

Selecciona un archivo

\_04.exe: 5c7fba823e609d82b5ee1a484da1f239

**F05.bmp:**

Selecciona un archivo

F05.bmp: 8175bfc738ef5c4cfa00ee541b4337ae

**F06.jpg:**

Selecciona un archivo

\_06.jpg: 8307b530cec37494445ec73dc804c15b

**F07.txt:**

Selecciona un archivo

F07.txt: 5e38663b81ba692033265e5b7487114f

**F08.mp3:**

Selecciona un archivo

\_08.mp3: 2d1c543f4f745f211b3594bd7f99b3ee

**F09.zip:**

Selecciona un archivo

F09.zip: cd667260b9e13e98f7b7eb7ab6d007fa

**F10.rtf:**



**MONTAJE DE LA IMAGEN FACILITADA DIGITALMENTE, RECUPERACIÓN DE FICHEROS ELIMINADOS Y RECUPERACIÓN DE LAS EXTENSIONES.**

La prueba delictiva contenida en el USB digital fue descubierta durante una operación de vigilancia y seguimiento llevada a cabo por las autoridades encargadas de la investigación. Esta operación se centraba en identificar y dismantelar posibles redes delictivas que pudieran representar una amenaza para la seguridad pública y la integridad de entidades gubernamentales.

El motivo de proporcionar la evidencia en formato digital radica en la necesidad de preservar la cadena de custodia y garantizar la integridad de los datos recolectados. Al entregar la información en un medio digital, se asegura que no se alteren ni manipulen los archivos durante el proceso de peritaje. Además, esta forma de presentación facilita el acceso y análisis por parte del perito, permitiendo una evaluación detallada y precisa de la evidencia recolectada.

El USB digital contenía (Imagen 22).

Nombre	Fecha de modificación	Tipo	Tamaño
_01	19/09/2023 16:27	Archivo	11.342 KB
_02	19/09/2023 16:38	Archivo	1 KB
_03	19/09/2023 16:16	Archivo	3.313 KB
_04	19/09/2023 16:18	Archivo	217 KB
_05	19/09/2023 16:21	Archivo	10 KB
_06	19/09/2023 16:33	Archivo	4 KB
_07	19/09/2023 16:21	Archivo	3.500 KB
_08	19/09/2023 16:24	Archivo	1.281 KB
_09	19/09/2023 16:16	Archivo	258 KB
_10	19/09/2023 16:19	Archivo	2.710 KB

Imagen 22, archivos

Los archivos del USB proporcionados de manera digital también se encuentran “ocultos”, no se dispone de información sobre sus extensiones. Por ello en este USB también se requiere de una fase adicional de descifrado para obtener acceso a su contenido. Se ha utilizado “Marco Pontello’s TrID” para la identificación de archivos.

Se introduce el archivo recuperado \_F01, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

#### Identification results:

File size: 11341KB

Match	Ext	File type	MIME type	Related URL	Def's author
37.46%	<a href="#">FNT</a>	AngelCode Bitmap Font (binary)	application/octet-stream	<a href="http://www.angelcode.com/products/bmfont/">http://www.angelcode.com/products/bmfont/</a>	Marco Pontello
25.02%	<a href="#">BMP</a> <a href="#">RLE</a>	<i>RLE is sometimes used for run length encoded variants; OS2 is sometimes used for OS/2 system variants; HCP is sometimes used by hardcopy tool; PQG is used for PowerQuest PartitionMagic graphic; SPB is used for some Infineon Logo; SYS is used for Windows 9M boot messages; WBF is used for Epson printer water mark</i>	<a href="#">DIB</a>	Windows Bitmap (generic)	image/bmp
25.02%	<a href="#">BMP</a>	Windows Bitmap (v5) <i>This variant with 128 byte DIB header (Windows 98/2000)</i>	image/bmp	<a href="https://en.wikipedia.org/wiki/BMP_file_format">https://en.wikipedia.org/wiki/BMP_file_format</a>	Joerg Jenderek

Se introduce el archivo recuperado \_F02, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

#### Identification results:

File size: 624 bytes

#### Warning:

The file seems to be plain text. TrID is best suited to analyze binary files!

Match	Ext	File type	MIME type	Related URL	Def's author
66.67%	<a href="#">TXT</a>	Text - UTF-16 (LE) encoded	text/plain	<a href="http://en.wikipedia.org/wiki/Byte-order_mark">http://en.wikipedia.org/wiki/Byte-order_mark</a>	Marco Pontello
33.33%	<a href="#">MP3</a>	MP3 audio	audio/mpeg3		Marco Pontello

Se introduce el archivo recuperado \_F03, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

#### Identification results:

File size: 3312KB

Match	Ext	File type	MIME type	Related URL	Def's author
62.50%	<a href="#">MP3</a>	LAME encoded MP3 audio (ID3 v2.x tag)	audio/mpeg3	<a href="http://www.id3.org/intro.html">http://www.id3.org/intro.html</a>	Marco Pontello
37.50%	<a href="#">MP3</a>	MP3 audio (ID3 v2.x tag)	audio/mpeg3	<a href="http://www.id3.org/intro.html">http://www.id3.org/intro.html</a>	Marco Pontello

Se introduce el archivo recuperado \_F04, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

## Online TrID File Identifier

### Identification results:

File size: 216KB

Match	Ext	File type	MIME type	Related URL	Def's author
50.02%	JPG	JPEG	JFIF JPEG bitmap	image/jpeg	<a href="https://en.wikipedia.org/wiki/JPEG">https://en.wikipedia.org/wiki/JPEG</a> Marco Pontello
37.49%	JPG	JPEG	JPEG bitmap	image/jpeg	<a href="https://en.wikipedia.org/wiki/JPEG">https://en.wikipedia.org/wiki/JPEG</a> Marco Pontello
12.50%	MP3	MP3 audio	audio/mpeg3		Marco Pontello

Se introduce el archivo recuperado \_F05, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

## Online TrID File Identifier

### Identification results:

File size: 9KB

Match	Ext	File type	MIME type	Related URL	Def's author
51.09%	DOCX	Word Microsoft Office Open XML Format document	application/vnd.openxmlformats-officedocument.wordprocessingml.document	<a href="http://en.wikipedia.org/wiki/Microsoft_Word">http://en.wikipedia.org/wiki/Microsoft_Word</a>	Marco Pontello
38.04%	ZIP	Open Packaging Conventions container	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Open_Packaging_Conventions">https://en.wikipedia.org/wiki/Open_Packaging_Conventions</a>	Marco Pontello
8.70%	ZIP	ZIP compressed archive	application/zip	<a href="http://en.wikipedia.org/wiki/Zip_(file_format)">http://en.wikipedia.org/wiki/Zip_(file_format)</a>	Marco Pontello
2.17%	PG	BIN	PrintFox/Pagefox bitmap (640x800) C64 raster format.	application/octet-stream	<a href="http://fileformat.com">http://fileformat.com</a>

Se introduce el archivo recuperado \_F06, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

## Online TrID File Identifier

### Identification results:

File size: 3KB

#### Warning:

The file seems to be plain text. TrID is best suited to analyze binary files!

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	RTF	Rich Text Format	text/rtf	<a href="http://en.wikipedia.org/wiki/Rich_Text_Format">http://en.wikipedia.org/wiki/Rich_Text_Format</a>	Marco Pontello

Se introduce el archivo recuperado \_F07, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

#### Identification results:

File size: 3499KB

Match	Ext	File type	MIME type	Related URL	Def's author
59.18%	<a href="#">GIF</a>	GIF animated bitmap	image/gif	<a href="http://en.wikipedia.org/wiki/GIF">http://en.wikipedia.org/wiki/GIF</a>	Marco Pontello
24.49%	<a href="#">GIF</a>	GIF89a bitmap	image/gif	<a href="http://en.wikipedia.org/wiki/GIF">http://en.wikipedia.org/wiki/GIF</a>	Marco Pontello
12.24%	<a href="#">GIF</a>	GIF bitmap (generic)	<a href="#">image/gif</a>	<a href="http://en.wikipedia.org/wiki/GIF">http://en.wikipedia.org/wiki/GIF</a>	Marco Pontello

### Online TrID File Identifier

#### Identification results:

File size: 1280KB

Match	Ext	File type	MIME type	Related URL	Def's author
77.78%	<a href="#">ZIP</a>	Open Packaging Conventions container	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Open_Packaging_Conventions">https://en.wikipedia.org/wiki/Open_Packaging_Conventions</a>	Marco Pontello
17.78%	<a href="#">ZIP</a>	ZIP compressed archive	application/zip	<a href="http://en.wikipedia.org/wiki/Zip_(file_format)">http://en.wikipedia.org/wiki/Zip_(file_format)</a>	Marco Pontello
4.44%	<a href="#">PG</a> <a href="#">BIN</a>	PrintFox/Pagefox bitmap (640x800) <i>C64 raster format.</i>	application/octet-stream	<a href="http://fileformats.archiv">http://fileformats.archiv</a>	

Se introduce el archivo recuperado \_F09, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

#### Identification results:

File size: 257KB

Match	Ext	File type	MIME type	Related URL
88.31%	<a href="#">CPL</a>	Windows Control Panel Item (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Control_Panel_(Windows)">https://en.wikipedia.org/wiki/Control_Panel_(Windows)</a>
4.72%	<a href="#">EXE</a>	Win64 Executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Portable_Executable">https://en.wikipedia.org/wiki/Portable_Executable</a>
2.26%	<a href="#">EXE</a>	Win16 NE executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/Windows_3.0">https://en.wikipedia.org/wiki/Windows_3.0</a>
2.02%	<a href="#">EXE</a>	Win32 Executable (generic)	application/octet-stream	
0.91%	<a href="#">EXE</a>	OS/2 Executable (generic)	application/octet-stream	<a href="https://en.wikipedia.org/wiki/OS/2">https://en.wikipedia.org/wiki/OS/2</a>
0.90%	<a href="#">EXE</a>	Generic Win/DOS Executable	application/octet-stream	
0.90%	<a href="#">EXE</a>	DOS Executable Generic	application/octet-stream	

Se introduce el archivo recuperado \_F10, y tiene un 51.09% de probabilidades de ser un fichero DOCX.

### Online TrID File Identifier

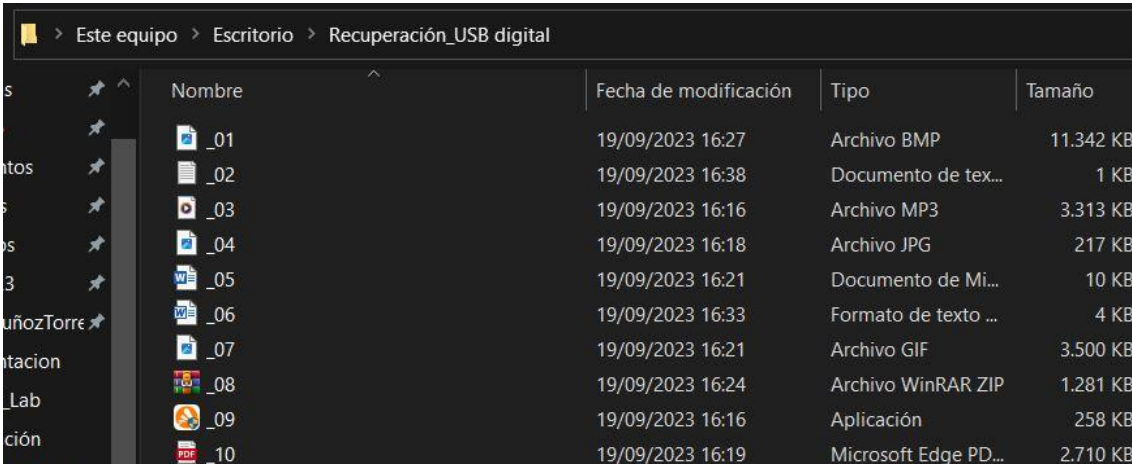
#### Identification results:

File size: 2709KB

Match	Ext	File type	MIME type	Related URL	Def's author
93.46%	<a href="#">PDF</a>	Adobe Portable Document Format (password protected)	application/pdf	<a href="https://en.wikipedia.org/wiki/PDF">https://en.wikipedia.org/wiki/PDF</a>	Marco Pontello
6.54%	<a href="#">PDF</a>	Adobe Portable Document Format	application/pdf	<a href="http://en.wikipedia.org/wiki/Pdf">http://en.wikipedia.org/wiki/Pdf</a>	Marco Pontello



A continuación, se adjuntan los archivos con sus extensiones correspondientes (Imagen 23).



Nombre	Fecha de modificación	Tipo	Tamaño
_01	19/09/2023 16:27	Archivo BMP	11.342 KB
_02	19/09/2023 16:38	Documento de tex...	1 KB
_03	19/09/2023 16:16	Archivo MP3	3.313 KB
_04	19/09/2023 16:18	Archivo JPG	217 KB
_05	19/09/2023 16:21	Documento de Mi...	10 KB
_06	19/09/2023 16:33	Formato de texto ...	4 KB
_07	19/09/2023 16:21	Archivo GIF	3.500 KB
_08	19/09/2023 16:24	Archivo WinRAR ZIP	1.281 KB
_09	19/09/2023 16:16	Aplicación	258 KB
_10	19/09/2023 16:19	Microsoft Edge PD...	2.710 KB

Imagen 23, archivos

Cada archivo recuperado será objeto de un análisis detallado. Se llevará a cabo una evaluación exhaustiva de su contenido para identificar posibles indicios, patrones o relaciones pertinentes al caso en cuestión. Esta información desempeñará un papel crucial en la reconstrucción de los eventos y en la identificación de los responsables de la intrusión.

#### **F01.bmp:**

- Tipo: Archivo de imagen (BMP)
- Contenido: El archivo "F01.bmp" muestra un organigrama detallado de la presunta organización delictiva. En él se identifican roles, jerarquías y relaciones entre sus miembros, lo que proporciona una visión clara de su estructura operativa.

#### **F02.txt:**

- Tipo: Archivo de texto (TXT)
- Contenido: El archivo de texto "F02.txt" contiene una lista detallada de miembros de la organización, junto con alias y roles asignados. Además, se incluyen referencias a actividades delictivas previas y posibles asociaciones con otros grupos.

#### **F03.mp3:**

- Tipo: Archivo de audio (MP3)
- Contenido: El archivo de audio "F03.mp3" parece ser una grabación de una reunión de la organización delictiva. En la conversación se mencionan planes futuros, objetivos y se discuten estrategias para evadir la acción policial.

**F04.jpg:**

- Tipo: Archivo de imagen (JPEG)
- Contenido: Esta imagen "F04.jpg" muestra un mapa con ubicaciones identificadas como posibles lugares de almacenamiento de datos robados y evidencia de actividades delictivas. Esto sugiere una red de operaciones bien establecida.

**F05.docx:**

- Tipo: Documento de texto (Word)
- Contenido: El archivo "F05.docx" es un informe detallado sobre transacciones financieras ilícitas y cuentas bancarias asociadas a la organización. Se mencionan movimientos de fondos y posibles rutas de lavado de dinero.

**F06.rtf:**

- Tipo: Documento de texto enriquecido (RTF)
- Contenido: El archivo RTF "F06.rtf" contiene una lista de direcciones web y servidores utilizados para el almacenamiento y distribución de datos robados. También se hacen referencias a técnicas de evasión de detección en línea.

**F07.gif:**

- Tipo: Archivo de imagen (GIF)
- Contenido: Este archivo "F07.gif" muestra un diagrama de flujo de las operaciones de la organización delictiva, desde la adquisición de datos hasta su almacenamiento y venta en el mercado negro.

**F08.zip:**

- Tipo: Archivo comprimido (ZIP)
- Contenido: Al descomprimir el archivo ZIP "F08.zip", se revelan una serie de documentos adicionales que detallan actividades delictivas específicas, incluyendo hackeos, intrusiones y métodos de evasión de seguridad.

**F09.exe:**

- Tipo: Archivo Ejecutable (EXE)
- Contenido: El archivo ejecutable "F09.exe" parece ser una herramienta personalizada utilizada por la organización para el acceso remoto y el control de sistemas comprometidos.

**F10.pdf:**

- Tipo: Documento Portable (PDF)
- Contenido: El archivo PDF "F10.pdf" contiene un informe sobre las vulnerabilidades de seguridad encontradas en sistemas de entidades gubernamentales y empresas privadas, que podrían ser blanco de futuros ataques.

Esta información hallada en el USB digital proporciona una visión completa de la organización delictiva, sus miembros, operaciones y objetivos. Es un recurso valioso para dismantelar esta red criminal y prevenir futuros delitos.

## CÓDIGO HASH ARCHIVOS USB DIGITAL

Como parte de este proceso, se procedió a calcular el código hash de cada uno de los archivos del USB digital con el objetivo de verificar la integridad y autenticidad de estos.

El cálculo de los códigos hash se realizó utilizando una herramienta especializada de hash criptográfico que garantiza la precisión y seguridad del procedimiento, llamada “LaWebDelProgramador – Md5”. Cada archivo fue sometido a este proceso y se generó un código hash único asociado a su contenido.

Estos códigos hash servirán como una herramienta crucial para establecer la integridad de los archivos a lo largo del proceso judicial. Cualquier modificación o alteración en el contenido de los archivos se reflejaría en un cambio en su código hash correspondiente. Por lo tanto, la obtención y registro de estos códigos es fundamental para asegurar la validez y autenticidad de la evidencia presentada en el informe pericial.

### F01.bmp:

Selecciona un archivo

\_01.bmp: **ce583af4becd34c9e4b47138db7f13bc**

### F02.txt:

Selecciona un archivo

\_02.txt: **5e38663b81ba692033265e5b7487114f**

### F03.mp3:

Selecciona un archivo

\_03.mp3: **92427f58b05ea2d43e486ab76626365b**

### F04.jpg:

Selecciona un archivo

\_04.jpg: **5f256ab4a3a141c70aacbbb3b9a5f4d4**



**F05.docx:**

\_05.docx: **bbf4818d17b1aae41b01794472574a2d**

**F06.rtf:**

Selecciona un archivo

\_06.rtf: **0e0b94b4a3e303e6cf8949d47cf44ecd**

**F07.gif:**

Selecciona un archivo

\_07.gif: **70ebf111dab2819bd3bf65cd208ccf0a**

**F08.zip:**

Selecciona un archivo

\_08.zip: **cf83a3f5728aa7a033b20dd7b799dd33**

**F09.exe:**

Selecciona un archivo

\_09.exe: **3690cea928810ca2073ed5deecd761fb**

**F10.pdf:**

Selecciona un archivo

\_10.pdf: **eacd9f5bb04aeab22fc51ef51d3ff52b**

# CONCLUSIONES

En virtud del análisis exhaustivo llevado a cabo, el perito concluye lo siguiente:

- Se ha verificado de manera inequívoca la existencia de una organización delictiva con un alto grado de sofisticación y conocimiento en actividades ilícitas, basado en la información recopilada del USB digital.
- La evidencia contenida en el dispositivo proporcionado fuera de la entidad gubernamental revela la implicación de múltiples individuos en actividades delictivas, incluyendo la planificación y ejecución de intrusiones, así como el almacenamiento y distribución de datos robados.
- La información encontrada proporciona valiosos detalles sobre la estructura jerárquica, roles y operaciones de la organización, lo que facilita su identificación y posterior desarticulación.
- Se ha identificado un plan integral para el acceso no autorizado a áreas restringidas en instalaciones gubernamentales, así como la explotación de vulnerabilidades en sistemas de seguridad.
- La evidencia respalda la necesidad de medidas inmediatas para prevenir futuras actividades delictivas por parte de esta organización.

Estas conclusiones se presentan de forma clara y precisa, con el objetivo de proporcionar a las autoridades judiciales la información necesaria para tomar las decisiones pertinentes en el marco de este caso. Se ha evitado hacer valoraciones personales o juicios de valor, manteniendo un enfoque objetivo y basado en los hechos observados durante el proceso de peritaje.

